



KAITSEMINISTEERIUM

Justiits- ja Digiministeerium
Suur-Ameerika 1, 15006 Tallinn
info@justdigi.ee

Teie: 01.05.2026 nr JDM/26-0172/-3K

Meie: 29.05.2026 nr 5-7/26/53-5

Eelnõu kooskõlastamine märkustega "Avaliku teabe seaduse muutmise seaduse eelnõu väljatöötamiskavatsus"

Kaitseministeeriumile on arvamuse avaldamiseks edastatud avaliku teabe seaduse ja teiste seaduste muutmise seaduse eelnõu. Kaitseministeerium kooskõlastab eelnõu järgmiste märkuste ja ettepanekutega arvestamisel:

1. andmejälgija;
2. riiklik postkast;
3. andmekorraldus;
4. dokumendihaldussüsteem (DORIS).

1. Andmejälgija

1.1 Esitatud eelnõu kohaselt peab andmejälgijaga liidestunud andmekogu vastutav töötleja tagama, et andmesubjektil on võimalik andmejälgija vahendusel tutvuda tema isikuandmetega seotud päringulogidega. Päringulogid peab andmejälgijasse edastama selle andmekogu vastutav töötleja, kes andmeid päris. Täiendavalt võib andmeid väljastanud andmekogu vastutav töötleja edastada andmejälgijasse sama päringuga seotud logikirje. Eelnõu seletuskirjas on selgitatud, et andmejälgijas võib päringulogisid ajutiselt mitte kuvada julgeolekuasutuste seaduse (edaspidi JAS) § 211 lõikes 3 sätestatud piirangute rakendamiseks. Seletuskirja kohaselt on andmesubjektil õigus selle teabega tutvuda ka andmejälgijast sõltumata, mistõttu ei ole põhjendatud jätta selliseid logikirjeid andmejälgijast täielikult ja tähtajatult välja. Eelnõu seletuskirjas esitatud argumentatsioon ei ole lõpuni korrektne. Andmejälgija on isikuandmete kaitse üldmääruse (edaspidi IKÜM) järgseid õigusi edendav tööriist, kuid IKÜM kohaldub julgeolekasutuse tegevusele ainult piiratud ulatuses. Seega ei ole korrektne väita, et näiteks luure- ja vastuluure täitmise ülesannete eesmärgil tehtud päringuga on andmesubjektil igal juhul õigus tutvuda. Kaitseministeerium on seisukohal, et julgeolekuasutusele ei tohi panna proaktiivset päringute avaldamise kohustust. Eelnõuga kaasneb oluline õigusselgusetus:

- 1.1.1 Eelnõu ei täpsusta, millistel juhtudel edastab ka päringu saanud andmekogu päringulogi andmejälgijasse ning seetõttu ei ole selge, kuidas on tagatud eriseaduses sätestatud andmesubjekti õiguse piirangu kohaldamine.
- 1.1.2 Eelnõu eesmärk on panna päringulogide edastamise kohustus andmekogu vastutavale töötlejale, kes andmeid pärivad (kavandatud § 43¹¹ lg 2³). Juhime tähelepanu, et selle sõnastuse kohaselt ei pea vastutav töötleja esitama andmejälgijasse logikirjeid nende päringute kohta, mille tegi asjaomase andmekogu volitatud töötleja.
- 1.1.3 Eelnõu sõnastus käsitleb andmete väljastamise päringulogide kuvamist andmejälgijas. Andmete väljastamist on kehtivas õiguses eristatud andmetele juurdepääsu andmisest. Eelnõus ega seletuskirjas ei ole kirjeldatud olukordi, kus asutusele ei väljastata andmeid

