

# Nõukogu arvamus (artikli 70 lõike 1 punkt b)



**Arvamus 23/2018 komisjoni ettepanekute kohta, mis käsitlevad Euroopa andmeesitamismäärust ja Euroopa andmesäilitamismäärust elektrooniliste tõendite hankimiseks kriminaalasjades (artikli 70 lõike 1 punkt b)**

**Vastu võetud 26. septembril 2018**

## Sisukord

Sissejuhatus .....	3
1. Määruse ettepaneku õiguslik alus (ELi toimimise lepingu artikkel 82) .....	4
2. Elektroonilisi tõendeid käsitlevate õigusaktide vajalikkus võrreldes vastastikuse õigusabi lepingute ja Euroopa uurimismäärusega .....	5
a) Elektroonilisi tõendeid käsitlevate õigusaktide vajalikkus, arvestades Euroopa uurimismääruses ja vastastikuse õigusabi lepingutes pakutavaid kaitsemeetmeid.....	5
b) Topeltkaristatavuse põhimõttest loobumine.....	6
c) Otse ettevõtete poole pöördumise tagajärg.....	7
3. Uus õiguskaitsepädevuse alus ja asukohakriteeriumi nii-öelda kadumine.....	8
4. „Teenuseosutaja“ mõistet tuleks piirata või täiendada seda andmesubjektide õiguste kaitsmise meetmetega .....	9
5. Mõisteid „tegevuskoht“ ja „esindaja“ tuleks nende ettepanekute kontekstis selgelt eristada nendest mõistetest isikuandmete kaitse üldmääruse kontekstis.....	10
a) Tegevuskoht .....	11
b) Esindaja.....	11
6. Uued andmekategooriad.....	12
7. Euroopa andmesäilitamismääruse ja andmeesitamismäärusega seotud menetluste analüüs ....	13
a) Määruste tegemise künniseid tuleks tõsta ning määrusi peavad tegema või kinnitama kohtud 14	
b) Andmete esitamise tähtaegu tuleks põhjendada .....	15
c) Euroopa andmeesitamismäärust ja andmesäilitamismäärust ei tohi kasutada, et taotleda muu liikmesriigi andmesubjekti andmeid, ilma et selle liikmesriigi pädevaid asutusi vähemalt eelnevalt teavitataks, eelkõige sisuandmete puhul.....	16
d) Euroopa andmesäilitamismäärusi ei tohi kasutada selleks, et hoida kõrvale teenuseosutajate andmete säilitamise kohustustest.....	16
e) Konfidentsiaalsus ja kasutajateave .....	17
f) Menetlus määruse täitmise tagamiseks, kui teenuseosutaja keeldub selle täitmisest .....	17
g) Määruste täitmise tagamine ja kolmanda riigi õigusest tulenev kohustuste konflikt (artiklid 15–16).....	18
h) Andmete edastamise turvalisus määrusele vastamisel .....	19
Järeldused.....	20

## Euroopa Andmekaitseõukogu

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) artikli 70 lõike 1 punkti b,

### ON VASTU VÕTNUD JÄRGMISE ARVAMUSE:

## Sissejuhatus

2018. aasta aprillis esitas komisjon ettepaneku võtta vastu määrus, mis käsitleb Euroopa andmeesitamismäärust ja Euroopa andmesäilitamismäärust elektrooniliste tõendite hankimiseks kriminaalasjades, ning ettepaneku võtta vastu direktiiv, millega kehtestatakse ühtlustatud normid kriminaalmenetluses tõendite kogumise eesmärgil esindajate määramise kohta. Need kaks ettepanekut COM(2018) 225 final ja COM(2018) 226 final täiendavad teineteist. Komisjoni üldesmärk on parandada liikmesriikide ametiasutuste ja teenuseosutajate, sh ka kolmandates riikides asuvate teenuseosutajate vahelist koostööd ning pakkuda lahendusi probleemile, mis on seotud õiguskaitsepädevuse kindlaksmääramise ja rakendamisega küberruumi puhul.

Kui määruse eelnõus on ette nähtud normid ja menetlused, mida kohaldatakse elektroonilise side teenuste osutajatega seotud andmesäilitamis- ja andmesitusmääruste tegemise, kättetoimetamise ja nende täitmise tagamise suhtes, siis direktiivi eelnõus on sätestatud miinimumnormid esindajate määramise kohta selliste teenuseosutajate puhul, kes ei asu ELis.

2017. aasta novembris,<sup>1</sup> enne kui komisjon oli eelnõud esitanud, tuletas artikli 29 töörühm meelde vajadust tagada mis tahes seadusandliku ettepaneku täielik kooskõlas eelkõige liidu kehtiva andmekaitsevaldkonna *acquis*'ga, aga ka liidu õiguse ja kohtupraktikaga üldiselt.

Eelkõige hoiatas artikli 29 töörühm andmekaitseõiguse ja eraelu puutumatus õiguse piiramise eest seoses telekommunikatsiooniteenuste ja infoühiskonna teenuste osutajate töödeldavate andmetega, eriti kui neid töötlevad täiendavalt õiguskaitseasutused, tuletas meelde vajadust tagada mis tahes ELi õigusakti kooskõla Euroopa Nõukogu kehtiva küberkuritegevuse konventsiooniga ehk Budapesti konventsiooniga ning ELi direktiiviga Euroopa uurimismääruse kohta ning soovitas täpsustada menetlusnorme, mida kohaldatakse elektroonilistele tõenditele juurdepääsemise suhtes riiklikul ja ELi tasandil, tagamaks, et uue õigusaktiga ei anta ametiasutustele uusi volitusi, mida neil riigisiselt ei oleks. Lisaks neile üldistele märkustele esitas artikli 29 töörühm märkusi seadusandlike võimaluste kohta, mida komisjon kaalus tol ajal seoses asjaomaste andmekategoriatega ja vastavate kaitsemeetmetega, mida kohaldatakse nendele andmekategoriatele juurdepääsu suhtes, võimaluse kohta esitada andmeesitamismäärusi/-taotlusi, et kohustada teenuseosutajaid esitama väljaspool ELi asuvaid andmeid, ning sisuliste ja menetluslike tingimuste kui vajalike kaitsemeetmete kohta, mis peaksid kaasema otsese juurdepääsuga andmetele.

Nüüd, kui on esitatud konkreetseid elektroonilisi tõendeid käsitlevad ettepanekud, soovib Euroopa Andmekaitseõukogu kavandatud õigusakte andmekaitse seisukohast üksikasjalikumalt analüüsida.

---

<sup>1</sup> Vt artikli 29 töörühma avaldus ([http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48801](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)).

## 1. Määruse ettepaneku õiguslik alus (ELi toimimise lepingu artikkel 82)

Elektroonilisi tõendeid käsitleva määruse eelnõu puhul on õigusliku alusena välja pakutud ELi toimimise lepingu artikli 82 lõige 1 kriminaalasjades tehtava õiguslase koostöö kohta, milles on sätestatud:

„1. Liidus põhineb kriminaalasjades tehtav õiguslane koostöö kohtuotsuste ja õigusasutuste otsuste vastastikuse tunnustamise põhimõttel ning hõlmab liikmesriikide õigus- ja haldusnormide lähendamist lõikes 2 ja artiklis 83 osutatud valdkondades.

Euroopa Parlament ja nõukogu võtavad seadusandliku tavamenetluse kohaselt vastu meetmed, et:

- a) kehtestada eeskirjad ja menetlused igat liiki kohtuotsuste ja õigusasutuste otsuste tunnustamise tagamiseks kõikjal liidus;
- b) ennetada ja lahendada kohtualluvuse konflikte liikmesriikide vahel;
- c) toetada kohtunike, prokuröride ning kohtute ja prokuratuuride töötajate koolitust;
- d) hõlbustada liikmesriikide õigusasutuste või samaväärsete asutuste vahelist koostööd kriminaalasjade menetlemisel ja otsuste täitmisel.“

Komisjon on ettepanekutele lisatud mõjuhinnangus rõhutanud järgmist: „Artikli 82 lõikes 1 on sätestatud, et kriminaalasjades tehtav õiguslane koostöö põhineb vastastikuse tunnustamise põhimõttel. See õiguslik alus hõlmaks võimalikke õigusakte, mis käsitlevad teenuseosutajatega tehtavat otsest koostööd, mille puhul taotleva liikmesriigi ametiasutus pöörduks otse täitjariigi üksuse (teenuseosutaja) poole ja kehtestaks talle isegi kohustusi. Seeläbi lisatakse vastastikusele tunnustamisele uus mõõde, mis läheb kaugemale tavapärasest õiguslasest koostööst liidus, mis on seni põhinenud menetlustel, millesse on kaasatud kaks õigusasutust, üks taotlevas riigis ja teine täitjariigis“ (rõhuasetus lisatud).

Arvestades selle õigusliku aluse kasutamise uudsust avaliku sektori asutuste ja eraettevõtete vaheliste otsetaotluste kontekstis, peab Euroopa Andmekaitsekoostöö nõukogu kahetsusväärseks, et komisjon pole esitanud täiendavat analüüsi ega hinnangut.

Sarnaselt tööühikute eelmises avalduses väljatooduga rõhutab ka Euroopa Andmekaitsekoostöö nõukogu oma kahtlusi selle õigusliku aluse asjakohasuse suhtes; neid kahtlusi toetab Euroopa Liidu Kohtu ja tema kohtujuristi analüüs arvamuses 1/15. Järelduste hulgas, mis on seotud artikli 82 kui Kanada ja ELi vahelise broneeringuinfo alase lepingu projekti õigusliku aluse õiguspärasusega, rõhutas kohus, et Kanada pädev asutus „ei ole ei õigusasutus ega samaväärne asutus“<sup>2</sup>. Elektroonilisi tõendeid käsitlevate ettepanekute kontekstis paistab üks peamisest eesmärkidest komisjoni märgitu põhjal olevat „liiga koormava“ õiguslase koostöö vältimine. Sellest tulenevalt tugineb ettepanek põhimõttele, et koostöö peaks toimuma ametiasutuse ja teenuseosutaja, mitte kahe ametiasutuse vahel. Ettenähtud menetluse alusel on eelkõige eraõiguslikel üksustel vastuvõtja roll ja nad vastavad õigusasutuste taotlustele.

