



Tiina Uudeberg
Justiits- ja Digiministeerium
info@justdigi.ee

Teie 28.11.2025 nr 7-1/9632

Meie 22.12.2025 nr 1.1-21/251949

Kutse huvigruppidele tagasiside andmiseks EL digivaldkonna lihtsustamispaketi kohta

Austatud proua kantsler

Täname võimaluse eest esitada arvamus EL digivaldkonna lihtsustamispaketi (digiomnibus) kohta. Riigi Infosüsteemi Amet (RIA) toetab omnibusi üldisi eesmärke, kuid rõhutab vajadust selgete rollide, realistlike tehniliste nõuete ja küberturbe kaalutluste selgesõnalise arvestamise järele. Ilma selleta on risk, et regulatiivne lihtsustamine ei vähenda, vaid suurendab praktilist ja õiguslikku ebakindlust. RIA detailsemad hinnangud on alljärgnevad.

Üldhinnangud eelnõudes toodud eesmärkidele ja pakutud lahendustele

1. RIA vaatest on eelnõudes toodud üldised eesmärgid – reeglite ühtlustamine, killustatuse vähendamine ja parema õigusselguse loomine – põhimõtteliselt toetatavad. Eesti digiriigi toimimine eeldab, et andmete taaskasutuse, turvalisuse ja kättesaadavuse reeglid oleksid võimalikult selged ja üheselt mõistetavad.
2. Samas on RIA jaoks oluline, et pakutud lahendused ei tooks kaasa olukorda, kus tehniline vastutus ja õiguslik vastutus ei ole omavahel kooskõlas. Kui kohustused muutuvad vahetult kohaldatavaks ELi määruse kaudu, peab olema selge, millises ulatuses eeldatakse RIA-lt tehnilist hinnangut, nõustamist või järelevalvelist rolli ning millal on tegemist teiste asutuste pädevusega. Lahendusi, mis jätavad selle piiri ebaselgeks, ei saa pidada piisavalt praktiliseks.
3. Seoses isikuandmete töötlemise reeglitega AI arendamisel ja kasutamisel on RIA jaoks oluline tagada, et arvestatakse ka avaliku sektori vajadustega. Näiteks peaks lubatud isikuandmete töötlemise õiguslikud alused hõlmama riigi poolt isikuandmete töötlemiseks kasutatavaid aluseid.

Avaandmete direktiivi muutumine määruseks

4. Avaandmete direktiivi muutumine määruseks on RIA vaates põhimõtteliselt toetatav, kuna see vähendab liikmesriikide vahelisi erinevusi ja loob ühtlasema õiguskeskkonna. Samas on oluline, et määruse tekst arvestaks selgelt küberturbe ja teenuste töökindluse aspektiga. RIA kogemus näitab, et masinloetavus ja API-põhine ligipääs ei ole pelgalt tehniline mugavus, vaid ka potentsiaalne riskivektor. Seetõttu peab määrus võimaldama proportsionaalseid kaitsemeetmeid, nagu ligipääsupiirangud, kasutusmahupiirid ja autentimine, ilma et neid käsitataks avaandmete põhimõtte rikkumisena. Väärtuslike andmestike nimekirjade osas on oluline, et nende laiendamine toimuks koos selge riskihinnangu loogikaga. Eesti kontekstis võib näiteks haldus- ja menetlusandmetel olla suur ühiskondlik väärtus, kuid nende avamine

ilma piisavate turva- ja privaatsusmehhanismideta looks märkimisväärseid riske nii andmekaitse kui ka küberturbe vaates.

