EESTI
INFOTEHNOLOOGIA JA
TELEKOMMUNIKATSIOONI
LIIT

Pr Liisa-Ly Pakosta
Justiits- ja digiminister
Justiits-ja Digiministeerium
Suur-Ameerika 1
10122 TALLINN

Teie 30.07.2026 nr 8-1/5650-1

Meie 6.08.2026 nr 6.1-1/133-1

Arvamus e-identimise ja e-tehingute usaldusteenuste seaduse, riigilõivuseaduse ja karistusseadustiku muutmise seaduse eelnõu kohta

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) esitab käesolevaga arvamuse e-identimise ja e-tehingute usaldusteenuse seaduse, riigilõivuseaduse ja karistusseadustiku muutmise seaduse eelnõu (edaspidi: eelnõu) kohta, millega reguleeritakse Euroopa Liidu määruse (EL)2024/1183 (edaspidi: eIDAS2) rakendamist ning Euroopa digiidentiteedikukru kasutuselevõttu Eestis.

Juhime tähelepanu, et eIDAS2 võeti vastu ja avaldati Euroopa Liidu Teatajas 2024. aasta aprillis ning selle riigisiseks rakendamiseks vajalike seaduse muudatuste tegemiseks on olnud aega üle kahe aasta. Seetõttu jääb meile arusaamatuks, miks otsustas Justiits- ja Digiministeerium eelnõu kooskõlastuse teha kiirustades andes huvigruppidele arvamuse kujundamiseks aega vaid 5 tööpäeva ja seda suvepuhkuste kõrgajal. Täname Justiits- ja Digiministeeriumit ITL-i kaasamise eest ka eelkonsultatsiooni käigus, kuid kuna ka see toimus juuli teises pooles ja lühikese tähtajaga, on osutunud tagasiside kokkupanek keeruliseks ja liikmesettevõtete eksperdid pole saanud eelnõud süvenenult analüüsida.

Esitame eelnõu kohta järgmised tähelepanekud ja ettepanekud:

1. Rollide koondumine RIA-sse ja täiendav järelevalvekulu

ITL juhib tähelepanu Riigi Infosüsteemi Ameti (RIA) rollide ulatuslikule koondumisele kavandatavas regulatsioonis. Eelnõu kohaselt hakkab sama asutus täitma samaaegselt mitut keskset rolli: digikukru lahenduse hankimine ja juurutamine, tegevusloa andmine ning järelevalve ja täitevmenetluse läbiviimine.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

ITL peab oluliseks tagada RIA hanke-, arhitektuuri- ja järelevalvefunktsioonide selge funktsionaalne sõltumatus. Selline rollide koondumine võib tekitada küsimusi funktsioonide sõltumatuse ning järelevalve erapooletuse kohta.

ITL on ka varasemalt teinud ettepaneku eraldada Riigi Infosüsteemi Ametist küberturvalisuse järelevalve roll ning toonud ühe võimaliku lahendusena näiteks järelevalve ülesannete üleviimise Tarbijakaitse ja Tehnilise Järelevalve Ametile. **Ka käesoleva eelnõu puhul peame oluliseks, et usaldusteenuste järelevalve oleks korraldatud institutsionaalselt sõltumatult. Oleme jätkuvalt seisukohal, et teostaja ja järelevalvaja rollid ei sobi kokku ühte asutusse ja leiame, et RIA ei tohi iseenda üle järelevalvet teha.**

Seaduseelnõu seletuskirjas on täiendavaks järelevalvekuluks RIA-le hinnatud 75 000 eurot aastas. RIA järelevalvele pannakse samas järgmised täiendavad ülesanded:

- digikukruteenuse pakkuja loamenetlused;
- riskihinnangute hindamine;
- turvaintsidentide menetlemine;
- tegevuslubade muutmine;
- EL-i aruandlus;
- registri järelevalve.

Seadus eeldab sisulist järelevalvet, kuid eelarve iseloomustab pigem vastavushindamisasutuse (Conformity Assessment Body, CAB) hinnangutele toetuvat formaalset järelevalvet. Loataotlusega tuleb järelevalvele täiendavalt esitada riskianalüüs, riskide mõju ja leevendusmeetmed.