Euroopa Andmekaitsekoostöö nõukogu märgib, et andmeesitamis- või andmesäilitamismääruste täitmise tagamise protsessiga võib kaasneda vastuvõtva ametiasutuse sekkumine olukorras, kus vastuvõttev teenuseosutaja ei täida oma kohustusi, mistõttu on vaja määruse täitmine tagantjärele tagada. Kuna

<sup>2</sup> Vt selle kohta arvamuse 1/15 punkt 103 ja kohtujuristi ettepaneku punkt 108.

aga kehtestatud korra peamine eesmärk on vastuvõtvat asutust mitte kaasata, kahtleb Euroopa Andmekaitsekoostöö nõukogu, kas eelnimetatud lisamenetlus õigustaks artikli 82 kasutamist õigusakti ainsa õigusliku alusena.

Seega on Euroopa Andmekaitsekoostöö nõukogu seisukohal, et artikli 82 kasutamiseks õigusliku alusena peavad koostöö peamised menetlusetapid toimuma kahe õigusasutuse vahel ja et kõnealuse koostöö korral tuleks kasutada muud õiguslikku alust.

## **2. Elektroonilisi tõendeid käsitlevate õigusaktide vajalikkus võrreldes vastastikuse õigusabi lepingute ja Euroopa uurimismäärusega**

Euroopa Andmekaitsekoostöö nõukogu märgib, et komisjon on võtnud kohustuse analüüsida kriminaaluurimist takistavaid tõkkeid, eelkõige seoses juurdepääsuga elektroonilistele tõenditele. Oma seletuskirjas annab komisjon ülevaate ettepaneku kontekstist ja rõhutab elektrooniliste tõendite volatiilsust, nende rahvusvahelist mõõdet ning vajadust kohandada koostöömehhanism digitaalajastuga. Ettepanekuid määruse ja direktiivi kohta, milles käsitletakse elektrooniliste tõendite edastamist ja neile juurdepääsemist, ei tehtud selleks, et asendada varasemad kriminaalasjades tehtavat õigusalast koostööd käsitlevad dokumendid, nagu Budapesti konventsioon, vastastikuse õigusabi leping ja Euroopa uurimismäärus (Euroopa uurimismääruse direktiiv). Komisjoni sõnul on elektroonilisi tõendeid käsitlevate ettepanekute eesmärk parandada ametiasutuste ja teenuseosutajate vahel kriminaalasjades tehtavat õigusalast koostööd nii Euroopa Liidus kui ka kolmandate riikidega, eelkõige Ameerika Ühendriikidega.

Kuna need uued lisavahendid on ette nähtud konkreetselt elektroonilistele tõenditele juurdepääsemiseks ja nende edastamiseks, hindab Euroopa Andmekaitsekoostöö nõukogu nende õigusaktide lisaväärtust võrreldes Euroopa uurimismääruse direktiivi ja vastastikuse õigusabi lepinguga.

### **a) Elektroonilisi tõendeid käsitlevate õigusaktide vajalikkus, arvestades Euroopa uurimismääruses ja vastastikuse õigusabi lepingutes pakutavaid kaitsemeetmeid**

Peamine argument, mille komisjon elektroonilisi tõendeid käsitlevate ettepanekute toetuseks esitab, on selliste elektrooniliste tõendite tagamise ja kogumise kiirendamine, mida teises riigis asuvad teenuseosutajad talletavad ja/või mis on seal nende valduses.

Euroopa Andmekaitsekoostöö nõukogu peab aga kahetsusväärseks, et vajadust uue õigusakti järele, millega korraldada juurdepääsu elektroonilistele tõenditele, mõjuhinnangus ei tõendatud. Ettepanekutes ei tõendata, et elektroonilisi tõendeid käsitleva ettepaneku eesmärgi saavutamiseks poleks olnud võimalik kasutada muid, vähem sekkuvaid vahendeid, kuigi kaaluda oleks võinud alternatiivseid lahendusi. Näiteks oleks võinud uurida võimalust muuta ja täiustada Euroopa uurimismääruse direktiivi. See oleks olnud kooskõlas ka Euroopa uurimismääruse direktiivis esitatud konkreetse nõudega hinnata 21. maiks 2019 vajadust teksti muuta<sup>3</sup>. Teine võimalus oleks võinud olla näha ette andmesäilitamismääruste kasutamine, et külmutada andmed seniks, kuni esitatakse vastastikuse

---

<sup>3</sup> Vt Euroopa uurimismääruse direktiivi artikkel 37.

õigusabi lepingul põhinev ametlik taotlus. Need variandid oleks võimaldanud säilitada neis dokumentides sätestatud kaitsemeetmed, tagades samal ajal, et taotletud isikuandmeid ei kustutata.

Euroopa Andmekaitsekoostöö nõukogu märgib, et Euroopa uurimismääruse direktiivis kehtestatud tähtajad on pikemad kui need, mis on esitatud elektroonilisi tõendeid käsitlevas ettepanekus. Määrust täitev asutus või ametiisik peab tegema Euroopa uurimismääruse tunnustamise otsuse 30 päeva jooksul<sup>4</sup> ning ta peaks määruse seejärel täitma 90 päeva jooksul<sup>5</sup>. Euroopa Andmekaitsekoostöö nõukogu leiab, et Euroopa uurimismääruse kohase 30-päevase järelemõtlemisaja võimaldamine täitvatele asutustele või ametiisikutele on oluline kaitsemeetme, mis võimaldab neil hinnata, kas täitmistaotlus on põhjendatud ning vastab kõigile Euroopa uurimismääruse koostamise ja edastamise tingimustele<sup>6</sup>.

Euroopa Andmekaitsekoostöö nõukogu tunneb muret, et elektroonilisi tõendeid käsitlevates ettepanekutes esitatud kümnepäevane tähtaeg, mis ei jäta Euroopa andmeesitamismääruse tunnustuse täitmiseks aega järelemõtlemiseks, takistab nõuetekohast hindamist, kas Euroopa andmeesitamismääruse tunnustus vastab kõigile tingimustele ja on nõuetekohaselt koostatud.

Seetõttu soovib Euroopa Andmekaitsekoostöö nõukogu anda Euroopa andmeesitamismääruse tunnustuse saajale rohkem aega otsustamiseks, kas määrus tuleks täita või mitte.

Euroopa Andmekaitsekoostöö nõukogu märgib, et Euroopa andmesäilitamismääruse tunnustuse puhul ei ole tagatise, et andmete säilitamine piirdub sellega, mis on vajalik nende esitamiseks. Andmeid võidakse säilitada üle 60 päeva, sest taotlevale asutusele pole kehtestatud tähtaega adressaadi teavitamiseks andmeesitamismääruse tegemisest loobumisest või selle tagasivõtmisest. Seega soovib Euroopa Andmekaitsekoostöö nõukogu kehtestada taotlevale asutusele vähemalt tähtaja määruse tegemisest loobumiseks või selle tagasivõtmiseks, et järgida isikuandmete kaitse üldmääruse kohast võimalikult vähete andmete kogumise põhimõtet<sup>7</sup>.

Samuti märgib Euroopa Andmekaitsekoostöö nõukogu, et Euroopa uurimismääruse direktiivis on sätestatud tõendite tagastamine taotlevalt riigilt määrust täitvale asutusele või ametiisikule<sup>8</sup>. Ettepanekus elektroonilisi tõendeid käsitleva määruse kohta sellist võimalust aga ei mainita. Selgusetuks jääb, mis juhtub elektrooniliste tõenditega pärast nende edastamist taotlevale asutusele.

Seega soovib Euroopa Andmekaitsekoostöö nõukogu esitada määruse ettepanekus rohkem teavet elektrooniliste tõendite kasutamise kohta pärast nende edastamist taotlevale asutusele, et järgida isikuandmete kaitse üldmäärust ja läbipaistvuse põhimõtet<sup>9</sup> ning vastastikuse õigusabi lepingutes kehtestatud sihtotstarbelisuse põhimõtet.

## **b) Topeltkaristatavuse põhimõttest loobumine**

Euroopa Andmekaitsekoostöö nõukogu tunnustab, et vastastikune tunnustamine sõltub topeltkaristatavuse kohaldamisest, mis on liikmesriikide jaoks moodus oma suveräänsuse säilitamiseks. Aina enam leitakse aga, et topeltkaristatavus takistab sujuvat õiguslast koostööd. ELi liikmesriigid on aina enam valmis koostööd tegema isegi siis, kui uurimistoimingud on seotud tegudega, mida ei käsitata nende riigisiseses õiguses süütegudena. Euroopa Andmekaitsekoostöö nõukogu tuletab aga meelde, et topeltkaristatavuse põhimõtte eesmärk on pakkuda täiendavat kaitsemeetmet tagamaks, et riik ei saa

---

<sup>4</sup> Euroopa uurimismääruse artikli 12 lõige 3.

<sup>5</sup> Euroopa uurimismääruse artikli 12 lõige 4.

<sup>6</sup> Euroopa uurimismääruse artikkel 6.

<sup>7</sup> Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt c.

<sup>8</sup> Euroopa uurimismääruse artikli 13 lõiked 3 ja 4.

<sup>9</sup> Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt a.

tugineda teise riigi abile, et kohaldada kriminaalkaristust, mida teise riigi õiguses ei eksisteeri. See takistaks näiteks riiki nõudmast muult riigilt abi kellegi vangistamiseks tema poliitiliste veendumuste eest, kui need veendumused pole taotluse saanud riigis kriminaalkorras karistatavad, või kellelegi süüdistuse esitamiseks abordi tegemise eest, kui see isik elab teises riigis, kus see pole ebaseaduslik. Topeltkaristatavuse põhimõttega kaasnevad sageli täiendavad piirangud või kaitsemeetmed seoses karistustega, kui need erinevad taotluse esitanud riigis ja täitjariigis liiga palju. Peamine näide sellest on teatavates vastastikuse õigusabi lepingutes sisalduv kohustus surmanuhtlust mitte kohaldada, kui seda kahest lepinguosalisest ühe õiguses ei eksisteeri.

Euroopa Andmekaitsekoostöögrupi märgib, et topeltkaristatavuse põhimõtte on ettepanekus elektroonilisi tõendeid käsitleva määruse kohta välistatud. See aga ei tähenda üksnes tavapärase vastastikuse tunnustamisega seotud formaalsuste, vaid ka topeltkaristatavuse põhimõttega seotud kaitsemeetmete kadumist.

Euroopa Andmekaitsekoostöögrupi märgib, et osutatud pole selle riigi õigusele, kus taotluse saanud teenuseosutaja asub, ning et mis tahes andmete säilitamise ja ka abonendi- või juurdepääsuandmete esitamise määruse võib teha mis tahes kuriteo puhul,<sup>10</sup> olenemata sellest, kas teistes liikmesriikides on kindlaks määratud sarnased kuriteod või mitte.

