E-identimise ja e-tehingute usaldusteenuste seaduse, riigilõivuseaduse ja karistusseadustiku muutmise seaduse eelnõu seletuskirja juurde

Lisa 3
Eelnõu kooskõlastustabel

E-identimise ja e-tehingute usaldusteenuste seaduse, riigilõivuseaduse ja karistusseadustiku muutmise seaduse eelnõu kooskõlastustabel

ID	Asutus	Asutuse kommentaar/tagasiside	JDM seisukoht
1.	**Sise-ministeerium**	Eelnõu § 1 punktiga 5 muudetakse e-identimise ja e-tehingute usaldusteenuste seaduse (edaspidi EUTS) § 3 lõiget 2, mille kohaselt võib pädev asutus korraldada usaldusteenuse infrastruktuuri loomise, haldamise ja ajakohastamise vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 46b lõikele 5. Eelnõu seletuskirja punktides 6 ja 6.6 on mainitud, et Riigi Infosüsteemi Amet (edaspidi RIA) teostab järelevalvet ning korraldab Euroopa digiidentiteedikukru (edaspidi digikukkur) hankemenetluse. Leiame, et antud kontekstis võib termin „pädev asutus“ olla liiga lai, mistõttu palume eelnõus täpsustada või seletuskirjas avada pädeva asutuse rollide lahususe temaatika, arvestades, et RIA, kui pädeva asutuse roll on olla digikukru teenusepakkuja üle järelevalvet teostav sõltumatu asutus, kes samas korraldab digikukru hanget ja haldab selle infrastruktuuri. Ühtlasi palume välja tuua, kuidas suhestub antud regulatsiooniga PPA roll, kes korraldab usaldusteenuse hankeid isikut tõendavate dokumentide (ID-1 dokumendid) väljaandmise kontekstis.	**Arvestatud,** seletuskirja täiendatud. Selgitame täiendavalt, et pädeva asutuse roll tuleneb EIDAS2 määruses liikmesriigile määratud erinevate kohustuste täitmisest. Selgitame täiendavalt, et seaduses sätestatakse üldised rollid. Digikukru detailsem rollijaotus on läbi räägitud ja kokku lepitud töörühma tasandil (nt digiidentiteedi juhtrühmas mh 19.06.2024 ja 16.07.2024).
2.		Eelnõu § 1 punktiga 6 lisatava § 3^1 kohaselt luuakse digiidentiteedikukrule tuginevate isikute register, kuhu registreeritakse Eestis asutatud isikud, kes kavatsevad tugineda Euroopa digiidentiteedikukrule avalike või erateenuste osutamiseks. Seletuskirja punktis 6.3 on märgitud, et kõik digikukrule tugineda	**Arvestatud.** Seletuskirja täiendatud selgitusega, et kõik need, kes peavad digikukrut oma e-identimist nõudvates e-teenustes aktsepteerima, peavad end registreerima digikukrule tuginevate isikute