Praktiline rakendatavus

5. Praktilise rakendatavuse seisukohalt vajab RIA hinnangul täpsustamist eelkõige rollijaotus. Tuleb selgelt määratleda, milline asutus vastutab tehnilise taristu, milline andmepoliitika ja milline järelevalve eest. Praegu on oht, et RIA-st kujuneb vaikimisi asutus, kellelt oodatakse nii tehnilist hinnangut, riskide maandamist kui ka sisulist tõlgendust, ilma et see roll oleks õiguslikult selgelt sätestatud. Samuti vajavad täpsustamist üleminekusätteid: direktiivilt määrusele üleminek peab olema ajaliselt ja sisuliselt selge, et vältida olukorda, kus RIA peab samaaegselt lähtuma nii senisest riigisisestest regulatsioonist kui ka vahetult kohaldatavast ELi õigusest.
6. Eesti jaoks on spetsiifiline see, et suur osa andmete taaskasutusest toimub teenuste ja liidete kaudu, mitte staatiliste andmekogude avaldamisena. RIA kogemus näitab, et sama tehniline liides võib teenindada nii avalikku taaskasutust kui ka kriitilisi riigisiseseid protsesse. See tähendab, et avaandmete reeglid mõjutavad otseselt ka riigi infosüsteemide töökindlust ja küberturvet. Lisaks tuleb arvestada, et Eesti on kõrge digitaalse küpsusega riik, mistõttu suureneb ka rahvusvaheline huvi meie andmete ja liidete vastu. See omakorda tõstab kuritarvituse ja teenustõkestuse riski ning eeldab, et ELi õigusraamistik ei seaks RIA-le ebarealistlikke ootusi „avatuse“ osas ilma piisavate kaitsevahenditeta.
7. RIA jaoks on murekohaks eelkõige see, et lihtsustamise eesmärgi all ei tekiks uusi kaudseid kohustusi, mida tuleb täita ilma vastava ressursi, volituse või õigusliku selguseta. Samuti on oluline vältida olukorda, kus määrus loob formaalselt ühtsed reeglid, kuid praktikas suureneb vajadus iga üksikjuhtumi eraldi tõlgendamiseks. RIA rolli vaates on kriitiline, et tehnilised juhised ja põhimõtted ei muutuks vaikimisi siduvaks „pehmeks õiguseks“ ilma, et nende õiguslik kaal ja vastutus oleksid selgelt määratletud.
8. Seoses avaandmete direktiivi ja andmehalduse määruse ühildamisel oleks vajalik tekitada enne õigusmuudatuste jõustumist uued väärtused, kuidas eristada avaandmeid ja kaitstud andmeid lisaks kõrgväärtusega andmetele. RIA vajab aega, et viia muutused sisse nii standardisse kui rakendustesse ja seda kirjeldajatele kommunikeerida.

Ühtse kontaktpunkti loomine

9. Esiteks on ühtse kontaktpunkti (*single-entry point, SEP*) loomine positiivne samm erinevatele teenuse osutajatele, kes peavad intsidentide kohta raporteid esitama. Kindlasti toetame seda, et raporti esitamise kohuslased saaksid seda teha võimalikult efektiivselt ja vähese ajakuluga.
10. Siiski ei ole praegu selgelt ja üheselt aru saada, kuidas SEP praktikas toimib. SEP loomisel on vajalik ühtlustada erinevate liikmesriikide standardid, millega intsidendid kvalifitseeritakse ja kuidas neid käsitletakse. Samuti on vajalik ühtlustada erinevate regulatsioonide alusel esitatavad intsidendiraportid ning nendes sisalduv vajalik info (NIS2, GDPR, DORA).
11. Küsitav on, kas SEP keskkond luuakse viisil, kus esmase teavituse saavad liikmesriigid, kes edastavad vajadusel info ENISA-le või haldab kogu SEP keskkonda ENISA, kes suunab intsidendiga seotud info vastavatele pädevatele asutustele liikmesriikides.
12. **RIA hinnangul ei ole lahendus, kus SEP keskkond luuakse ENISA juurde ning ENISA saadab kogu vajamineva info edasi liikmesriikide pädevatele asutustele jätkusuutlik. See võib pikendada ajakriitilises olukorras intsidendi käsitlemise aega.** Loogilisem oleks ülesehitus, kus SEP raporteerimiskeskond luuakse liikmesriikide juurde, kes edastavad võimaliku riikide ülese intsidendiohu korral info ENISA-le, mille kaudu saadetakse teave teiste riikide pädevatele asutustele.
13. **Näeme, et andmete koondamine ja keskse andmebaasi/andmehoidla loomine sisaldab endas võimalikku turvariski.** Suure tõenäosusega tuleb info koondamisel luua ENISA juurde

andmebaas seoses SEP raportitega. Kui selline andmebaas tekib (ilmselt on vaja päringud vastu võtta, valideerida, talletada intsidendiinfo, et seda edasi saata/töödelda), on tegemist äärmiselt tundlikku infot sisaldava andmebaasiga. See omakorda loob võimaliku keskse sihtmärgi, mille kompromiteerimine võib avaldada äärmiselt laiaulatuslikku mõju kogu EL siseturvalisusele. Vajalik on luua usaldus, et loodud süsteem on turvaline, ettevõtte ja kodanikud teavad, kuidas nende andmeid kasutatakse ja millised meetmed on kasutusele võetud, et turvalisus oleks tagatud. Vastasel juhul võib tekkida situatsioon, kus intsidendiraporteid ei esitata põhjusel, et süsteemi kui tervikut ei usaldata. RIA hinnangul ei pruugi olla mõistlik luua ühte kesket andmebaasi, vaid hajutada info, et kogu tundlik info ei oleks talletatud keskselt. Samuti soovitame selgelt määratleda krüpteerimisstandardid, muuhulgas peaks arvestama selged ja kindlad kriteeriumid juurdepääsu osas ja reeglid korrapärase auditeerimise jaoks.

Lugupidamisega

(allkirjastatud digitaalselt)

Joonas Heiter
peadirektor

Lauri Kriisa
Lauri.Kriisa@ria.ee