Andmeesitamismäärusi võib teha ja täita aga ainult juhul, kui taotlevas riigis on võrreldavas riigisiseses olukorras sama kuriteo korral võimalik kasutada sarnast meetet<sup>11</sup>. Nagu komisjon on selgitanud määruse ettepaneku seletuskirjas, tunnistatakse tehingu- ja sisuandmete eripära, sest neid peetakse tundlikumateks. Tehingu- ja sisuandmeid puudutavad määrused põhinevad vähemalt kolmeaastasel vabadusekaotuse maksimumkunnisel, et tagada proportsionaalsus ning mõjutatud isikute õiguste austamine<sup>12</sup>. Euroopa Andmekaitsekoostöögrupi rõhutab aga, et ELis pole veel ühtlustatud kuritegusid, mis on karistatavad vabadusekaotusega, mille maksimaalne pikkus on vähemalt kolm aastat.

Euroopa Andmekaitsekoostöögrupi on vastu sellele, et loobutakse topeltkaristatavuse põhimõttest, mille eesmärk on tagada, et riik ei saa tugineda teiste riikide abile, et väljaspool tema territooriumi kohaldaks tema riigisisest kriminaalõigust riik, kes ei rakenda samasugust lähenemisviisi, eriti kui arvestada muude traditsiooniliste ja oluliste kaitsemeetmete kadumist kriminaalõiguse valdkonnas (vt punkt 3 asukohakriteeriumide kohta ja punkti 7 alapunkt g võimaliku vastuolu kohta kolmandate riikide õigusega).

### **c) Otse ettevõtete poole pöördumise tagajärg**

Euroopa Andmekaitsekoostöögrupi tunnistab, et elektroonilised tõendid on erataristus aina enam kättesaadavad ning need võivad asuda väljaspool uurivat riiki ja kuuluda teenuseosutajatele.

Euroopa Andmekaitsekoostöögrupi märgib, et pärast Yahoo<sup>13</sup> ja Skype<sup>14</sup> kohtuotsuseid Belgias ning terrorirünnakute kontekstis on vaja sujuvamat ja kiiremat koostööd avaliku ja erasektori üksuste vahel. Mõjuhinnaangus viitab komisjon kolmele menetlusvahendile, mis hõlmavad nii avaliku sektori asutusi kui ka teenuseosutajaid. Need on õiguslane koostöö, otsene koostöö ja otsene juurdepääs. Kui esimese puhul neist ei kannu Euroopa uurimismääruse täitmise vastutust teenuseosutaja, vaid

<sup>10</sup> Kavandatava elektroonilisi tõendeid käsitleva määruse artikli 5 lõige 3 ja artikli 6 lõige 2.

<sup>11</sup> Kavandatava elektroonilisi tõendeid käsitleva määruse artikli 5 lõige 2.

<sup>12</sup> Kavandatava elektroonilisi tõendeid käsitleva määruse artikli 5 lõike 4 punkt a.

<sup>13</sup> Hof van Cassatie (Belgia kassatsioonikohus), YAHOO! Inc., nr P.13.2082.N, 1. detsember 2015.

<sup>14</sup> Correctionele Rechtbank van Antwerpen, afdeling Mechelen (Antwerpeni kriminaalkohus, Mecheleni osakond), nr ME20.F1.105151-12, 27. oktoober 2016 (Skype on otsuse edasi kaevanud).

määrust täitev asutus või ametiisik<sup>15</sup>, siis teine, otsene koostöö, põhineb teenuseosutaja koostööl. Teenuseosutaja seisukohast on kõige sekkuvam otsene juurdepääs, sest avaliku sektori asutustel on võimalik saada juurdepääs andmetele ilma vahendaja abita.

Seega kardab Euroopa Andmekaitsekoostöö, et kui teenuseosutajate poole pööratakse otse, ei taga nad isikuandmete kaitset sama tõhusalt, kui avaliku sektori asutused on võimelised ja kohustatud seda tegema, ning rõhutab, et seetõttu ei kohaldu ka teatavad menetluslikud tagatised, mis on õigusalase koostöö kontekstis isikutele ja ettevõtetele ette nähtud<sup>16</sup>. Näiteks peaks taotluse saanud teenuseosutaja pöörduma määruse vaidlustamiseks muu (liikmes)riigi kohtusse, samas kui õigusalase koostöö kontekstis pöörduks ta oma riigi ametiasutuste poole. Euroopa Andmekaitsekoostöö soovib lisada määruse ettepanekusse täiendavad alused, millega tagatakse, et teenuseosutajad kaitsevad üksikisikute põhiõigusi, nagu õigust isikuandmete kaitsele ning era- ja perekonnaelu austamisele, ning et teavitatakse pädevat andmekaitseasutust, et tagada kontrolli võimalikkus.

### 3. Uus õiguskaitsepädevuse alus ja asukohakriteeriumi nii-öelda kadumine

Euroopa Andmekaitsekoostöö märgib, et komisjon rõhutab, et üks suuremaid muutusi, mis nende ettepanekutega kaasneb, on asukohakriteeriumide kadumine ning pädevate asutuste võimalus taotleda andmete säilitamist ja esitamist olenemata sellest, kus neid andmeid tegelikult säilitatakse.

Andmekaitse seisukohast pole uudne, et ELi andmekaitsealased õigusaktid on kohaldatavad olenemata sellest, kus asjaomaste isikute andmeid säilitatakse. Isikuandmete kaitse üldmäärust kohaldatakse, kui vastutav töötleja või volitatud töötleja asub ELis või kui töödeldakse ELi andmesubjektide andmeid, isegi kui vastutav töötleja või volitatud töötleja ei asu ELi territooriumil;<sup>17</sup> viimasel juhul peavad nad määrama oma esindaja ELis<sup>18</sup>. Andmekaitse seisukohast on oluline märkida, et laiendatud territoriaalse kohaldamisala eesmärk on täielikuma kaitse tagamine ELi andmesubjektidele, olenemata sellest, kus nende andmeid töötlev ettevõtte asub.

Seega, kuigi asukohakriteeriumide kadumine võib olla kriminaalõiguse valdkonnas uudne, ei kujuta see endast andmekaitse seisukohast suurt muutust. Samuti märgib Euroopa Andmekaitsekoostöö, et seos ELi territooriumiga säilib, sest üksnes teenuseosutajad, kes pakuvad teenuseid liidus, kuuluvad ettepanekute kohaldamisalasse, ning asjaolu, et taotlusi saab esitada üksnes kriminaaluurimiste kontekstis, osutab seosele ELiga (kuna kuritegu pandi toime liikmesriigi territooriumil või kuna kannatanu või kurjategija oli liikmesriigi kodanik).

Kui kriminaalõiguses kaotatakse nüüd asukohakriteeriumid, on Euroopa Andmekaitsekoostöö jaoks kõige olulisem küsimus see, kuidas tagada, et selline muutus ei kahjustaks andmekaitse ning andmesubjektide ja taotluse saanud teenuseosutajate kriminaalmenetlusõigusi. Siinkohal tunnistab Euroopa Andmekaitsekoostöö, et ELis on menetluslikud tagatised vähemalt osaliselt ühtlustatud ning need tuleb Euroopa inimõiguste konventsiooni alusel ette näha. Seega võib väita, et asukohakriteeriumide kadumise mõju oleks tõenäoliselt piiratum juhul, kui tõendeid taotletakse ELis,

---

<sup>15</sup> Artiklid 10–16.

<sup>16</sup> Vt rahvusvahelise andmekaitse seisukohast ka „Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes“, rahvusvahelise andmekaitse ja side töörühm, 63. kohtumine, 9.–10. aprill 2018, Budapest (Ungari).

<sup>17</sup> Vt artikkel 3, eelkõige lõige 2.

<sup>18</sup> Vt artikkel 27.



võrreldes vastupidise olukorraga, kus kolmandate riikide ametiasutused taotlevad andmeid ELis asuvate ettevõtete kohta samadel tingimustel, mis on sätestatud elektroonilisi tõendeid käsitleva määruse eelnõus. Euroopa Andmekaitsekoostöögruppi tunneb eelkõige muret sellepärast, et see võib kaasa tuua rohkem probleemseid olukordi. Ametiasutustel kolmandas riigis, kus kohaldatakse kriminaalõiguse valdkonnas teistsuguseid ja võimalik et vähem menetluslikke tagatisi, võib seega olla juurdepääs andmetele, mida kaitstaks ELis täiendavate kaitsemeetmetega. Selles suhtes väljendab Euroopa Andmekaitsekoostöögrupp veel kord muret kaksikmoraali ja põhiõiguste nõrgenemise pärast, kui kolmanda riigi ametiasutuse esitatud taotluse korral ei kohaldata teenuseosutajate ja andmesubjektide suhtes liidu õiguses sätestatud menetluslikke tagatisi.

Kuna selle uue õiguskaitsepädevuse alusega, mis ei olene andmete asukohast, kaasneb menetlus, mis põhineb peamiselt pädevate asutuste otsetaotlustel teenuseosutajatele, tunneb Euroopa Andmekaitsekoostöögrupp muret, et taotluste saajatest eraettevõtted, kes pole seotud sellise õigusliku vahendiga nagu vastastikuse õigusabi leping, millega tavaliselt reguleeritakse õigusasutuste vahelist andmevahetust ja milles on sätestatud kaitsemeetmed, ei pruugi kohaldada andmekaitsealaseid kaitsemeetmeid. Vastastikuse õigusabi lepingute kontekstis kaasnevad minimaalsete andmekaitsealaste kaitsemeetmetega näiteks konfidentsiaalsuskohustused ja sihtotstarbelisuse põhimõte, mis tähendab seda, et andmeid ei töödelda muul eesmärgil.

Seega tuleb Euroopa Andmekaitsekoostöögruppi meelde, et kohaldada tuleks vähemalt direktiivis 2016/680 sätestatud kaitsemeetmeid, sealhulgas seoses andmete edastamisega, ning eelkõige artiklit 39, juhul kui teenuseosutaja asub kolmandas riigis ja selles valdkonnas puudub kaitse piisavuse otsus. Eelkõige rõhutab Euroopa Andmekaitsekoostöögrupp, et selles artiklis on osutatud eeskätt taotleva asutuse liikmesriigis asuva pädeva andmekaitseasutuse teavitamisele määrus(t)est ning andmete edastamise dokumenteerimisele, ka seoses põhjendusega, miks edastamine kolmanda riigi pädevale asutusele pole tõhus või asjakohane.