- aga asutusele on antud juurdepääsuõigus mõne teise asutuse andmekogu andmetele.
- 1.1.4 Eelnõu kohaselt on andmejälgija riiklik infosüsteem, kuhu edastatakse üle X-tee tehtud päringulogid. Selline sõnastus viitab, et andmejälgija infosüsteem töötleb, sh säilitab päringulogide andmeid. Kui andmejälgijasse koonduvad kõikidesse andmekogudesse esitatud päringute logikirjed (sh isikuandmed), moodustub arvestatav korrastatud andmete kogum. Eelnõu seletuskirjas ei ole esitatud analüüsi, miks ei ole andmejälgija näol tegu andmekoguga ning sellele ei kehtestata põhimäärust. Kui andmejälgija tehniline lahendus ei vasta eelnõus kirjeldatule, tuleks eelnõu sõnastust vastavalt muuta.
 - 1.1.5 Andmejälgija infosüsteemi vastutav töötleja on Justiits- ja Digiministeerium ning volitatud töötleja Riigi Infosüsteemi Amet. Eelnõus ei ole kirjeldatud nende asutuste õigusi ega kohustusi andmejälgija infosüsteemi pidamisel, seejuures andmejälgija infosüsteemi turvameetmeid.
 - 1.1.6 Tõime eelnevalt välja, et eelnõu seletuskirja kohaselt tuleks julgeolekuasutusel andmete kuvamisel andmejälgijas rakendada JAS § 211 lõikes 3 sätestatud andmesubjekti õiguse piirangut. Seletuskirjas ei ole aga analüüsitud, millistel juhtudel andmejälgija julgeolekuasutuse tegevusele kohalduma peaks ning kas eelnõu sõnastuse järgi üldse kohaldubki. Eelnõu järgi tuleb päringulogid edastada päringu teinud andmekogu vastutaval töötlejal. On selge, et JAS § 311 alusel on julgeolekuasutusel juurdepääs avaliku teabe seaduse (edaspidi AvTS) alusel asutatud andmekogu andmetele. Küll aga ei ole nt Välisluureamet ühegi andmekogu vastutav töötleja AvTSi tähenduses ning andmeid päritakse töötlussüsteemidesse, millele AvTS ei kohaldu.
 - 1.1.7 Eelnõu seletuskirjas ei ole esitatud andmejälgija infosüsteemi põhiseaduspärasuse analüüsi, kirjeldatud selle tehnilist teostatavust ega nähtu, et andmejälgija infosüsteemi rakendamiseks oleks planeeritud rahalisi vahendeid.
 - 1.1.8 Teeme ettepaneku sätestada seadusesse, et julgeolekuasutuse tehtud päringuid riiklikesse andmekogudesse andmesubjektile andmejälgija kaudu ei avaldata.
- 1.2 Kaitseväge korralduse seaduses (edaspidi KKS) sätestatud julgeoleku- ja luureülesannetele tuginedes on Kaitseväel õigus teha varjatud päringuid ning piirata andmesubjekti teabeõigust kaitseväeluure raames tehtud päringute osas. Kuigi üldseaduse ja eriseaduse kollisiooni korral rakendub eriseadus, on õigusloome normitehnikale tuginedes vajalik üldseaduse tasandil vastav õigus seaduses sätestada. Sellest lähtuvalt palume kaaluda antud klausli lisamist AvTS-i. Samuti palume kaaluda võimalust, et selliste logimise erandid oleksid kõrvale jäetud andmejälgijasse jõudmise suhtes (ka varjatuna) ning selle vajadust AvTS sõnaselgelt kajastada. KKS ja ka JAS näevad ette varjatud päringute tegemise õiguse, isikute õiguste piiramise mh andmetele juurdepääsu osas ning ei ole otseselt piiratud selle varjatuse perioodi tähtajaliselt. Samuti ei ole IKÜM-st tulenevad läbipaistvus ja selle nõuded asjakohased luure- ja julgeoleku funktsioonide puhul EL õiguse pädevuste piiritlemise tõttu. AvTS VTK-s on välja toonud, et andmejälgijas võib päringulogisid ajutiselt mitte kuvada samadel alustel, mille alusel lubab eriseadus andmesubjektile vastavat teavet ajutiselt mitte anda. Kaitseministeerium teeb ettepaneku sellele tuginedes üldseaduse tasandil konkreetne säte lisada.
- 1.3 Kuna eelnõu kohaselt peab andmejälgija liidestumine olema teostatud hiljemalt 1. juuniks 2027, palume tähtaja edasilükkamist. Tegemist on niivõrd ulatusliku arendustegevusega, mille vajadusega ei ole senistes töö- ega arendusplaanides arvestatud. Arvestades arenduste mahtu, vajalike ressursside planeerimise aega ning võimalikke sõltuvusi teistest infosüsteemidest, on kavandatud tähtaeg ebarealistlik.

