Majandus- ja Kommunikatsiooniministeerium
Suur-Ameerika 1, 10122 Tallinn
Maris Ots (maris.ots@mkm.ee)

Tallinn, 21.10.2026

Arvamus avaliku teabe seaduse § 43[10] muutmise seaduse eelnõu (digitaalidentiteedi registreerimine) kohta

Viide: teie 07.10.2026 kiri nr 2-2/3461-1

Esitaja: Levi Hankins, asutaja ja tegevjuht, Third Rail Systems OÜ (registrikood 17488655), Tallinn

Toetan eelnõu eesmärki siduda iga digitaalidentiteet tuvastatava ja vastutava isikuga. Minu mure on see, et eelnõu paneb vastutuse isikule, kuid jätab tema nimel tegutseva tarkvara tegutsemise piirid täielikult seadusest välja.

1. Puudujääk

Eelnõu määratleb digitaalidentiteedi kui püsiva ja ainulaadse tunnuse, mille alusel saab tarkvaraline lahendus kavandada või sooritada toiminguid selle registreerinud füüsilise isiku eest. Seletuskiri läheb kaugemale: neid toiminguid käsitatakse isiku enda toimingutena ning nende eest jääb vastutama isik ise. Seletuskirja kohaselt digitaalidentiteedi ülesandeid, õigusi ega tegutsemise piire eelnõuga ei reguleerita; volitamine ja ulatus jäetakse poolte kokkuleppe ja konkreetsete teenuste tingimuste hooleks. Andmekogus töödeldakse üksnes isiku ees- ja perekonnanime, isikukoodi ja teovõime piiramise andmeid ning digitaalidentiteedi alusel tegutsevate tehniliste lahenduste kohta andmeid ei koguta.

Seletuskiri ise toob aga välja vastuargumendi. Selle enda hinnangul ei taga hea tava, sertifitseerimine, juhised, standardid ega lepingulised piirangud üksi ega koos selget vastutusahelat ega kolmanda isiku kontrollivõimalust. Ometi määravad eelnõu kohaselt agendi piirid praktikas just need lepingulised tingimused, enamasti teenusepakkuja standardsed kasutustingimused. Kasutaja ei saa neid läbi rääkida ning agendi tegevuse tõttu kahju kannatanud isik ei ole nende tingimuste pool. Risk on praktiline. 2026. aasta juulis jõudsid OpenAI küberrünnakuvõimekuse testis vähendatud kaitsemeetmetega töötanud agendid internetti ning kompromiteerisid omandatud juurdepääsuandmete abil mitme päeva jooksul Hugging Face'i tootmistaristu, nagu mõlemad ettevõtted on teatanud. 20. oktoobril 2026 avaldatud METR-i välishinnang Anthropicu 2026. aasta augusti riskiaruandele leidis, et Anthropicu järelevalve ei oleks hiljutist intsidenti tõenäoliselt tuvastanud ja et seda saab lihtsate võtetega välja lülitada; praegust madalat riski seostas hinnang peamiselt mudelite piiratud võimekusega, mitte kaitsemeetmetega. Just volitusi, mida ei saa piiritleda ega kiiresti tagasi võtta, sellised juhtumid ära kasutavadki.

2. Olemasolev eeskuju: DORA artikkel 30

Finantssektoris on sarnane probleem juba lahendatud. Digitaalse tegevuskerksuse määruse (EL) 2022/2554 (DORA) kohaselt jääb finantsüksus väljasttellitud teenuste eest täielikult vastutavaks

(artikli 28 lõike 1 punkt a), kuid artikkel 30 sätestab IKT-teenuse osutajaga sõlmitava lepingu kohustusliku miinimumsisu. Igas sellises lepingus peavad olema teenuste selge ja täielik kirjeldus ning lõpetamisõigused (artikli 30 lõike 2 punktid a ja h). Kriitilisi või olulisi funktsioone toetavate teenuste lepingutes peavad lisaks olema piiramatud juurdepääsu-, kontrolli- ja auditeerimisõigused, mille tegelikku kasutamist ei tohi muud lepingulised kokkulepped takistada ega piirata (artikli 30 lõike 3 punkti e alapunkt i). Just see on siin oluline: teenuseosutaja standardtingimused ei saa seda tühistada. Sama ülesehitus sobib digitaalidentiteedile: toiming kuulub isikule ning seadus kehtestab miinimumnõuded tingimustele, mille alusel tarkvara tema nimel tegutseb. Tänan selle paralleeli eest Andreas J. Gorisekit (AJG Strategy & Navigation).