#### **4. „Teenuseosutaja“ mõistet tuleks piirata või täiendada seda andmesubjektide õiguste kaitsmise meetmetega**

Seoses teenuseosutajatega kiidab Euroopa Andmekaitsekoostöögrupp heaks laia määratluse, mis võib hõlmata nii sideteenuseid kui ka OTT-teenuseid, sest kõik need teenused on funktsionaalselt võrdväärsed ning seega võib kavandatud meetmetel olla sarnane mõju eraelu puutumatusle õigusele ja teabevahetuse konfidentsiaalsuse õigusele, nagu rõhutatud artikli 29 tööühma avalduses ja varem arvamuses 01/2017 kavandatud e-privatsuse määruse kohta. Elektroonilisi tõendeid käsitleva määruse ettepanek hõlmab teenuseosutajaid, kes osutavad elektroonilise side teenuseid, mis on määratletud Euroopa Parlamendi ja nõukogu direktiivi (millega kehtestatakse Euroopa elektroonilise side seadustik) artikli 2 lõikes 4, infoühiskonna teenuseid, mis on määratletud direktiivi (EL) 2015/1535 artikli 1 lõike 1 punktis b ja „mille puhul andmete säilitamine on kasutajale osutatava teenuse olemuslik komponent, sealhulgas sotsiaalvõrgustikud, internetipõhised kauplemiskohad, mis lihtsustavad kasutajatevahelisi tehinguid, ja muud veebimajutusteenus pakkujad“, ning interneti domeeninime ja IP-numbriteenusid, „nagu IP-aadressi pakkujad, domeeninimede registrid, domeeninimede registraatorid ning seotud privatsus- ja vaheserveri teenused“<sup>19</sup>.

---

<sup>19</sup> Kavandatava elektroonilisi tõendeid käsitleva määruse artikli 2 lõike 3 punkt c.

Kuna aga teenuseosutaja on määruse eelnõu tähenduses „füüsiline või juriidiline isik, kes osutab ühe või mitme järgmise kategooria teenuseid“, tunneb Euroopa Andmekaitsekoostöögrupi muret selle üle, et see õigusakt võib hõlmata nii vastutavaid töötajaid kui ka volitatud töötajaid isikuandmete kaitse üldmääruse tähenduses. „Teenuste pakkumine“, nagu see on määratletud määruse eelnõu artikli 2 lõikes 4, hõlmab ühe või mitme liikmesriigi füüsilistele või juriidilistele isikutele võimaluse andmist kasutada loetletud teenuseid ning sisulist seost asjaomase liikmesriigiga (liikmesriikidega); need tegevused hõlmavad tegevusi, mida volitatud töötaja sooritab vastutava töötaja jaoks, näiteks andmete säilitamist.

Seega kardab Euroopa Andmekaitsekoostöögrupp, et ilma piirangute kehtestamiseta teenuseosutajatele, kes tegutsevad vastutavate töötajate isikuandmete kaitse üldmääruse tähenduses, ning ilma volitatud töötaja konkreetse kohustusega vastutavat töötajat andmesaamis- või andmesaailitamismääruse saamise korral teavitada, võidakse andmesubjektide õigusi eirata. See on nii eelkõige seetõttu, et võimalike vastuoluliste kohustuste korral, mis ei võimalda adressaadil saadud määrusi täita, kutsutakse õigusasutusi määruse eelnõus üles pöörduma kõige asjakohasema osalise poole, olenemata kohaldatavatest andmekaitsestandarditest, eriti kuna taotleja võidakse igasugust teavet, mitte üksnes isikuandmete kaitse üldmääruse kohaldamisalasse kuuluvaid isikuandmeid<sup>20</sup>.

Isikuandmete kaitse üldmääruses on sätestatud, et volitatud töötaja tegutseb üksnes vastutava töötaja juhiste alusel. Seega on vastutava töötaja ülesanne tagada, et andmesubjektide õigusi austatakse, ning anda neile asjakohast teavet, ka nende andmete vastuvõtjate kohta, näiteks andmetega tutvumise õiguse kasutamise kontekstis. Volitatud töötaja ei saa neid taotlusi andmesubjektidelt ja tal ei ole õigust neile vastata, välja arvatud juhul, kui vastutav töötaja seda sõnaselgelt teha palub.

Euroopa Andmekaitsekoostöögrupp rõhutab, et välja arvatud juhul, kui andmesubjektide õigusi on isikuandmete kaitse üldmääruse kohaldamisel piiratud, ei pruugi andmesubjektid, kelle suhtes isikuandmete kaitse üldmäärust kohaldatakse, saada oma õigusi tõhusalt kasutada, kui vastutaval töötajal pole võimalik esitada täielikku teavet. Samuti märgib Euroopa Andmekaitsekoostöögrupp, et teabe esitamata jätmise tõenäosus on veel suurem, kui volitatud töötajale pole kehtestatud konkreetset kohustust vastutavat töötajat teavitada, kui taotleatakse andmeid andmesubjektide kohta, kellel pole õigust saada isikuandmete kaitse üldmäärusest tulenevat kaitset. Andmeid taotlenud õigusasutustel pole sel juhul tingimata kohustust teavitada andmesubjekte täiendavast töötlemisest, mida nad teevad. Seega kutsub Euroopa Andmekaitsekoostöögrupp üles kitsendama kohaldamisala vastutavatele töötajatele isikuandmete kaitse üldmääruse tähenduses või lisama sätte, milles selgitatakse, et kui teenuseosutaja, kelle poole pöörduti, pole vastutav töötaja, peab ta vastutavat töötajat teavitama.

## **5. Mõisteid „tegevuskoht“ ja „esindaja“ tuleks nende ettepanekute kontekstis selgelt eristada nendest mõistetest isikuandmete kaitse üldmääruse kontekstis.**

Arvestades, et andmete suhtes asukohakriteeriumid ei kohaldu, piirdatakse kavandatud määruse kohaldamisalasse kuuluvate andmesaamis- ja andmesaailitamismääruste adressaatide puhul teenuseosutajatega, kes asuvad ELis või mujal ning kes pakuvad teenuseid liidus ja kellel on kohustus

---

<sup>20</sup> Vt artikli 7 lõiked 3 ja 4.

määrata esindaja kooskõlas direktiivi eelnõus esitatud nõuetega. „Tegevuskoha“ ja „esindaja“ mõisted on seega õigusaktide eelnõudes määratletud.

Euroopa Andmekaitsekoostöögruppi märgib, et need mõisted esinevad ka muude ELi õigusaktide kontekstis, eelkõige isikuandmete kaitse üldmääruses. Seetõttu tuleks täpsustada nende mõistete määratlust ja piiritlemist ettepanekute eelnõude kontekstis ja isikuandmete kaitse üldmääruse kontekstis.

### **a) Tegevuskoht**

Euroopa Andmekaitsekoostöögruppi tuleb ühtlasi meelde, et „tegevuskoha“ mõistet määruse eelnõu kontekstis ei tohi segi ajada sama mõistega isikuandmete kaitse üldmääruse kontekstis. Määruse eelnõu tähenduses on artikli 2 lõikes 5 määratletud „tegevuskoha“ mõiste laiem kui isikuandmete kaitse üldmääruses, sest see on „tegelik majandustegevusega tegelemine määramata aja jooksul stabiilse taristu kaudu, kust osutatakse teenuseid, või stabiilne taristu, kust juhitakse majandustegevust“, olenemata sellest, kas selle tegevuskoha tegevuse raames töödeldakse isikuandmeid. Seega kui määruse eelnõus määratletud „tegevuskoht“ hõlmaks igal juhul „tegevuskohta“ isikuandmete kaitse üldmääruse tähenduses, ei pruugi vastupidine kehtida.

Seetõttu hoiatab Euroopa Andmekaitsekoostöögruppi, et teenuseosutajate tegevuskohad määruse eelnõu tähenduses ei pruugi tingimata viidata sellele, et täidetakse artikli 3 lõike 1 kohaseid isikuandmete kaitse üldmääruse kohaldamise tingimusi. Sellega seoses kutsutakse vastutavaid töötajaid ja volitatud töötajaid üles kontrollima, kas isikuandmete kaitse üldmäärust ei saa kohaldada artikli 3 lõike 2 alusel, mis eeldab esindaja määramist ELis ja ühtse kontaktpunkti mehhanismi puudumist.

### **b) Esindaja**

Artikli 29 tööühm rõhutas oma avalduses, et vältida tuleks isikuandmete kaitse üldmääruse artikli 27 kohase esindaja määramise kohustuse ja elektroonilisi tõendeid käsitleva määruse eelnõu kohase esindaja määramise kohustuse segiajamist.

Euroopa Andmekaitsekoostöögruppi soovib seoses käesoleva ettepaneku eelnõuga neid soovitusi meenutada ning eelkõige rõhutada, et tema arusaama kohaselt tuleb elektroonilisi tõendeid käsitlevate ettepanekute kontekstis igal juhul määrata esindaja direktiivi eelnõu (milles käsitletakse esindaja määramist) tähenduses, tal peavad olema konkreetsed funktsioonid lisaks teenuseosutaja antud volitustele, tal peab olema õigus vastata taotlustele ja tegutseda teenuseosutaja nimel ning suurem vastutus kui isikuandmete kaitse üldmääruse kohasel esindajal.

Samuti rõhutab Euroopa Andmekaitsekoostöögruppi, et kohustus määrata elektroonilisi tõendeid käsitlevate ettepanekute eelnõude kohaselt igal juhul esindaja, olenemata sellest, kas teenuseosutaja asub ELis või mitte, elektroonilisi tõendeid käsitleva direktiivi eelnõu kohane võimalus määrata samale teenuseosutajale isegi mitu esindajat ning kohustus teavitada liikmesriikide ametiasutusi esindaja määramisest erinevad isikuandmete kaitse üldmäärusest, milles pole sätestatud sellist kohustust teatada määratud esindajast, tema määramise suhtes kohaldatavaid erandeid ega esindaja piiratud vastutust.

Arvestades olulisi erinevusi ühel juhul teenuseosutaja ja teisel juhul vastutava töötaja või volitatud töötaja rollis, vastutuses ja suhetes muude tegevuskohtadega, soovib Euroopa Andmekaitsekoostöögruppi juhul, kui teenuseosutaja ei asu ELis, aga kui tema suhtes kohaldatakse isikuandmete kaitse üldmäärust vastavalt artikli 3 lõikele 2 ja elektroonilisi tõendeid käsitlevat

määrust, määrata kaks eraldiseisvat esindajat, kellel on selged ja eristatavad funktsioonid vastavalt õigusaktidele, mille põhjal nad on määratud.

