EESTI ANDMEKAITSE LIIT

19 detsember 2025

Tallinn

Lugupeetud Justiits- ja digiministeerium,

allpool on Eesti Andmekaitse Liidu vastus kutsele (28.11.2025 nr 7-1/9632) anda tagasidet EL digivaldkonna lihtsustamispaketi kohta.

- **Kas toetate eelnõudes toodud eesmärke ja pakutud lahendusi? Palun tooge välja, milliseid toetate ja miks? Milliseid ettepanekuid Teie ei toeta ja miks?**

Osaliselt toetame art 12(5) (andmesubjekti päringutele vastamine), art 13(4) (privaatsusteabe esitamise piirangud), art 35 (andmekaitsealase mõjuhinnangu nõuded) muudatusi, kuna nendega lihtsustakse eelkõige väike ja keskmistel ettevõtetel IKÜMi mõistlikku rakendamist.

Samas ei toeta me Art 12(5) muudatuse ettepaneku seda osa, mis näeb ette, et andmesubjektid võivad oma isikuandmete kohta teabe saamiseks esitada päringu vaid isikuandmete kaitselistel eesmärkidel ehk „andmesubjekt kuritarvitab antud õigusi muul eesmärgil kui oma andmete kaitsmine“, sest on küsitav kas pakutud piirang on proportsionaalne. Täiesti sisustamata on mõiste “oma andmete kaitsmise eesmärk” ning kui see õigus jätta vastutavatele töötlejatele, siis läheb see otsesse vastuollu IKÜMi läbipaistvuse ja vastutuse põhimõttega. Näiteks võib isikuandmete vastutav töötleja isegi keelduda päringule vastamast, kui tema hinnangul ei ole selline päring esitatud andmekaitselisel eesmärgil. Sellisel juhul on andmesubjektil võimalik ilmselt pöörduda järelevalveasutuse poole, kelle ülesandeks tundub saavat ka päringu eesmärgi hindamine ning hindamine, kas vastutav töötleja peab päringule vastama või ei. On ilmselge, et vastutavate töötlejate huvides on võimalikult palju sellistele päringutele mittevastamine, mistõttu näeme, et pakutud lahendus võib tekitada täiendavat koormust järelevalveasutusele ning ei taga andmesubjektide õigust teada kuidas nende isikuandmetega ümber käiakse.

Toetame ka art 33 muutmise ettepanekut, millega ühtlustatakse andmesubjekti ja järelevalveasutuse isikaundmete alase rikkumise teavitamise nõue mõlemat tuleb teavitada ainult kõrge riskiga rikkumiste puhul. See vähendaks nii vastutavate töötlejate kui järelevalveasutustetöökoormust ning aitaks keskenduda kõrge riskiga juhtumite menetlemisele ja kahjulike tagajärgede maandamisele. Usume, et see on olnud ka täna

järelevalveasutuste ootus. Toetame ka teavitamise tähtajapikendamist 96-le tunnile. See leevendaks eelkõige olukordi kus tähtaja arvestuse sisse jääb nädalavahetus.

Tervitame AI omnibusi loogikat, et kohustuste täitmine lükatakse edasi seniks, kuni on töötatud välja tööriistad (standardid ja juhised) vastavate kohustuste rakendamiseks.

Samuti toetame pisemaid muudatusi nagu nt kitsaste protseduuriliste toimingute puhul kõrge riskiga tehisintellekti kohustuste vähendamine (st kui high risk AI puhul on ainult AI element tegemas narrow proceduraltask'i, ei pea seda high risk AI-na registreerima).

Toetame ka eriliigiliste isikuandmete töötlemiseks selge õigusliku aluse loomist AI mudelite kallutatuse vältimiseks.

Toetame AI omnibusi võimalikult kiiret läbi menetlemist, eriti Tehisaru määruse kõrge riski kohustuste edasilükkamise vaatest, et vältida olukorda, kus kohustused hakkavad kehtima enne, kui neid edasi lükatakse. Praegune olukord tekitab ettevõtetele ebakindlust ja võimalikke ebamõistlikke kulusid.

- **Kas toetate avaandmete direktiivi muutumist määruseks? Kas näete, et oleks vajalik muuta väärtuslike andmestike nimekirju. Kui jah, siis kuidas ja miks?**

EAKL-I arvates on hetkel seadustes mida *digital omnibus* ümber kujundab, nii Andmehalduse kui Andmemäärus, täpselt defineerimata mis on "avaandmed" ja mis on "avalikud andmed". Parima praktika tava järgi on avaandmed need, mida *creative commons* litsentsiga saab iga soovija ükskõik mispidi analüüsida ja kasutada (ja avaandmeteks ei tohiks olla isikuandmed) ning avalikud andmed on need, mida kodanikud (ja ettevõtted ning asutused) on riigile kohustatud seaduse alusel esitama ja riik on kohustatud kodanikele avalikustama. Ilmselgelt on riigi käes olevad andmed väärtuslikud ning nende põhjal lisaväärtuse loomine oleks hüve mitte ainult riigile, vaid ka kodanikele, eriti kui lisaväärtus kodanike elu paremaks teeb, kuid see ei peaks tulema riigi kodanike privaatsusõiguste arvelt. Uus planeeritav Avaandmete määrus, mis ühendab siis Andmehalduse ja Andmemääruse peaks sisaldama konkreetset definitsiooni mille järgi avaliku sektori asutused saaksid aru, mis on siis avaandmed ja mis avalikud andmed.