3. Ettepanekud

a) Põhitingimused iga digitaalidentiteedi kasutuse puhul: kirjeldus, mida tarkvara võib isiku eest teha ja kui kaua, ning isiku õigus see viivitamata tagasi võtta. Isikul peaks olema ka juurdepääs tema nimel tehtud toimingute logile. Registreeringutel peaks vaikimisi olema kehtivusaeg, mitte püsivus, nii et volitus lõpeb, kui seda ei uuendata.

b) Rangemad tingimused, kui tarkvara teeb makseid, võtab õiguslikke kohustusi või töötleb eriliigilisi isikuandmeid: selgesõnaline eelnev luba sellise toimingute kategooria jaoks ning isiku juurdepääsu- ja auditeerimisõigused. Seletuskiri juba tunnistab, et isik võib digitaalidentiteedile kohaldada rahalise summa või töödeldavate andmete piiranguid; seadus peaks tegema nende piirangute seadmise võimaluse kohustuslikuks.

c) Kehtetuks tunnistamine peab toimima turvalises suunas. Kui teenus ei suuda registreeringu kehtivust kinnitada, tuleb digitaalidentiteeti käsitada kehtetuna. See järgib EUDI rahakoti mobiilse juhiloa töös valitud lähenemist, mille kohaselt ebaõnnestunud kehtivuskontroll muudab volituse kehtetuks. Tänan selle tähelepaneku eest Alvar Soomet.

d) Andmekogu peaks näitama volitust, mitte ainult isikut: vähemalt seda, millist väljaandjat või võtit tegutsev tarkvara kasutab, ning olekut koos ajalooga, et üksiku agendi saaks tagasi võtta ilma kõiki teisi registreeringuid lõpetamata. See järgib Nodachi avaldatud analüüsi (toimetaja Priit Kaasik).

e) Ettevõtete nimel tegutsevad agendid. Digitaalidentiteedi saab registreerida üksnes füüsiline isik, kuid seletuskirja enda näide on ettevõtjad, kes haldavad kümneid agente, ning ühe tunnuse all võib tegutseda üks või mitu tarkvaralist lahendust. Eelnõu peaks sätestama, kes vastutab, kui tarkvara tegutseb juriidilise isiku nimel, ning toimingute logist peaks nähtuma, milline agent millise toimingu tegi. Sellele on avalikult tähelepanu juhtinud ka Peeter P. Mõtsküla.

f) Üks tunnus, palju teenuseid. Kui registreerimine on tasuline ja üks tunnus võib hõlmata mitut tarkvaralist lahendust, kipuvad inimesed kasutama ühte tunnust kõigi automatiseeritud päringute jaoks. See muudab tunnuse püsivaks vahendiks isiku tegevuse sidumiseks eri teenuste vahel, mis on vastuolus võimalikult väheste andmete kogumise põhimõttega (isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt c). Andmekogu peaks võimaldama eraldi tunnuseid iga agendi või eesmärgi jaoks ilma lisatasuta. Sellele on avalikult tähelepanu juhtinud Aivo Olev.

4. Vastutus

Seletuskirja kohaselt lahendatakse vastutuse küsimusi valdkonna õiguse alusel ning need ei ole seotud digitaalidentiteedi registreerimisega. See on õige ja see tuleks selgesõnaliselt välja öelda: agendi toimingute käsitamine isiku enda toimingutena ei mõjuta teenusepakkuja enda vastutust. See hõlmab ka tootevastutust kahju kannatanud isiku ees direktiivi (EL) 2024/2853 alusel, mille kohaselt vastutavad mitu vastutavat ettevõtjat solidaarselt (artikkel 12) ning seda vastutust ei saa lepinguga välistada ega piirata (artikkel 15).

5. Miks see on oluline

USA mereväes anti delegeeritud volitus kirjalikult. Allkiri „by direction“ tähendas, et ülem oli nimetanud, kes võib allkirjastada ja milleks, ning võis volituse igal ajal tagasi võtta. Registreering ilma sellise kirjaliku ulatuseta muudab isiku vastutavaks toimingute eest, mida ta ise kunagi ei määratlenud.

Lugupidamisega

Levi Hankins
Asutaja ja tegevjuht, Third Rail Systems OÜ
levi@thirdrailsystems.ee | +372 5385 4769