## 6. Uued andmekategooriad

Kavandatava määruse artiklis 2 on määratletud eri andmekategooriad: abonendiandmed, juurdepääsuandmed, tehinguandmed ja sisuandmed. Komisjoni ettepaneku põhjenduses 20 on täpsustatud, et „[k]äesoleva määruse andmekategooriad hõlmavad abonendiandmeid, juurdepääsuandmeid, tehinguandmeid (neid kolme kategooriat nimetatakse „muudeks kui sisuandmeteks“) ja sisuandmeid. Selline eristus (v.a juurdepääsuandmed) on olemas paljude liikmesriikide õigusaktides ja ka Ameerika Ühendriikide kehtivas õigusraamistikus, mis lubab teenuse osutajatel esitada vabatahtlikult muid kui sisuandmeid välisriigi õiguskaitseasutustele“.

Sellega seoses rõhutab Euroopa Andmekaitsekoostöögrupp, et olenemata sellest, kas andmesubjektile viidatakse kavandatavas määruses kui „abonendile“ või „kasutajale“, tuleks kõiki nelja eespool nimetatud andmekategooriat käsitada vastavalt ELi andmekaitsealastele õigusaktidele isikuandmetena, sest need sisaldavad teavet, mis on seotud tuvastatud või tuvastatava füüsilise isikuga. Samamoodi tuleb märkida, et komisjoni ettepaneku artikli 2 punktis 6 määratletud elektroonilised tõendid hõlmavad kõiki nelja andmekategooriat ja on seega seotud isikuandmetega. Selle asemel et kehtestada tõenditele juurdepääsemist käsitlevad õigusnormid, mis on kindlaks määratud ja mida on täpsustatud kooskõlas riigisisese õiguse ja kohtumenetlustega, on kavandatud määruses sätestatud uued sisulised ja menetluslikud tingimused seoses juurdepääsuga isikuandmetele.

Kavandatud määruses on kehtestatud uued isikuandmete alamkategooriad, mille suhtes kohaldatakse erinevaid menetluslikke juurdepääsutingimusi, aga Euroopa Andmekaitsekoostöögrupp meenutab, et Euroopa Liidu Kohtu asjakohase praktika kohaselt pole eraelu puutumatuse põhiõiguse riive tuvastamisel oluline, kas asjaomane eraeluga seotud teave on delikaatne või mitte või kas asjaomased isikud on selle riive tõttu pidanud taluma mingeid ebamugavusi.

Samuti meenutab Euroopa Andmekaitsekoostöögrupp, et seoses muude kui sisuandmetega, mis hõlmavad komisjoni ettepaneku kohaselt abonendiandmeid, juurdepääsuandmeid ja tehinguandmeid, on Euroopa Liidu Kohus teinud liidetud kohtuasjades C-203/15 ja C-698/15 Tele2 Sverige AB otsuse, mille kohaselt võimaldavad metaandmed nagu liiklusandmed ja asukohaandmed koostada asjaomaste isikute profiili, mis on õigust eraelu puutumatusele arvestades sama tundlik teave kui sideseansi sisu ise<sup>21</sup>.

Seetõttu kordab Euroopa Andmekaitsekoostöögrupp juba artikli 29 tööühma 29. novembri 2017. aasta avalduses (mis käsitleb andmekaitse ja eraelu puutumatuse aspekte elektroonilistele tõenditele piiriülese juurdepääsu puhul) väljendatud kahtlusi ja muret seoses „muude kui sisuandmete“ ja sisuandmete piiritlusega ning nelja isikuandmete kategooriaga, mis on esitatud kavandatud määruses. Need neli esitatud kategooriat ei tundu olevat selgelt piiritletud ja juurdepääsuandmete määratlus jääb võrreldes teiste kategooriatega ebamääraseks. Euroopa Andmekaitsekoostöögrupp peab seega kahetsusväärseks, et komisjoni mõjuhinnaangus ega ettepanekus ei põhjendatud rohkem nende uute isikuandmete alamkategooriate loomist, ning väljendab oma muret seoses tagatiste eri tasemetega, mis puudutavad isikuandmete kategooriatele juurdepääsemise sisulisi ja menetluslikke

---

<sup>21</sup> Kohtuotsus, Euroopa Liidu Kohus, 21. detsember 2016, punkt 99.

tingimusi, eriti arvestades seda, et praktikas on mõnel juhul keeruline hinnata, millisesse andmekategooriasse taotletavad andmed kuuluvad. Näiteks IP-aadressid võiks liigitada nii tehinguandmeteks kui ka abonendiandmeteks.

Sellega seoses tuleb Euroopa Andmekaitsekoostöögrupi meelde, et eraelu austamist ja isikuandmete kaitset elektroonilise side puhul (e-privatsus) käsitleva määruse ettepaneku põhjenduses 14 leiab komisjon, et „[e]lektronilise side andmete mõiste tuleks määratleda piisavalt laial ja tehnoloogianeutraalsel viisil, et see hõlmaks mis tahes teavet edastatud või vahetatud sisu kohta (elektronilise side sisu) ning teavet elektroonilise side teenuste lõppkasutaja kohta, mida on töödeldud elektroonilise side sisu edastamise, levitamise või vahetamise võimaldamiseks, sealhulgas andmed side lähte- ja sihtkoha jälitamiseks ja kindlaks tegemiseks, geograafiline asukoht ning side kuupäev, kellaaeg, kestus ja liik“. Kuna praegust ja tulevast e-privatsuse raamistikku ning sellega seotud eraelu puutumatus piiranguid kohaldatakse õigusnormide suhtes, millega reguleeritakse õiguskaitseasutuste juurdepääsu elektroonilistele tõenditele, soovib Euroopa Andmekaitsekoostöögrupp lisada kavandatud määruksesse laiema elektroonilise side andmete määratluse, tagamaks, et asjakohaseid kaitsemeetmeid ja juurdepääsutingimusi, mis kehtestatakse, kohaldatakse ühetaoliselt nii „muude kui sisuandmete“ kui ka sisuandmete suhtes.

## 7. Euroopa andmesäilitamismääruse ja andmeesitamismäärusega seotud menetluste analüüs

Üldjoontes paistab andmeesitamise- või andmesäilitamismääruse esitamise menetlus olevat järgmine:

- pädev õigusasutus – taotlev asutus – teeb olenevalt taotletavate andmete liigist ja määruse liigist määruse kooskõlas artiklites 5 ja 6 loetletud (piiratud) tingimustega ning saadab selle ühtlustatud tunnistust kasutades teenuseosutaja esindajale või teenuseosutaja mis tahes tegevuskohta ELis ehk adressaadile;
- tunnistuse saamisel täidab adressaat määruse – st edastab andmed 10 päeva või erakorralisel juhul 6 tunni jooksul või säilitab neid kuni 60 päeva –, välja arvatud juhul, kui seda on võimatu teha, sest tunnistus on mittetäielik, vääraratu jõu tõttu või kui see on adressaadi jaoks *de facto* võimatu või kuna adressaat keeldub vastuoluliste kohustuste tõttu, mis tulenevad põhiõigustest või kolmanda riigi põhiõigustest või muudest põhjustest;
- kui adressaat pole saanud määrust täitnud, esitamata põhjendusi, mida taotlev asutus peab vastuvõetavaks, on ette nähtud menetlused, mille kohaselt pädev täitevasutus liikmesriigis, kus teenuseosutaja asub või on esindatud, tagab määruste täitmise, välja arvatud juhul, kui kohaldatavad on piiratud alused keeldumiseks ning täitevasutus esitab vastuväite määruse tunnustamise või täitmise tagamise suhtes;
- kui adressaat esitab määruse suhtes põhjendatud vastuväite, mis põhineb vastuolulistel kohustustel, suunab taotlev asutus asja oma liikmesriigi pädevasse kohtusse, mis vastutab seejärel võimaliku vastuolu hindamise eest ja määruse jõusse jätmise eest vastuolu puudumise korral. Kui esineb vastuolu, mis tuleneb põhiõigustest või kolmanda riigi põhiõigustest, pöördub pädev kohus oma riigi keskasutuste kaudu kolmanda riigi keskasutuste poole, andes vastamiseks 15-päevase tähtaja, mida võidakse põhjendatud taotluse korral pikendada 30 päeva võrra, või kui adressaat on tuginenud muudele keeldumispõhjustele, teeb see kohus ise kindlaks, kas jätta määrus jõusse või see tühistada;

- ilma et see piiraks isikuandmete kaitse üldmääruse ja direktiivi EL 2016/680 kohaselt kättesaadavate õiguskaitsevahendite kasutamist, on isikutel, kelle andmed saadi andmeesitamismääruse abil, õigus ka tõhusatele õiguskaitsevahenditele selle määruse vastu.

Euroopa Andmekaitsekoostöögrupp hindas määruse eelnõus ette nähtud menetlusi ja sätestatud kaitsemeetmeid seoses eri etappidega ning soovib seoses teatavate aspektidega allpool esitatud kaitsemeetmeid ja muudatusi.

## **a) Määruste tegemise künniseid tuleks tõsta ning määrusi peavad tegema või kinnitama kohtud**

Mis puudutab määruste tegemise tingimusi, siis kiidab Euroopa Andmekaitsekoostöögrupp heaks põhimõtte, mille järgi on kaitsemeetmed tehingu- või sisuandmete juurdepääsu korral rangemad. Samas märgib ta aga, et arvestades asjaolu, et kriminaalkaristused pole liikmesriikide vahel täielikult ühtlustatud, osutab viide kuritegudele, „mis on taotlevas riigis karistatavad vabadusekaotusega, mille maksimaalne pikkus on vähemalt kolm aastat“<sup>22</sup> siiski erinevatele künnistele ja muudele erinevustele andmesubjektide andmete kaitstes ELis.

Ühtlasi rõhutab Euroopa Andmekaitsekoostöögrupp, et eelkõige arvestades abonendiandmete laia määratlust, paistab esitatud künnis üsna madal selliste andmesäilitamismääruste ja andmeesitamismääruste puhul, mis puudutavad abonendi- või juurdepääsuandmeid, sest sisuliselt oleks nende määruste tegemine õigustatud kõigi kuritegude puhul. Samuti on sellistel asutustel, kellel on õigus määrusi teha, tehingu- või sisuandmeid puudutavate andmeesitamismääruste kontekstis rohkem piiranguid võrreldes nende asutustega, kellel on õigus teha andmesäilitamis- või andmeesitamismäärusi, millega nõutakse abonendi- või juurdepääsuandmete esitamist, sest prokurörid võivad teha või kinnitada üksnes viimati nimetatud määrusi, samas kui kohtunikud, kohtud või eeluurimiskohtunikud võivad teha või kinnitada kõiki määrusi.