Teeme ettepaneku täiendada eelnõud ja seletuskirja selliselt, et oleks üheselt selge: **teenusepakkuja tehnilise vastavuse, riskijuhtimise ja turvameetmete sisuline hindamine toimub vastavushindamise käigus vastavushindamisasutuste poolt. RIA järelevalve ülesanne on kontrollida vastavushindamise tulemuste olemasolu, kehtivust ning nende alusel teenuseosutaja vastavust õigusaktide nõuetele, analoogselt kehtiva kvalifitseeritud usaldusteenuste järelevalvemudeliga.**

See vastaks paremini ka seletuskirjas kirjeldatud järelevalve rahastamise mahule. Kui seadusandja eesmärk on anda RIA-le sisuline riskide hindamise ning tehniliste ja regulatiivsete turvaintsidentide menetlemise funktsioon, eeldaks see märkimisväärselt suurema erialase võimekuse loomist.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Praktikas tähendaks see dubleerivate ametikohtade loomist valdkondades, kus vastav kompetents on juba olemas vastavushindamisasutustes ning osaliselt ka RIA teistes üksustes, mis tegelevad digikukruhankimise ja arhitektuuri kujundamisega.

2. Digikukru, e-identimise süsteemide usaldusväärsuse taseme hindamine ja sertifitseerimine ning loa andmine

2.1. Euroopa digiidentiteedikukru (edaspidi: digikukkur) sertifitseerimise, usaldusväärsuse taseme hindamise ja pakkumise loa andmise protsessid ei ole eelnõus piisavalt selgelt reguleeritud. Näiteks ei selgu, kes ja millises menetluses hindab ning kinnitab digikukru usaldusväärsuse taseme „Kõrge“. On mõistetav, et oluline osa asjassepuutuvast regulatsioonist on eIDAS määruses ning selle alusel välja antud rakendusaktides. Palume siiski vähemalt seletuskirjas selgitada, mis kuulub digikukru sertifitseerimise skoopi, kes ja mis menetluses kinnitab digikukru usaldusväärsuse taseme ning mis on digikukru pakkuja loa menetluse skoobis.

Segadust lisab see, et digikukrut ja selle pakkumist on käsitletud usaldusteenuste ja usaldusteenuste osutajate peatükis (EUTS peatükk 2.). Digikurku regulatsioon on näiteks eIDAS määruses e-identimise süsteemide all. Vt sellega seoses ka täpsemat ettepanekut allpool, kirja punktis 8.1.

2.2. EUTS-is sätestatud siseriiklikku e-identimise usaldusväärsuse tasemete hindamise nõudeid ja korda ei peaks rakendama nende e-identimise süsteemide osas, mis on läbinud juba sertifitseerimise vastavalt eIDAS määrusele. Seetõttu teeme ettepaneku lisada eIDAS määruse ja rakendusaktide kohaselt sertifitseeritud e-identimise süsteemid eelnõuga EUTS § 1 lõikesse 5.

3. Nõuded kvalifitseeritud usaldusteenuse osutajale, usaldusteenusele ja digikukru pakkujale/pakkumisele ning loa andmise protsess

3.1. Digikukru sertifitseerimise ja loa kehtivusajad

Eelnõu § 1 punktiga 16 EUTS-i lisatavas § 6 lõikes 5 on pakutud digikukru pakkuja loa kehtivusajaks kuni 5 aastat ja seda tulenevalt eeldusest, et digikukkur on sertifitseeritud 5 aastaks vastavalt eIDAS määrusele.

Oleme seisukohal, et loa väljastamine kuni 5 aastaks seab küsimuse alla järelevalve ja loa menetluse proportsionaalsuse ja õigustatuse võrreldes teiste teenuseliikidega. Nii e-identimise kui ka usaldusteenuste puhul kehtib luba 2 aastat. Iseenesest ei pea olema loa andmine vaikimisi sünkroonis sertifitseerimisega.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Usaldusteenuste osas on varasemalt ettepanekuid tehtud loa menetluse (kui ka sertifitseerimistsükli) pikendamiseks vähemalt 3 aastani, kuna korduva vastavushindamise ja loa menetluskoormus on väga suur. Teeme ettepaneku kehtestada digikurku pakkuja loa kehtivusajaks 3 aastat.