2. Riiklik postkast

- 2.1 Eelnõu kohaselt hakatakse riiklikku postkasti rakendama ühtse kanalina ametlike teadete ja dokumentide kättoimetamiseks füüsilistele isikutele. Eelnõule lisatud rakendusaktide kavandite hulgas sisaldub ka riikliku postkasti põhimääruse kavand, mille kohaselt on riikliku postkasti vastutav töötleja Riigi Infosüsteemi Amet ning volitatud töötlejateks teadete ja dokumentide saatjad. Lisaks on eraldi sihtrühmana nimetatud andmeandjad. Juhime tähelepanu, et põhimääruse kavandis ei ole erinevate osapoolte rollid ja vastutus piisavalt selgelt määratletud. Eelkõige jääb ebaselgeks, millistel alustel käsitatakse osapooli volitatud töötlejatena ning millistel juhtudel andmeandjatena. Selline ebaselgus võib praktikas põhjustada tõlgendusprobleeme õiguste, kohustuste ja vastutuse jaotumisel.
- 2.2 Esineb vastuolusid volitatud töötleja õiguste ja kohustuste kirjelduses. Näiteks on volitatud töötleja

kui saatja õiguste hulgas sätestatud, et volitatud töötlejal on õigus kehtestada saatjale tehnilised liidestamise nõuded, tööprotseduurid ja juhendid ning peatada või piirata saatja ligipääsu kesksel lahendusele juhul, kui saatja tegevus ohustab süsteemi turvalisust või töökindlust. Selline sõnastus tekitab olukorra, kus saatja näib kehtestavat nõudeid iseendale, mistõttu jääb regulatsiooni tegelik adressaat ja eesmärk ebaselgeks. Leiame, et rollid ning nendega seotud õigused ja kohustused vajavad selgemat ja üheselt mõistetavat sõnastamist.