Eelkõige peab Euroopa Andmekaitsekoostöögrupp kahetsusväärseks, et madalaim künnis, mis annab õiguskaitseasutustele võimaluse taotleda juurdepääsu abonendi- ja juurdepääsuandmetele mis tahes kuriteo puhul, põhineb Euroopa Liidu Kohtu praktika (milles keskendutakse muudele andmetele) ümberpööratud tõlgendamisel, et teha kindlaks, milliseid kaitsemeetmeid kohaldada. Euroopa Liidu Kohus rõhutas seoses liiklus- ja asukohaandmetega konkreetselt, et pädevate ametiasutuste juurdepääs peab piirduma üksnes raske kuritegevuse vastu võitlemisega<sup>23</sup>. Euroopa Andmekaitsekoostöögrupp saaks aru, kui ettepanekuga loodaks võimalus taotleda juurdepääsu väga elementaarsele teabele, mis võimaldaks üksnes isiku tuvastada, ilma et sideandmeid kohtu eelneva loata avaldataks. Andmekaitsekoostöögrupp taunib aga komisjoni laia ümberpööratud tõlgendust sellest otsusest ning kutsub üles kehtestama rangemad kaitsemeetmed, et piirata muudele abonendiandmetele ja juurdepääsuandmetele juurdepääsemise aluseid. Euroopa Andmekaitsekoostöögrupp soovib piirata juurdepääsu nendele andmetele määruse eelnõus esitatud kuritegude loeteluga või vähemalt „raskete kuritegudega“, eriti arvestades madalamat eelneva loa künnist, mis nende andmete suhtes kehtestatud on.

---

<sup>22</sup> Vt artikli 5 lõike 3 punkt a.

<sup>23</sup> Vt kohtuasi C-203/15, punkt 125.

Ühtlasi rõhutab Euroopa Andmekaitsekoogu, et selline ümberpööratud tõlgendus viib ka selleni, et ettepanekuga antakse prokuröridele võimalus teha määrusi või kinnitada nende tegemist. Euroopa Andmekaitsekoogu on seisukohal, et välja arvatud taotluste korral, mis puudutavad väga elementaarseid teavet, mis võimaldaks üksnes isiku tuvastada, ilma et avaldataks sideandmeid, kujutab see endast sammu tagasi võrreldes Euroopa Liidu Kohtu praktikaga, mis puudutab juurdepääsu sideandmetele. Oma kohtupraktikas, mis puudutab juurdepääsu sideandmetele õiguskaitse eesmärgil, on Euroopa Liidu Kohus piiranud võimalust sellist juurdepääsu anda, sätestades muude kriteeriumide hulgas, et „välja arvatud nõuetekohaselt põhjendatud kiireloomulistel juhtudel“<sup>24</sup> peab juurdepääs olema „allutatud kohtu või sõltumatu haldusasutuse teostatavale eelnevale kontrollile“ ja põhinema riigi pädevate asutuste põhjendatud taotlusel, mis on esitatud kuriteo ennetamise, avastamise või menetlemise raames.<sup>25</sup>

Euroopa Andmekaitsekoogu tuletab meelde, et mõiste „kohus“ on liidu õiguse autonoomne mõiste ja et Euroopa Liidu Kohus on järjepidevalt rõhutanud ja tuletanud meelde kriteeriume, sealhulgas sõltumatuse kriteeriume,<sup>26</sup> mis tuleb kohtuks kvalifitseerumiseks täita, mis ei paista prokuröride puhul täidetud olevat, nagu ka Euroopa Inimõiguste Kohus on oma kohtupraktikas<sup>27</sup> meenutanud.

Seetõttu kaasnevad artikli 4 lõike 1 punktidega a ja b ning lõike 3 punktidega a ja b menetlused, mille puhul kohaldatakse abonendi- ja juurdepääsuandmete suhtes oluliselt vähem kaitsemeetmeid, sest neid andmeid saab taotleda prokurör üksi, ilma et täiendavat kontrolli kohaldaks selle riigi ametiasutus, kus taotletud andmed asuvad või kus asub taotluse saanud ettevõtte esindaja, ning ilma sõltumatu haldusasutuse kontrollita.

Samuti võtab Euroopa Andmekaitsekoogu teadmiseks nii-öelda täiendava kaitsemeetme, mis on sätestatud artikli 5 lõikes 2, mille kohaselt saab andmeesitamismääruse teha üksnes juhul, kui võrreldavas riigisiseses olukorras on sama kuriteo korral võimalik kasutada sarnast meetet. Samas hoiatab Euroopa Andmekaitsekoogu selle sätte vastupidise mõju eest: selle asemel et pakkuda täiendavaid kaitsemeetmeid, tundub see innustavat liikmesriike laiendama oma riigisiseseid võimalusi taotleda abonendi- või juurdepääsuandmete esitamist, tagamaks, et võimalik on teha kõnealuse määruse kohaseid andmeesitamismäärusi.

## **b) Andmete esitamise tähtaegu tuleks põhjendada**

Euroopa Andmekaitsekoogu märgib, et Euroopa andmeesitamismäärustele tuleb vastata hiljemalt kümne päeva jooksul alates tunnistuse saamisest, välja arvatud juhul, kui taotlev asutus esitab andmete varasema avaldamise põhjused, ning erakorralistel juhtudel hiljemalt kuue tunni jooksul, nagu sätestatud artikli 9 lõigetes 1 ja 2.

Euroopa Andmekaitsekoogu pole aga näinud ühtegi kriteeriumi, mille alusel oleks ametiasutustel kohustus tõendada vähemalt tagantjärele andmete esitamise olukorra erakorralisust, et tagada võimalik kontroll selle väga kiire menetluse kasutamise üle, samas kui kuuetunnine tähtaeg osutab tõenäoliselt väga vähesele kontrollile enne andmete esitamist, kui mitte teenuseosutaja kontrolli täielikule puudumisele. Mõjuhinnaangus rõhutatakse, et pädevatel asutustel on vaja andmetele pääseda juurde aegsasti. Kõik mõjuhinnaangus esitatud näited puudutavad aga tõendeid, mida on vaja raskete kuritegude korral (pantvangidega terrorismijuhtumid, lapse pideva seksuaalse väärkohtlemise juhtumid), aga tuginemine tõendite volatiilsusele ei paista pädevat, kui

<sup>24</sup> Vt kohtuasi C-203/15, punkt 120.

<sup>25</sup> Vt liidetud kohtuasjad C-293/12 ja C-594/12, punkt 62.

<sup>26</sup> Vt nt kohtuasi C-203/14.

<sup>27</sup> Vt nt *Moulin vs. Prantsusmaa*, 23. november 2010.

kiireloomulisust ei toeta miski muu kui see andmete võimalik volatiilsus. Samuti ei anna andmete volatiilsus täiendavat põhjendust selle kohta, kas olukordades, kus volatiilsus on ainus kiireloomulisust toetav seik, on juurdepääs vähemate kaitsemeetmetega proportsionaalne.

Ühtlasi kahtleb Euroopa Andmekaitsekoostöögrupi vajaduses sätestada kuuetunnine tähtaeg, kui samas sätestatakse, et kui teenuseosutaja ei saa oma kohustust täita, ei kohaldata seda tähtaega enne, kui taotleja asutus esitab „viie päeva jooksul“ täiendavad selgitused.

Seega kutsub Euroopa Andmekaitsekoostöögrupp üles lisama mõjuhinnangusse täiendavaid elemente, et põhjendada vajadust nende tähtaegade järele olukordades, kus kuritegu, mis on toime pandud või mille eest süüdistus esitatakse, pole raske, ning kui selliseid üksikasjalikke elemente ei lisata, siis kutsub andmekaitsekoostöögrupp üles kehtestama sõnaselged kriteeriumid erakorralisuse põhjendamiseks Euroopa andmesaitamismääruse tunnustuste väljaandmise korral. Näiteks võidakse kehtestada samasugune mudel nagu Euroopa uurimismääruse direktiivis. Euroopa uurimismääruse direktiivis on sätestatud lühem tähtaeg, kui see on põhjendatud „menetlustähtaegade, süüteo raskuse või muude eriti kiireloomuliste asjaolude tõttu“ (vt artikli 12 lõige 2) või 24-tunnine tähtaeg kriminaalmenetluse tagamise vahendite üle otsustamiseks (vt artikli 32 lõige 2). Määruse eelnõu mõjuhinnangus pole esitatud üksikasju, millega saaks põhjendada, miks need tähtajad pole tõhusad; rõhutatakse üksnes seda, et saadetud taotluste hulk koormab taotlusi saavad õigusasutused üle, mistõttu nad ei suuda tähtaegadest kinni pidada.

### **c) Euroopa andmesaitamismäärust ja andmesäilitamismäärust ei tohi kasutada, et taotleda muu liikmesriigi andmesubjekti andmeid, ilma et selle liikmesriigi pädevaid asutusi vähemalt eelnevalt teavitataks, eelkõige sisuandmete puhul**

Euroopa Andmekaitsekoostöögrupp meenutab, et olemasolevates õigusaktides on õiguslane koostöö ja seega täiendavad kaitsemeetmed sätestatud eelkõige selleks, et kontrollida taotluste vajalikkust ja proportsionaalsust, ning rõhutab, et need kaitsemeetmed on veelgi enam põhjendatud juhtudel, kui taotletud andmed on sisuandmed, mille puhul piiratakse andmesubjektide õigust oma isikuandmete ja eraelu kaitsele rohkem. Sellega seoses meenutab Euroopa Andmekaitsekoostöögrupp, et Euroopa uurimismääruse direktiivis on sätestatud võimalus elektroonilist sidet teise liikmesriigi abiga pealt kuulata (vt artikkel 30) ning kohustus teatada andmete pealtkuulamisest teise liikmesriigi pädevale asutusele, kelle abi ei ole vajalik, kui asjaomane andmesubjekt asub sel hetkel või pealtkuulamise ajal selle liikmesriigi territooriumil (vt artikkel 31).

Euroopa Andmekaitsekoostöögrupp ei leia, et elektroonilisi tõendeid käsitleva määruse eelnõus ette nähtud menetlus, mille kohaselt on lubatud esitada sisuandmeid, ilma et kaasataks vähemalt selle liikmesriigi pädevaid asutusi, kus andmesubjekt asub, on põhjendatud.

### **d) Euroopa andmesäilitamismäärusi ei tohi kasutada selleks, et hoida kõrvale teenuseosutajate andmete säilitamise kohustustest**

Euroopa Andmekaitsekoostöögrupp märgib, et Euroopa andmesäilitamismääruste peamine eesmärk on vältida andmete kustutamist.