Uue Avaandmete määruse ning Andmemääruses olevad nõuded andmete avaldamise (*disclosure*) võiksid sisaldada ka täpsemaid suuniseid – andmete kvaliteedi ja hulga kohta ja avaldamise sageduse kohta, kuna andmete avaldamine ei ole tasuta avaldajale ning piisava kvaliteedi puudumine ei võimalda andmetest lisandväärtust toota.

- **Millised aspektid ja ettepanekud vajaksid täpsustamist või lisaselgitusi, et oleksid praktikas rakendatavad?**

Pooldame ühtset teavituskanalit, et sama rikkumise pinnalt ei tuleks mitmes kohas ning mitu korda teavitada. Samas teeb ühtse teavituse keeruliseks erinevates aktides toodud erinevad teavitustähtajad ning tekib küsimus, et kui küberturbe intsident on samal ajal kui andmekaitse intsident, siis kas peab jätkuvalt esitama mitu teavitust (24h möödumisel NIS2 esmane teavitus, 72h möödumisel NIS2 teisene teavitus ja 96h möödumisel GDPR teavitus?). Seetõttu teeksime ettepaneku ühtlustada ka ühtse teavituskanali kaudu edastatavate teavituste tähtaegasid.

Art 4 (1) "Isikuandmed" (*Personal data*) - mõiste muudatused on tekitanud väga elavad diskussiooni erialases ringkonnas. Mõistame Komisjoni soovi juurutada Ühtse Kriisilahendusnõukogu (SRB) lahendist tulenevat praktikat, kui omnibuses toodud mõiste SRB lahendiga võrreldes laiendatud. Pooldame seda, et selgitatakse ja defineeritakse täpsemalt konteksti, millistel juhtudel ei ole isikuandmed enam isikuandmed nign milliseid andmekaitse nõudeid ei peaks täitma olukorras, kus päriselt andmete saajal ei ole mõistlikult võimalik isikut enam antud andmete pinnalt tuvastada. Leiame, et seda oleksvõimalik reguleerida ka selliselt, et sisustada täpsemalt pseudonüümimise mõiste ja siduda see kohustusega viia läbi regulaarset hindamist, et hinnata kas pseudonüümimine on piisavalt tugev.

Isikuandmete mõiste praeguse sõnastuse laiendamine tekitab küsimusi selles osas, kuidas praktikas rakendada. Täpsemalt, milliseid andmekaitse nõudeid peab täitma juhul, kui saaja jaoks ei ole andmed enam isikuandmed. Näiteks kas on vajalik andmetöötluslepingu sõlmimine, kui vastutava töötleja vaatest on tegemist isikuandmetega, kuid saaja vaatest ei ole saadavad andmed isikustatud andmed. Sarnased küsimused võivad tekkida ka muude vastutava töötleja kohustuste täitmisel (nt andmelekkest teavitamine, Transfer Impact Assessment (TIA), volitatud töötlejate avaldamine andmesubjektile jms). Teeme ettepaneku selgelt IKÜM-is sätestada, et juhul, kui saaja jaoks ei ole tegemist isikuandmetega, ei ole kohustust sõlmida ka andmetöötluslepingut.

AI treenimise/arendamise õiguslikud alused. Aastaid nähti vaeva, et hoida IKÜM tehnoloogianeutraalne, kuid nüüd on sisse kirjutatud konkreetse tehnoloogiaga seotud sätted. Kuigi tervitame, et on selgelt välja toodud, et eriliigilisi isikuandmeid võib kasutada AI kallutatuse vähendamiseks, tundub AI treenimise üldise õigusliku aluse lisamine IKÜM-isse liigne ja ebavajalik. Ka muude tehnoloogiate puhul käib arendustegevus sisuliseltõigustatud huvi või isiku nõusoleku alusel. Seetõttu leiame, et ka täna kehtiv regulatsioon võimaldab AI treenimist viia läbi õigustatud huvi ja nõusoleku alusel. Antud sätete lisamine võib tekitada küsimusi, et kas muude tehnoloogiate arendamise puhul ei saa enam kasutada õigusliku alusena õigustatud huvi.