3. Andmekorraldus

- 3.1 Eelnõu § 1 p 1 (AvTS §-i 3¹ lg 6). Muudatuse kohaselt avaldatakse andmekirjeldused, kuid üldiseks kasutamiseks antakse üksnes selline osa teabest, mis ei sisalda juurdepääsupiiranguga teavet ning mille üldiseks kasutamiseks andmisega ei kaasne juurdepääsupiiranguga teabe avalikuks tuleku oht. Märgime, et kõigi andmekirjelduste puhul ja andmekogude tehniliste dokumentide avaldamisel peab alati kaaluma ka küberturvalisusega seotud riski. Eelkõige tuleb vältida sellise teabe avalikustamist, mis võimaldab tuvastada süsteemide arhitektuuri, turvameetmeid, andmevahetuslahendusi või muid tehnilisi asjaolusid, mille pinnalt võib suurened küberrünnakute, volitamata juurdepääsu või andmete väärkasutuse risk. Samuti tuleb hinnata, kas erinevate avalikustatud andmekoosseisude riskasutus võib võimaldada tuletada juurdepääsupiiranguga või isikuandmeid sisaldavat teavet. Tänu tehisarude kiirele arengule on lihtne avaandmete kaudu riigi haavatavusi tuvastada ning kasutada neid oma eesmärkide edendamiseks, mh mittekonventsionaalse rünnaku planeerimisel ja elluviimisel. Avaandmete avaldamisega seotud riskitase võib suure tõenäosusega muutuda hübriidsõja olukorras. Valdkondlikud eksperdid on välja toonud, et Venemaa kasutab küberruumi ning avalikult kättesaadavat teavet sihipärase ja efektiivse tööriistana oma välis- ja julgeolekupoliitiliste eesmärkide toetamiseks.
- 3.2 Juurdepääsupiirangu sätestamise kord ja andmevaldaja mõiste. Kooskõlastustabelis (lk 34–35) on esitatud arvamus, et teabevaldajatel on vähene teadlikkus ja suutlikkus andmetega seotud riske tuvastada ja asjakohaselt andmetele ligipääsupiiranguid seada. Juhime tähelepanu, et Kaitseministeeriumi haldusalale olulist teavet võivad töödelda erinevad teabevaldajad, kellel ei pruugi olla täielikku ülevaadet ega pädevust hinnata teabe sensitiivsust riigikaitse, julgeoleku, andmekaitse ja küberturvalisuse vaatest. Samal teabel võib olla korraga mitu teabevaldajat (näiteks riigikaitseobjektide ja ruumandmete puhul), mistõttu võivad riskihinnangud ja juurdepääsupiirangute vajadus erineda. Teeme ettepaneku sätestada, et juurdepääsupiirangu kehtestamise või avalikustamise otsustamisel tuleb arvestada kõigi asjaomaste teabevaldajate hinnangute ning vajaduse korral kaasata pädevad asutused, et tagada andmete avalikustamise mõju terviklik hindamine, sealhulgas riigikaitsele, sisejulgeolekule, andmekaitsele ja küberturvalisusele. Ühe teabevaldaja jaoks võivad need andmed liigituda avaandmeteks, teise asutuse jaoks võib selle teabe avaandmetena avalikustamine olla oht julgeolekule. Rõhutame, et andmekogud, mis täidavad riigikaitse, julgeoleku- või luurealaseid eesmarke ning koguvad andmeid varjatult ja on liidestatud X-teega, peavad jääma avaliku teabe seaduse reguleerimisalast välja.
- 3.3 Eelnõu § 1 p 9 (AvTS 43⁵ lg 3). Palume täiendada sätet nii, et nende andmekogude põhimäärused, mille volitatud töötlejal on kahtlus, et kaaluda tuleb riigikaitse ja riigi julgeoleku või muu Kaitseministeeriumi haldusala ülesannete täitmisega seotud küsimusi, tuleb esitada kooskõlastamiseks Kaitseministeeriumile ja julgeolekuasutustele. Riigikaitse ja riigi julgeoleku jaoks oluliste andmekogude põhimäärused on vaja kooskõlastada pädevate asutustega, et tagada andmekogude ja nendes sisalduva andmekoosseisu (sh nt nende avaandmetena avalikustamine ja koosmõju teiste avalikustatud andmekoosseisudega) mõju hindamine riigikaitse, julgeoleku ja sisejulgeoleku vaatest. Kaitseministeerium ja selle allasutused näevad ohuna, kui avaldatakse detailselt riigikaitseobjektide kohta ruumiandmeid, ruumiobjekte või muid sensitiivseid andmeid (sh erinevate registrite avaandmed nt ehitisregister jmt). Riigikaitset korraldavaid asutusi ei ole seni paljudel juhtudel kaasatud teabe avalikustamise (avaandmetena kättesaadavaks tegemise) otsustusprotsessi. Seetõttu puudub Kaitseministeeriumi valitsemisalal selge ülevaade, kas on hinnatud teabe avalikuks tuleku ohte nii riigikaitse kui ka sisejulgeoleku tagamise vaates.

4. Dokumendihaldussüsteem Doris

- 4.1 Eelnõu § 1 p 15 (AvTS § 4313 lõige 5) näeb ette dokumendihaldussüsteemi DORIS kõigi asutuste jaoks. Varasema kokkuleppe kohaselt ei puuduta riigiülese dokumendihaldussüsteemi kasutusele võtmine Kaitseministeeriumi valitsemisala. Palume AvTS § 4313 lõiget 5 täiendada nii, et Kaitseministeeriumi valitsemisalale nimetatud paragrahvi ei kohaldata. Palume täpsustada, kas

dokumendihaldussüsteemile on kohustuslik rakendada andmejälgijat põhjusel, et süsteem omab x-tee liidest.

Lugupidamisega

(allkirjastatud digitaalselt)

Hanno Pevkur
minister