Kuigi Euroopa Andmekaitsekoostöögrupp tunnistab, et need määrused võivad mõnel juhul vajalikud ja proportsionaalsed olla, taunib ta kaitsemeetmete puudumist nende määruste tegemise korral. Eelkõige soovib Euroopa Andmekaitsekoostöögrupp, et kui andmesäilitamismäärused puudutavad üksnes konkreetseid andmeid, kuigi eelnõu näib lubavat ulatuslikke taotlusi, ja kui sellised määrused



tehadse andmete kohta, mis tuleb kooskõlas andmete säilitamise põhimõttega kustutada, ei saa teenuseosutaja kunagi määrusele tugineda, et töödelda andmeid pärast algset kustutamiskuupäeva. Teisisõnu tuleks andmed „külmutada“.

Seost andmesäilitamismääruse ja järgneva andmete esitamise taotluse vahel, olgu see Euroopa andmesäilitamismäärus, Euroopa uurimismääruse taotlus või vastastikuse õigusabi taotlus, tuleks tugevdada tagamaks, et Euroopa andmesäilitamismäärusi tehakse üksnes siis, kui muu taotluse esitamine on kindel (mitte üksnes võimalus, mida kaalutakse), ning et kui muu taotlus tagasi lükatakse, aegub ka andmesäilitamismäärus, ilma et tuleks oodata 60 päeva,<sup>28</sup> kui järgnev taotlus lükatakse tagasi varem.

### **e) Konfidentsiaalsus ja kasutajateave**

Euroopa Andmekaitsekoostöö nõukogu märgib, et määruse eelnõusse on lisatud konkreetne artikkel<sup>29</sup> saadetud määruste konfidentsiaalsuse kohta. Et vältida segadust ja arusaamatusi seoses õigusega andmekaitsele, meenutab Euroopa Andmekaitsekoostöö nõukogu, et kuigi isikuandmete kaitse üldmääruses on sätestatud, et andmesubjektide õiguste piiramine selleks, et tagada süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine, peaks olema õigusaktides sätestatud ja seega peaks see teave olema avalikult kättesaadav,<sup>30</sup> ning et asjaomased seadusandlikud meetmed peavad sisaldama konkreetseid sätteid andmesubjekti õiguse kohta olla piirangust teavitatud, välja arvatud juhul, kui see võib mõjutada piirangu eesmärki,<sup>31</sup> pole selles määruses sätestatud kohustust teavitada andmesubjekte eraldi igast juurdepääsutaotlusest, mille õiguskaitseasutused on esitanud.

Samal ajal tuleb Euroopa Andmekaitsekoostöö nõukogu meelde, et andmekaitse direktiivis on sätestatud andmesubjektide õigus saada seda teavet pädevatelt asutustelt endilt, välja arvatud juhul, kui seda õigust on piiratud; see õigus on kõigil andmesubjektidel, mitte üksnes neil, kes elavad ELi territooriumil.

### **f) Menetlus määruse täitmise tagamiseks, kui teenuseosutaja keeldub selle täitmisest**

Euroopa Andmekaitsekoostöö nõukogu märgib, et kui adressaat määrust ei täida, on määruse eelnõu artiklis 14 sätestatud määruse täitmise tagamise menetlus, mis põhineb õigusalasel koostööl taotleva asutuse ja täitjariigi pädeva asutuse vahel.

Paistab aga, et see menetlus võimaldab täitevasutusel keelduda edastatud määruse täitmise tagamisest üksnes menetluslikel põhjustel (samadel, mida kohaldatakse adressaadi puhul, peamiselt seoses esitatud teabe puudulikkusega või andmete esitamise faktilise võimatusega) või kuna asjaomased andmed on tema riigisisese õiguse kohaselt immuniteedi või privileegiga kaitstud või andmete avaldamine võib mõjutada selliseid riigi põhihuve nagu riiklik julgeolek ja kaitse<sup>32</sup>.

Seetõttu väljendab Euroopa Andmekaitsekoostöö nõukogu taas muret selle pärast, et võrreldes muude õigusaktidega puudub edastatud määruse topeltkontroll vastuvõtva pädeva asutuse poolt. Isegi keeldumine määruse täitmisest põhjusel, et sellega rikutaks harta sätteid, tundub kujutavat endast kõrgemat künnist tavapärasest künnisest, mis on seotud asjaomase isiku põhiõiguste rikkumisega. Võttes eeskujuks Euroopa vahistamismääruse, mille puhul on sätestatud keeldumise kohustuslikud ja

---

<sup>28</sup> Vt artikli 10 lõige 1.

<sup>29</sup> Vt artikkel 11.

<sup>30</sup> Vt artikli 23 lõike 1 punkt d.

<sup>31</sup> Vt artikli 23 lõike 2 punkt h.

<sup>32</sup> Vt artikli 14 lõige 2.

vabatahtlikud alused, või vähemalt Euroopa uurimismääruse direktiivi, milles on üldiselt sätestatud, et eeldust, et „vabadusel, turvalisusel ja õigusel rajaneva ala loomine liidus põhineb vastastikusel usaldusel ja eeldusel, et teised liikmesriigid järgivad liidu õigust, austades eelkõige põhiõigusi“, saab vaidlustada,<sup>33</sup> tuleks määruse eelnõus näha ette vähemalt klassikaline miinimumerand, et kui on põhjendatud alus arvata, et määruse täitmise tagamisega rikutakse asjaomase isiku põhiõigusi ning et täitjariik ei täidaks oma kohustusi seoses hartas tunnustatud põhiõiguste kaitsmisega, tuleks määruse täitmise tagamisest keelduda.

### **g) Määruste täitmise tagamine ja kolmanda riigi õigusest tulenev kohustuste konflikt (artiklid 15–16)**

Euroopa Andmekaitsekoostöögrupi avaldab heameelt määruse eelnõus adressaatidele kehtestatud võimaluse üle keelduda määruse täitmisest põhjusel, et see oleks vastuolus põhiõigustega, sest määruse eesmärk on pakkuda kaitsemeetmeid vastuoluliste õiguslike kohustuste korral. Samuti peab andmekaitsekoostöögrupi oluliseks, et ettepanekus on sätestatud konsulteerimine kolmandate riikide ametiasutustega, vähemalt konflikti esinemise korral, ning kohustus määrus tühistada, kui kolmanda riigi ametiasutus esitab vastuväite.

Menetlust, mis on ette nähtud selleks, et keelduda määruse täitmisest, kui kohustus on vastuolus kolmanda riigi õigusaktidest tulenevate kohustustega, tuleks aga oluliselt täiendada.

Euroopa Andmekaitsekoostöögrupi märgib, et määruse eelnõus usaldatakse eraettevõttele kui andmeesitamismääruse adressaadile hindamine, kas määrus oleks vastuolus kolmanda riigi kohaldatavate õigusaktidega, millega keelatakse taotletud andmete avaldamine. Ettevõtte peab esitama põhjendatud vastuväite, mis sisaldab kõiki olulisi üksikasju kolmanda riigi õiguse, selle kõnealusel juhul kohaldatavuse ja vastuoluliste kohustuste laadi kohta.

Eelkõige tunneb Euroopa Andmekaitsekoostöögrupi muret selle pärast, et kui selline vastuväide esitatakse, hindab taotleva asutuse liikmesriigi pädev kohus üksi, kas vastuolu on olemas või mitte, sest üksnes siis, kui kohus tuvastab vastuolu, võtab ta ühendust kolmanda riigi ametiasutustega. Seega antakse pädevale ELi kohtule selles kontekstis pädevus tõlgendada lõplikult kolmanda riigi õigust, ilma et ta oleks sel teemal ekspert. Seega leiab Euroopa Andmekaitsekoostöögrupi, et kohustus konsulteerida kolmanda riigi pädevate asutustega on kõnealuses ettepanekus liiga piiratud. Andmekaitse valdkonnas juhib Euroopa Andmekaitsekoostöögrupi seadusandja tähelepanu asjaolule, et kui kolmanda riigi pädev kohus tõlgendab isikuandmete kaitse üldmäärust hindamaks, kas see on vastuolus tema enda nõuetega, jäävad ELi andmekaitseasutused ja pädevad kohtud pädevaks, et hinnata sellise edastamise õiguspärasust, mis põhineb kolmanda riigi kohtu või haldusasutuse otsusel, millega nõutakse isikuandmete kaitse üldmääruse kohaldamisalasse kuuluvate isikuandmete edastamist või avaldamist<sup>34</sup>.

Samuti rõhutab Euroopa Andmekaitsekoostöögrupi, et kolmanda riigi õiguse hindamine, mida teeb ELi taotleva riigi pädev kohus, peab põhinema objektiivsetel elementidel, ning tunneb muret kriteeriumide pärast, mida pädev kohus peab artikli 15 lõike 4 ja artikli 16 lõike 5 kohaselt kolmanda riigi õiguse hindamisel arvesse võtma. Kohtul tuleks hinnata asjaolu, „kas kolmanda riigi õigusega püütakse põhiõiguste kaitse või kolmanda riigi riikliku julgeoleku või kaitsega seotud põhiõiguste kaitse asemel ilmselgelt kaitsta pigem muid huve või on selle eesmärk varjata ebaseaduslikku tegevust kriminaaluurimiste raames esitatud õiguskaitsealaste taotluste eest“, või hinnata huve,

<sup>33</sup> Vt Euroopa uurimismääruse direktiivi põhjendus 19.

<sup>34</sup> Vt isikuandmete kaitse üldmääruse artikkel 48.

„mida kolmanda riigi asjaomane õigusakt kaitseb, sealhulgas kolmanda riigi huvi andmete avaldamist ära hoida“. Näiteks tunneb Euroopa Andmekaitseõukogu muret, et kuigi see peaks olema tõenditel põhinev hindamine, milles võetakse arvesse vähemalt kogu kättesaadavat teavet, arvestades otsuse võimalikku mõju, tundub sõnastus („is being aimed to“ – „on selle eesmärk“) ebaselge ja seda tuleks muuta („has the aim/objective to“).

Euroopa Andmekaitseõukogu peab kahetsusväärseks, et ainus olukord, kus kolmanda riigi ametiasutustega konsulteeritaks ja kus nad saaksid andmeesitamismääruse täitmise suhtes vastuväite esitada, on siis, kui see pädev ELi kohus leiab, et esineb asjaomane konflikt, edastab kõik andmed asjaomase kolmanda riigi keskasutustele ning selle kolmanda riigi keskasutus esitab vastuväite lühikese, kuni 50-päevase tähtaja jooksul (15 päeva, mida võidakse pikendada 30 päeva võrra ning millele võidakse lisada viis lisapäeva pärast viimast võimalikku meeldetuletust). Kõigil muudel juhtudel oleks pädeval kohtul õigus andmeesitamismäärus jõusse jätta ning määrata rahaline karistus teenuseosutajale, kes keeldub määruse täitmisest. Seetõttu tunneb Euroopa Andmekaitseõukogu muret, et pädevatel ELi kohtutel pole ulatuslikumat kohustust konsulteerida asjaomaste kolmandate riikide pädevate asutustega, kindlustamaks, et menetlusega tagatakse süsteemsemalt mõlema poole argumentide arvessevõtmine, ning näitamaks üles rohkem austust kolmandate riikide õigusaktide suhtes.