Tervitame küpsiste klausli täpsustamist ja selle isikuandmeid puudutava osa toomist IKÜMisse, kuid see täpsustus ei ole siiski piisavalt kaugeleulatuva mõjuga, et anda andmesubjektile tegelik ülevaade veebis toimuva jälitamistegevuse (*tracking*) kohta.

ePrivaatsuse direktiivilt IKÜM-le üleminek reguleerimaks isikuandmete töötlemist lõppkasutaja seadmes uue IKÜM artikli 88a kaudu tuues üle ePrivaatsuse art 5 lõige 3 "lõppkasutaja seadmesse salvestatule on vaja lõppkasutaja nõusolekut", mõningate täiendustega, näiteks on piiratud nimekiri madala riskiga ja vajalikest eesmärkidest, mis ei vaja õiguspäraseks toimimiseks nõusolekut (nt edastamine; selgesõnaliselt taotletud teenus; sihtrühma mõõtmine vastutava töötleja enda tarbeks; turvalisuse tagamine). Kuid ikka räägitakse ainult küpsistest ja nõusolekutest küpsistele, jättes tähelepanuta jälitamise (*tracking*) muud tehnoloogiad ning jälitamise vajalikkuse või õiguspärasuse.

EAKL ei ole kindel, et väljapakutud muudatused toovad kaasa selguse teiste jälgivate tehnoloogiate puhul (pixel, eTag etc), mille puhul võib vaielda, et lõppkasutaja seadmesse siiski midagi ei salvestata. Ehk oleks võinud Euroopa Komisjon siin julgem olla ning defineerinud tehnoloogia mittespetsiifilise veebis jälgimise vastuvõetavad tingimused? Küsitav on ka, et kas lihtsalt küpsiseid reguleerides on võimalik lahendada niinimetatud „nõusoleku väsimus"? Küpsiste puhul, kui veebilehitsejate standardid on praktilised ja kasutajakogemus selge, on võimalik nõusoleku väsimuse vähendamine, ilma nõusoleku tugevust õigusliku alusena kahjustamata.

Samas on positiivne, et koos IKÜM artikliga 88b saab komisjon mandaadi brauseri/ rakenduse vahendatud nõusolekute andmise standardiseerimiseks; kui standardid on kehtestatud, peavad vastutavad töötlejad pärast lühikest ajapikendust austama masinloetavaid kasutajavalikuid, kusjuures nende puhul, kes neid järgivad, eeldatakse vastavust.

- **Kas on Eesti jaoks spetsiifilisi aspekte, mis mõjutavad valdkonna seniseid praktikaid. Palun tooge konkreetseid näiteid, viidake võimalusel analüüsidele-raportitele.**

ROPA (isikuandmete töötlemise register) kohustuse kehtestamine 750 või enama töötajaga ettevõtetele – Eesti kontekstis tundub, et selline muudatus võib tekitada praktikas probleeme. ROPA on andmekaitsekohustuste keskpunkt, mille olemasolu tagab ja aitab ka teiste andmekaitse kohustuste täitmist praktikas teostada. Kui seda pole, siis on praktiliselt ettevõtetel keerukas ka koostada nt privaatsusteadet ajakohasena, vastata andmesubjekti päringutele, kiireltreageerida andmeleketele jms. Lisaks sellele võib jääda mulje, et kui on 750 või vähem töötajat, siis pole eriti vaja andmekaitse vaatest pingutada ning see ei aita tõsta teadlikkust andmekaitse teemade olulisusest laiemalt (vajalik ka nt tõhusa andmehalduse ja AI rakendamiseks). Lisaks on ülevaade ettevõtte või asutuse andmetöötlemise toimingutest ja kasutatavatest rakendustest vajalik selleks, et andmetest lisaväärtust saada. Lisaks on Eestis väga palju isikuandmete vastutavaid töötlejaid, kus töötab vähem kui 750 inimest. Seega Eesti suhtes tähendaks selline piirang seda, et väga paljud ettevõtted vabaneksid väga

olulisest kohustusest. Võibolla tuleks tekitada võimalus liikmesriigil seda piirangut ise muuta, et iga liikmesriik saaks omale sobiva mugavduse teha ja näiteks lähtuda isikuandmete kogusest, mida töödeldakse.

- **Palun tooge välja muud teemad, mis on nimetatud aktide puhul Teile murekohaks.**

Andmete töötlemise dokumenteerimise kohustust ei peaks muutma. See on IKÜM halduskoormusest kõige suurema väärtusega osa ettevõtte või asutuse jaoks. Teades mis andmeid ettevõte töötleb võimaldab rohkemat kui IKÜM-ga vastavus, võimaldab ka andmete abil teha paremaid juhtimis- ja äriotsuseid.

Digiallkirjastanud EAKL juhatuse nimel,

_____

Maili Torma