3.2. Digikurku pakkumise ja usaldusteenuse loa taotlemine ning taotluses esitatavad andmed

Eelnõu § 1 punktidega 17-19 täiendatavas EUTS § 7 lõikes 3 on nõutud hulk uusi andmeid ja tõendeid taotluse esitamiseks, kuid need on halvasti defineeritud. Esitatavate andmete osas tekib küsimus, et kas need on vajalikud tegevusloa andmiseks ning kuidas nende sisu muutus mõjutab tegevusluba ja milliseks muutub teenuseosutaja halduskoormus.

Näiteks nõutakse EUTS § 7 lg 3 punktiga 1 lisaks muudele andmetele tegevusvoo skeemi. Mis see täpsemalt on ja mille kohta see käima peaks? Milline on suhe nõutud usaldusteenuse kirjeldusse ja kuidas mõjutab skeemi sisu muutus tegevusluba? Samuti on toodud selles punktis välja nõue esitada "sertifikaat selle olemasolu korral". **Palume täpsustada, mis laadi sertifikaadist jutt käib.**

EUTS § 7 lg 3 p 1^1 on nõutud põhjendatud järeldust usaldusteenuse ja selle osutaja vastavuse või mittevastavuse kohta. Vastavushindamise asutus väljastab vastavalt eIDAS määruses, rakendusaktides, rahvusvahelistes ja ETSI standardites reguleeritud ning akrediteerimisasutuse kinnitatud vormis vastavushindamise aruande ning usaldusteenuse vastavussertifikaadi. Selles ei esitata eelnõus kirjeldatud laadi "koondjäreldust". **Palume see punkt viia vastavusse vastavushindamise nõuete ja standarditega.**

EUTS § 7 lg 3 p 1^1 NIS2-st tulenevate nõuete hindamine toimub eIDAS määruse kohaselt. Eesti seadus ei muuda seda asjaolu ega pea seda eraldi välja tooma. Lisaks tekitab küsimusi, milline peab olema audiitori pädevus selles osas. EIDAS määruse alusel on audiitori pädevus määratud.

EUTS § 7 lg 3 p 1^1 ja § 7 lg 3 p 3 esitavad lisanõudeid võrreldes senisega. EIDAS määruse alusel kontrollitakse ka NIS2 nõuetele vastavust ning kohustuslikuks rakendamiseks NIS2 alusel vastu võetud Euroopa Komisjoni rakendusmääruses on selged nõuded riskianalüüsi(de) loomisele ja uuendamisele, intsidentide mõju tõlgendamisele ja menetlemisele. **Arusaamatu on, milleks need tuleb loa taotlemisel eraldi esitada järelevalvele.** Järelevalve võib alati küsida neid, kui tekib täiendavaid küsimusi või kahtlusi. Samuti tekitab see küsimuse, kui vastavat riskianalüüsi uuendatakse, kas siis tuleb ka uuesti luba taotleda või teavitada asjaolude muutumisest? See oleks ebaõiglane koormus usaldusteenuse/kurku pakkujate suhtes, kuna riskianalüüsi tuleb hoida asjakohasena.

EUTS § 7 lg 3 punktile 4 vastavalt tuleb esitada tõend kehtiva vastutuskindlustuse kohta. Seda kontrollib audiitor juba vastavushindamisel ning samuti on see märgitud vastavushindamise andesse. Miks peaks selle järelevalvele eraldi esitama?

4. Rollide defineerimise ja vastutuse küsimused

4.1. Digikukruteenuse pakkuja registreerimisasutuse (Registration Authority, RA) roll ei ole defineeritud

Tänase ID-kaardi puhul on mudel Politsei- ja Piirivalveamet (PPA) – sertifikaadi väljaandja (Certification Authority, CA) – sertifikaat, digikukru puhul aga PPA – Rahvastikuregister – isikuidentifitseerimise andmete (Person Identification Data, PID) pakkuja – digikukru pakkuja. **Kes otsustab uues mudelis PID peatamise, PID tühistamise ja digikukru peatamise?** ITL-i hinnangul on seda vaja kindlasti täpsustada, sest see tekitab täiendava riski potentsiaalse intsidendi vastutuse hindamisel.