Nagu juba rõhutatud artikli 29 töörühma avalduses ja eespool, meenutab Euroopa Andmekaitseõukogu, et erilist tähelepanu tuleks pöörata kolmandate riikide vastuvõetavatele sarnastele õigusaktidele, mis võivad mõjutada andmesubjektide õigusi ja nende õigust eraelu puutumatusse ELis; eriti tuleks tähelepanu pöörata riskile, et võetakse vastu sarnaseid õigusakte, mis on otseses vastuolus ELi andmekaitsealaste õigusaktidega.

Samuti rõhutab Euroopa Andmekaitseõukogu, et taotleva asutuse liikmesriigi pädev kohus isegi ei pruugi olla pädev kohus määruse eelnõu artikli 14 kohaseks määruse täitmise tagamiseks ning et see suurendaks vastuoluliste menetluste riski ja lisakontrollide puudumise riski vastuoluliste õigusaktide olukorras. See tuleneb asjaolust, et mõnel juhul võib olla kaasatud kolm riiki: määruse teinud asutuse riik, teenuseosutaja kolmas riik ning liikmesriik, kus asub teenuseosutaja ELi esindaja ja kus määruse täitmine tagada tuleks. Praegu sätestatud menetluse kohaselt saaks taotleva asutuse liikmesriigis A asuv kohus tõlgendada ise teenuseosutaja kolmanda riigi B õigust, ilma et ta taotleks selle kolmanda riigi asutustelt seisukohtade esitamist (kuigi nad vaidleksid määrusele vastu) ning paluda ELi liikmesriigi C kohtul tagada tehtud otsuse täitmine ilma võimaluseta vastuväide esitada.

Ühtlasi kiidab Euroopa Andmekaitseõukogu andmeesitamismääruste puhul heaks eriõiguskaitsevahendite kehtestamise lisaks isikuandmete kaitse üldmääruses ja direktiivis EL 2016/680 sätestatud õiguskaitsevahenditele. Artikli 29 töörühm nõudis juba oma eelmises avalduses selliste kaitsemeetmete kehtestamist. Euroopa Andmekaitseõukogu peab aga kahetsusväärseks, et selliseid õiguskaitsevahendeid pole ette nähtud ka andmesäilitamismääruste jaoks, sest nende määrustega võib samuti kaasneda nende isikute põhiõiguste piiramine, kelle andmeid säilitatakse. Andmesäilitamismääruste tulemusel võidakse säilitada andmeid kauem, kui seda oleks tehtud kooskõlas andmekaitse normidega. Seega kaasneb andmesäilitamismäärusega iseenesest asjaomase andmesubjekti põhiõiguste piiramine ning selle põhjendus tuleb üle vaadata ja selle puhul tuleb kohaldada eriõiguskaitsevahendeid, eriti juhtudel, kui andmesäilitamismäärus on tehtud koos andmeesitamismäärusega andmete saamiseks. Nagu soovitatud artikli 29 töörühma avalduses, tuleks ette näha õiguskaitsevahendid, mis on vähemalt samaväärsed nendega, mida saab kasutada riigisisises asjas.

## **h) Andmete edastamise turvalisus määrusele vastamisel**

Euroopa Andmekaitsekoostöö nõukogu märgib, et määruse eelnõus käsitletakse üksnes määru, mis adresseeritakse Euroopa Liidus asuvatele adressaatidele ning seega pole selles sätestatud konkreetset kanalit andmete vahetamiseks adressaatide ja teenuseosutajatega, kes asuvad väljaspool Euroopa Liitu.

Kuigi Euroopa Andmekaitsekoostöö nõukogu väljendab heameelt, et ELi üldisest andmekaitseraamistikust rohkem kõrvale ei kalduta, tuleb ta meelde, et iga määrus, mis saadetakse adressaadile, kelle puhul kaasneb edastamine väljapoole ELi, peaks vastama isikuandmete kaitse üldmääruses kehtestatud õigusraamistikule. Kõrvalehoidumine õiguslase koostöö õigusraamistikust, milles on ette nähtud andmekaitsealased kaitsemeetmed, mida tuleb järgida, ei tohiks kaasa tuua ka seda, et andmesitamis- või andmesäilitamismääruste adressaadid kalduvad nende määruste täitmisel kõrvale andmete edastamise nõuetest.

Kuigi Euroopa Andmekaitsekoostöö nõukogu väljendab heameelt selle üle, et puudub säte, millega kehtestatakse kohustus krüptitud andmeid dekrüptida,<sup>35</sup> tunneb ta muret, et ettepanekute eelnõudes pole kehtestatud adressaatidele konkreetset nõuet hinnata esitatavate andmete autentsust, ning rõhutab, et sellises hindamises seisneb traditsiooniliste õiguslase koostöö põhinevate vahendite lisaväärtus, ning hoiatab suurenenud riskide eest, mis kaasnevad asjaomastele andmesubjektidele sellise hindamise puudumisega.

## Järeldused

Selle hinnangu põhjal soovib Euroopa Andmekaitsekoostöö nõukogu esitada kaasseadusandjatele järgmised soovitused:

- 1) määruse õiguslik alus ei peaks olema ELi toimimise lepingu artikli 82 lõige 1;
- 2) uue õigusakti vajalikkust tuleks võrreldes kehtiva Euroopa uurimismääruse direktiivi või vastastikuse õigusabi lepinguga paremini näidata, muu hulgas analüüsid üsikasjalikult põhiõigusi vähem riivavaid võimalusi, näiteks nende olemasolevate instrumentide muutmist või kõnealuse õigusakti kohaldamisala piiramist andmesäilitamismäärustega, kombineerituna muude kehtivate menetlustega, mis käsitlevad andmetele juurdepääsu taotlemist;
- 3) määruses tuleks sätestada pikem tähtaeg, et võimaldada määrust täitval teenuseosutajal tagada, et põhiõiguste kaitsega seotud kaitsemeetmeid saab järgida;
- 4) topeltkaristatavuse põhimõtte tuleks säilitada, et jätta alles kohustus võtta arvesse mõlemas asjaomas riigis tagatud (riik, kus asub taotleja ametiasutus, ja riik, kus asub teenuseosutaja) kaitsemeetmeid, eriti juhul, kui loobutakse andmete asukoha kriteeriumidest;
- 5) määruse kohaldamisala tuleks piirata vastutavate töötajatega isikuandmete kaitse üldmääruse tähenduses või see peaks sisaldama sätet, milles on kehtestatud, et kui teenuseosutaja, kelle poole pöördui, pole vastutav töötaja, vaid volitatud töötaja, peab ta vastutavat töötajat teavitama;
- 6) määrus peaks hõlmama andmete edastamisega seotud kaitsemeetmeid, kui teenuseosutaja asub kolmandas riigis ja selles valdkonnas puudub kaitse piisavuse otsus, või määruses tuleks viidata direktiivile 2016/680, kui andmete edastamise suhtes kohaldatakse neid kaitsemeetmeid;
- 7) kuna kohustuslik esindaja määramine erineb isikuandmete kaitse üldmääruse kohasest esindaja määramisest, tuleks määruses täpsustada, et elektroonilisi tõendeid käsitleva

---

<sup>35</sup> Vt mõjuhinnangu põhjendus 19 ja lk 240.

määruse kohaselt määratud esindaja peaks olema eraldiseisev isikuandmete kaitse üldmääruse artikli 3 lõike 2 kohaselt määratud esindajast;

- 8) määrus peaks sisaldama laiemat elektroonilise side andmete määratlust, tagamaks, et asjakohaseid kaitsemeetmeid ja juurdepääsutingimusi, mis kehtestatakse, kohaldatakse nii muude kui sisuandmete kui ka sisuandmete suhtes;
- 9) määruses tuleks tõsta määruste tegemise künniseid ning määrusi peavad tegema või kinnitama kohtud, välja arvatud abonendiandmete puhul, eeldusel et selle andmekategooria määratlust kitsendatakse oluliselt, et see hõlmaks väga elementaarset teavet, mis võimaldab üksnes isiku tuvastada, ilma et saadaks juurdepääs sideandmetele;
- 10) määruses peaks juurdepääs abonendi- ja juurdepääsuandmetele olema piiratud üksnes määruses loeteluna toodud kuritegude või vähemalt „raskete kuritegudega“;
- 11) andmete esitamise tähtaega tuleks määruses paremini põhjendada, eriti erakorralistel juhtudel, ning kiire kuuettunnise menetluse kasutamise võimalus peaks hõlmama taotlejate asutuste kohustust tõendada kasvõi tagantjärele erakorralisust, millel selle menetluse kasutamine põhineb, et võimaldada kontrollida selliste erandlike õiguste kasutamist;
- 12) loobuda tuleks menetlusest, mille kohaselt on lubatud esitada sisuandmeid, ilma et kaasataks selle liikmesriigi pädevaid asutusi, kus andmesubjekt asub;
- 13) Euroopa andmesäilitamismääruse tegemisega seotud kaitsemeetmeid tuleks määruses täiustada;
- 14) määrus peaks hõlmama vähemalt klassikalist miinimumerandit, et kui on põhjendatud alus arvata, et määruse täitmise tagamisega rikutakse asjaomase isiku põhiõigusi ning täitjariik ei järgi oma kohustusi kaitsta hartas tunnustatud põhiõigusi, tuleks määruse täitmise tagamisest keelduda;
- 15) määruses tuleks ette näha ulatuslikum kohustus konsulteerida õigusaktide vastuolu korral selle kolmanda riigi pädevate asutustega, kus asub teenuseosutaja, kellelt andmete esitamist taotletakse, et vältida üheainsa kohtu subjektiivseid tõlgendusi;
- 16) andmesäilitamismääruste kehtivus ja andmete säilitamise kestus peaks olema rohkem seotud andmesäilitamismäärustega kaasnevate andmesäilitamismäärustega;
- 17) andmete edastamise turvalisus peaks olema paremini tagatud;
- 18) ette tuleks näha andmete autentsuse kontrollimine, eelkõige juhul, kui võidakse esitada krüptitud andmed.

Euroopa Andmekaitsekojukoogu nimel

eesistuja

(Andrea Jelinek)