		soovivad ettevõtjad peavad end registreerima kukrule tuginevate isikute riiklikus registris, kuid avaliku sektori asutuste, sealhulgas kohaliku omavalitsuse üksuste ja riigiasutuste registreerimise praktiline korraldus ei ole sama selgelt kirjeldatud. Samas tuleneb seletuskirja punktist 6.6, et avaliku sektori asutused peavad digikukrut oma e-identimist nõudvates e-teenustes aktsepteerima ning valdavalt toimuks see TARA kaudu. Palume seletuskirjas täpsustada, kas ja millisel juhul peab avaliku sektori asutus, kohaliku omavalitsuse üksus või Regionaal- ja Põllumajandusministeeriumi valitsemisala asutus end iseseisvalt registreerima kukrule tugineva isikuna või kas TARA kui keskse autentimisteenuse kasutamisel toimub registreerimine keskse vahendaja kaudu. Samuti palume selgitada, kuidas kajastatakse registris vahendaja kasutamist ja vahendussuhet olukorras, kus avaliku sektori teenuse osutaja kasutab autentimiseks riigi keskset autentimisteenust. Selline täpsustus on vajalik, et avaliku sektori asutustel ja kohaliku omavalitsuse üksustel oleks õigel ajal selge, millised registreerimis-, teavitamis- ja andmete ajakohastamise kohustused neile digikukru kasutuselevõtuga kaasnevad.	riiklikus registris See hõlmab ka avaliku sektori asutusi, sealhulgas kohaliku omavalitsuse üksuseid ja riigiasutusi. Tänane kavatsus on TARA tänased kliendid registreerida ühekordselt võimalikult lihtsalt RP registrisse, et avaliku sektori asutustel oleks sellega seotud võimalikult väike halduskoormus.
3.		Eelnõu § 1 punktiga 7 täiendatakse seadust §-ga 4^1, milles kehtestatakse turvaintsidentide teavitamise regulatsioon. Selle lõike 1 kohaselt teavitab digikukru pakkuja või usaldusteenuse osutaja pädevat asutust viivitamata turvaintsidendist, mis oluliselt mõjutab või võib mõjutada usaldusteenuse, digikukru või selle kaudu osutatava teenuse turvalisust, töökindlust või usaldusväärsust. EUTS-is on kasutusel terminid „usaldusteenuse osutaja“ ja „kvalifitseeritud usaldusteenuse osutaja“, mille erisust ei ole välja toodud. Palume kontrollida, kas digikukru puhul peaks kasutama mõistet „kvalifitseeritud usaldusteenuse osutaja“.	**Selgitame,** et erinevus usaldusteenuse osutaja ja kvalifitseeritud usaldusteenuse osutaja vahel tuleneb eIDASest ja ei vaja seetõttu EUTSis dubleerimist. Kuna usaldusteenuse kvalifitseerituse staatust eelnõu ei täpsusta, on intsidentidest teavitamise kohustus nii kvalifitseeritud, kui ka kvalifitseerimata usaldusteenuse osutajatel. Täpsustame, et digikukru pakkuja ei ole usaldusteenuse pakkuja eIDAS tähenduses.
4.		EUTS § 5 lõige 3 kohaselt dokumenteerib kvalifitseeritud usaldusteenuse osutaja usaldusteenuse osutamisel tehtud toimingud ning säilitab sellekohast tegevuslogi kümme aastat kirje loomisest	**Arvestatud**, tegevuslogide säilitamise tähtaeg EUTS § 5 lõikes 3 muudetud 12 aastale.

		arvates. PPA soovib juhtida tähelepanu, et 2026. aasta kevadel läbi viidud eIDAS auditi raames andis audiitor hinnangu, et eIDAS määruse ja rahvusvahelise ETSI standardi[1] kohaselt peavad logid ja tõendid sertifikaatide kasutustingimustega nõustumise kinnituse kohta olema kättesaadavad kuni 12 aastat. Kvalifitseeritud sertifikaadi maksimaalne kehtivusaeg on kuni 5 aastat ja ETSI standardi kohaselt tuleb sertifikaatidega seotud sündmusi logida vähemalt 7 aastat pärast sertifikaadi kehtivuse lõppu. Tsiviilseadustiku üldosa seaduse (TsÜS § 146 lg 4) kohaselt on tahtliku rikkumise korral nõuete aegumistähtaeg kümme aastat. Kuna vaidlused võivad tekkida vahetult enne ja selle tähtaja piiril ning neile lisandub menetlusaeg, tagab 12 aastane logide puhver selle, et vajalikud tõendid ja logid (sertifikaatide kehtivusajad, sertifikaatide kasutustingimuste logid) on kohtuvaidluste tarbeks kättesaadavad. [1] ETSI EN 319 411-1 (OVR-6.4.6-01 ja REG-6.3.4-17)	
5.		Eelnõu § 1 punktidega 8–13 muudetakse EUTS paragrahvi 5, milles reguleeritakse nõuded kvalifitseeritud usaldusteenuse osutajale, usaldusteenuse osutamisele, digikukru pakkujale ja digikukru pakkumisele. Eelnõu seletuskirja kohaselt on digikukkur täiendav riiklik isikutuvastusvahend ID-kaardi ja teiste kehtivate eID vahendite kõrval. Riiklike isikut tõendavate dokumentide ja eID vahendite puhul on nende väljaandmise (sh taotlemine, väljastamine) ja kehtetuks tunnistamise põhimõtted ning kehtivusaeg õigusaktides reguleeritud. Digikukrule ei ole eelnõuga vastavat regulatsiooni ette nähtud ja inimestele ning digikurku pakkujale võib jääda selgusetuks, millised tingimused peavad olema digikukru puhul täidetud. Vastav regulatsioon, sh digikukru kehtivusaeg ei ole sätestatud ka eIDAS määruses. Digikukru pakkuja peaks teadma, kui kaua ta vastutab oma teenuse eest ja samuti on kasutajal oluline teada, mis tingimustel talle	**Selgitame,** et olukorras kus EL tasandil on digikukru ökosüsteem alles arenemas, ei peetud veel võimalikuks nende küsimuste sätestamist õigusaktides sellises detailsuses. Ka tulevikus kirjeldatakse enamus nendest küsimustes hanketingimustes ja/või teenuse poliitikas. Samas nõustume põhimõtteliselt selguse olulisusega ning ei välista tulevikus ka õigusmuudatuste vajalikkust.