4.2. Turvaintsidentide mõiste ja digikukru pakkuja vastutuse ebaselgus

Seletuskirja järgi peab digikukru pakkuja raporteerima turvaintsidente, mille mõiste on laiem kui küberintsident. Näitena tuuakse välja auditeeritud protsessi rikkumine. Samal ajal ei ole selge, kus lõpeb digikukru pakkuja vastutus ja kus algab PPA või mõne muu identiteedi allika vastutus. Kui seadus seda ei täpsusta, jääb märkimisväärne tõlgendamisruum järelevalvele.

5. Tuginevate isikute registreerimise kohustus

5.1. Seletuskirja täpsustamine ja kooskõla eIDAS2 määrusega

Teeme ettepaneku täpsustada seletuskirja peatükis „Peamised sihtrühmad“ (lk 14) toodud punkti 3 sõnastust, et see oleks kooskõlas eIDAS2 artikli 5f lõikega 2 ning väldiks võimalikku eksitavat tõlgendamist. Praegusest sõnastusest võib jääda mulje, et aktsepteerimiskohustus laieneb üldiselt kõigile panganduse, finantsteenuste, side, transpordi, energeetika, tervishoiu ja hariduse valdkonna ettevõtjatele. eIDAS2 kohaselt laieneb kohustus siiski üksnes neile erasektori tuginevatele isikutele, kellelt õigusakti või lepingulise kohustuse alusel nõutakse veebis tugevat kasutaja autentimist.

Teeme ettepaneku sõnastada peamiste sihtrühmade (lk 14) punkt 3 järgmiselt:

„3) *erasektori tuginevad isikud, kellelt õigusakti või lepingulise kohustuse alusel nõutakse veebis tugevat kasutaja autentimist, muu hulgas panganduse, finantsteenuste, side, transpordi, energeetika, tervishoiu ja hariduse valdkonnas, välja arvatud mikro- ja väikeettevõtjad, kes on aktsepteerimiskohustusest vabastatud*.“

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Muudatus ei muuda seletuskirja sisu, vaid viib selle sõnastuse paremini kooskõlla eIDAS artikli 5f lõikega 2 ning sama seletuskirja teistes osades juba kasutatud terminoloogiaga.

5.2. **Tuginevate isikute register**

Eelnõuga nähakse ette tuginevate isikute registri loomine. Kas on kaalutud võimalust korraldada tuginevate isikute registreerimine olemasoleva registri, näiteks äriregistri, kaudu, selle asemel et luua eraldiseisev register? ITL hinnangul võiks olemasolevate riiklike registrite kasutamine vähendada halduskoormust ning vältida dubleerivate registrilahenduste loomist.

6. Erasektorit puudutavate kohustuste tähtajad

Juhime tähelepanu erasektorit puudutavate kohustuste rakendamise tähtaegadele. Seletuskirjast nähtub, et kohustatud isikute jaoks on vajalikud mitmed riiklikud eeldused, sealhulgas tuginevate isikute registri loomine, registreerimiskorra kehtestamine, pääsusertifikaatide väljastamise korraldus ning muud digikukru ökosüsteemi toimimiseks vajalikud tugilahendused. Samuti on seletuskirjas märgitud, et osa vastavaid lahendusi valmib alles 2026. aasta lõpus või 2027. aastal.

Seetõttu peame oluliseks rõhutada, et erasektori kohustatud isikutel peab pärast nende eelduste tegelikku valmimist olema mõistlik aeg süsteemide analüüsimiseks, arendamiseks, testimiseks ja kasutuselevõtuks. Vastasel juhul võib tekkida olukord, kus õigusaktist tulenevad kohustused rakenduvad enne, kui nende täitmiseks vajalikud tehnilised ja menetluslikud eeldused on loodud.

Teeme ettepaneku täiendada seletuskirja selgitusega, et kohustuste rakendamisel ja järelevalve teostamisel tuleb arvestada ka riigi poolt vajalike tehniliste ja organisatsiooniliste eelduste tegeliku valmimise ajaga. Ettevõtjatele peab pärast nende eelduste valmimist jääma mõistlik aeg lahenduste arendamiseks, testimiseks ja kasutuselevõtuks ning ettevõtjate valmisoleku hindamisel tuleb seda samuti arvesse võtta.

Mingil juhul ei tohi ettevõtjate suhtes rakendada järelevalvemeetmeid ega käsitada kohustuste mittetäitmist rikkumisena olukorras, kus kohustuste täitmiseks vajalikud riiklikud eeldused ei ole õigeaegselt või täiel määral valminud.

7. Sunniraha ülemmäära vähendamine

eIDAS 2 artikli 16 eesmärk on sätestada rikkumiste eest kohaldatavate haldustrahvide maksimaalne määr, milleks on kuni 5 miljonit eurot või juriidilise isiku puhul 1% eelneva majandusaasta ülemaailmsest käibest. Tegemist on karistusõigusliku meetmega, mis peab olema tõhus, proportsionaalne ja hoiatav.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Eelnõus on aga sama suur ülemmäär ette nähtud ka sunnirahale (eelnõu § 1 punktiga 41 lisatav EUTS § 23^1). See ei ole põhjendatud, kuna sunniraha olemus erineb haldustrahvist. Sunniraha ei ole karistus, vaid haldussunni meede, mille eesmärk on motiveerida adressaati ettekirjutust täitma. Seetõttu peaks ka sunniraha ülemmäär olema proportsionaalne selle eesmärgiga ega peaks olema võrdsustatud maksimaalse haldustrahvi määraga.

Leiame, et maksimaalse haldustrahviga samaväärse igakordse sunniraha kehtestamine ei ole põhjendatud ning võib kaasa tuua ebaproportsionaalse haldussunni kohaldamise. **Palume kaaluda § 23^1 muutmist selliselt, et sunniraha ülemmäär oleks kooskõlas selle meetme eesmärgi ja olemusega.** Näiteks võib võtta eeskuju hiljuti NIS2 direktiivi ülevõtmiseks muudetud küberturvalisuse seadusest, kus maksimaalne trahv on direktiivist tulenevalt 7 miljonit eurot, kuid sunniraha oluliselt madalam (70 000 eurot).

8. Ettepanekud regulatsiooni ülesehituse ja õigusselguse parandamiseks

8.1. Digikukru regulatsiooni paigutus seaduses

Teeme ettepaneku paigutada digikukrut reguleerivad sätted EUTS-is eraldi peatükki. See muudaks seaduse ülesehituse selgemaks ning koondaks sisuliselt seotud regulatsiooni ühte kohta, hõlbustades nii seaduse mõistmist kui ka rakendamist.

Praeguse eelnõu kohaselt on digikukru pakkujat käsitlevad sätted koondatud samasse peatükki usaldusteenuste ja usaldusteenuse osutajate regulatsiooniga. Selline lahendus ei ole seaduse süsteemsuse seisukohalt põhjendatud, kuna digikukru regulatsioon on olemuslikult tihedamalt seotud e-identimise kui usaldusteenustega.

Praegune regulatsiooni ülesehitus võib tekitada ka õigusselgusetust. Näiteks on usaldusteenuseid reguleeriva EUTS peatüki § 7 lõike 3 punktis 5 loa taotlemise üldnõuete hulgas sätestatud digikukru pakkujale kohalduvad nõuded. Sättest ei nähtu aga üheselt, et need nõuded kohalduvad üksnes digikukru pakkujale, mistõttu võib jääda mulje, et need laienevad kõigile loa taotlejatele. See näide kinnitab, et digikukrut käsitlev regulatsioon tuleb koondada eraldi peatükki.

Kui eraldi peatüki loomist ei peeta võimalikuks, tuleks digikukrut käsitlevad sätted paigutada e-identimist reguleerivasse peatükki.

8.2. Isikukoodi digikukrusse kandmise reguleerimine seaduse tasandil

Palume kaaluda täiendavalt, kas eelnõu § 1 punktiga 13 EUTS-i lisatavas § 5 lõikes 11 sätestatud nõuet on vajalik reguleerida seaduse tasandil. Sätte kohaselt peab digikukru pakkuja kandma digikukrusse lisaks komisjoni rakendusmääruses (EL) 2024/2977 nõutud kohustuslikele isikutuvastusandmetele ka kasutaja isikukoodi.

Juhul kui Euroopa Liidu õigus jätab liikmesriigile selles küsimuses kaalutlusruumi, võiks kasutaja isikukoodi digikukrusse kandmise otsustamine jääda pädeva asutuse otsustada, mitte olla sätestatud seaduses.

8.3. **Loa andmisest keeldumise aluste kattuvus**

Teeme ettepaneku jätta eelnõu § 1 punktiga 24 EUTS-i lisatava § 9 lõike 1 punkt 4 eelnõust välja. Leiame, et § 9 lõike 1 punkt 4 on üleliigne, kuna selles sätestatud alus on juba hõlmatud § 9 lõike 1 punktiga 1.

Loa andmisel on määrav, kas taotleja, tema osutatav usaldusteenus või digikukkur vastab õigusaktides sätestatud nõuetele. Kui vastavushindamise või sertifitseerimise hindamise aruandes esinevad puudused mõjutavad hinnangut nõuetele vastavuse kohta, on loa andmisest võimalik keelduda juba § 9 lõike 1 punkti 1 alusel. Kui aruandes esinevad puudused nõuetele vastavuse hinnangut ei mõjuta, ei peaks need iseseisvalt olema loa andmisest keeldumise aluseks.

Lisaks on mõiste „olulised vastuolud“ ebaselge ega võimalda üheselt kindlaks teha, millistel juhtudel võiks sellele tuginedes loa andmisest keelduda. Seetõttu ei suurenda eelnõuga lisatav punkt 4 õigusselgust, vaid loob täiendava määratlemata keeldumise aluse. Õigusselguse põhimõttest (Põhiseadus § 10 ja § 13 lõige 2) tulenevalt peab loa taotlejale olema ettenähtav, milliste konkreetsete asjaolude esinemisel võib loa andmisest keelduda. Käesoleval juhul on see eesmärk juba saavutatud EUTS § 9 lõike 1 punktiga 1, mistõttu puudub vajadus täiendava, sisuliselt kattuva keeldumise aluse sätestamiseks.

8.4. **Sertifikaadi kehtetuks tunnistamise aluste ammendavus**

Teeme ettepaneku jätta eelnõust välja eelnõu § 1 punktiga 37 EUTS-i lisatava § 19 lõike 4 punkt 16. Leiame, et § 19 lõike 4 punktides 1–15 on sertifikaadi kehtetuks tunnistamise alused ammendavalt reguleeritud. Eelnõus sisalduv § 19 lõike 4 punktis 16 sätestatud üldine alus ei lisa regulatsioonile sisuliselt midagi, kuid võimaldab tunnistada sertifikaadi kehtetuks ka selliste nõuetele mittevastavuste korral, millel puudub sisuline mõju sertifikaadi usaldusväärsusele või nõuetele vastavusele. Selline regulatsioon ei ole kooskõlas proportsionaalsuse põhimõttega, kuna ei erista olulisi rikkumisi ebaolulistest.

Kui EUTS § 19 lõike 4 punkti 16 eelnõust välja jätmist ei peeta võimalikuks, teeme alternatiivselt ettepaneku sõnastada EUTS § 19 lõike 4 punkt 16 järgmiselt:

„16) sertifikaadi väljastamise järel ilmnenud asjaolu, et sertifikaadi väljastamine ei vastanud usaldusteenuse osutamise loa tingimustele või Euroopa Parlamendi ja nõukogu määruses (EL) nr 910/2014 või käesolevas seaduses sätestatud nõuetele ning sellel on sisuline mõju sertifikaadi usaldusväärsusele või nõuetele vastavusele.“

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Antud sõnastus seob sertifikaadi kehtetuks tunnistamise üksnes sellise nõuetele mittevastavusega, mis mõjutab sisuliselt sertifikaadi usaldusväärsust või nõuetele vastavust, ning väldib olukordi, kus sertifikaat tunnistatakse kehtetuks ebaoluliste või vähese mõjuga rikkumiste tõttu.

Loodame, et leiate võimaluse ITL-i ettepanekuid eelnõu edasises menetluses arvestada. Oleme valmis neid ka suuliselt selgitama.

Lugupidamisega

/allkirjastatud digitaalselt/

Doris Põld
Tegevjuht

Keilin Tammepärg, keilin.tammeparg@itl.ee