		kukkur antakse. Samuti võiks olla õiguslikult reguleeritud, kas lapsevanem või eestkostja saab digikukru taotleda lapse või eestkostetava eest, kas digikukru saamisele kehtib vanusepiirang, mis on digikukru andmisest keeldumise alused, millal tunnistatakse digikukkur kehtetuks jne. Vastav regulatsioon tagaks õigusselguse, läbipaistvuse ja ka digikukru pakkumise järjepidevuse, mistõttu teeme ettepaneku kehtestada see siseriiklikus õiguses.	
6.		EUTS § 5 lõige 5 kohaselt tuvastab kvalifitseeritud usaldusteenuse osutaja enne kvalifitseeritud sertifikaadi väljastamist isikusamasuse Euroopa Parlamendi ja nõukogu määruses (EL) nr 910/2014 artikli 24 lõike (1a) alusel. Sama lõike punkti (d) puhul, kontrollib seda isikut tõendavate dokumentide seaduse (edaspidi ITDS) § 2 lõikes 2 nimetatud dokumendi, välisriigis väljastatud kehtiva reisidokumendi või isikut tõendavate dokumentide seaduse § 4 lõikes 1 sätestatud tingimustele vastava muu dokumendi alusel ning kontrollib esitatud teabe usaldusväärsust. Teeme ettepaneku parema arusaadavuse huvides määratleda, kas isikut tõendava dokumendi väljaandjal (PPA-l) on digikukru raames õiguslik kohustus väljastada kvalifitseeritud elektroonilisi atribuutide kinnitusi (QEAA), mis on kinnitatud ametliku elektroonilise pitseriga. Lisaks oleks oluline selgelt defineerida väljaandja vastutuse ulatus seoses võimalike süsteemitõrgetega, sealhulgas ekslike isikuandmete edastamise, kehtivuse ja kehtetuks tunnistamise staatuse teenuste ajutise või püsiva kättesaamise osas ning osapooli mõjutavate tehniliste katkestuste korral. Volituse ja vastutuspiiride selgesõnaline määratlemine tagab õiguskindluse, selgitades paremini ka riigi vastutust andmete õigsuse ja teenuse kättesaadavuse eest ning maandab võimalikest tehnilistest tõrgetest või andmeedastushäiretest tulenevaid riske.	**Selgitame**, et tänase arusaama kohaselt ei hakka PPA ise QEAA-ks. Küll aga hakkab Siseministeeriumi valitsemisala autentseks allika pakkujaks mõnede registrite osas (nt rahvastikuregister, ITDAK). Nõuded QEAA-dele on eIDASes ja rakendusaktides sätestatud ning on otsekohalduvad (ehk nende alusel saab ka järelevalvet teostada). Klientidega lepinguid sõlmides saab nendes katkestustega seotud kohustusi kirja panna. Riigi seisukohalt ei saa meie hinnangul sellisele teenusele sätestada toimepidevuse nõudeid, kui tegu pole elutähtsa teenusega.
7.		EUTS §-i 5 lisatakse lõige 11, mille kohaselt kannab digikukru pakkuja digikukrusse lisaks rakendusmääruses (EL) 2024/2977 nõutud kohustuslikele isikutuvastusandmetele ka digikukru kasutaja	**Arvestatud**, seletuskirja täiendatud. Digikukru skoobis on ainult Eesti isikukoodi omavad residendid, sh e-residendite toetamist

		isikukoodi. Palume eelnõus täpsustada, kas digikukrusse kantakse Eesti isikukood või võib see olla ka mõne muu riigi isikukood. Seletuskirjas on viidatud Eesti isikukoodile. Kuna isikukood ei ole kohustuslik andmeväli ja teiste riikide digikukrud ei pruugi isikukoodi sisaldada, siis kuidas sellise digikukruga Eesti teenustes isikuid tuvastatakse. Ka eelnõu seletuskirjas on öeldud, et kodanikud saavad võimaluse kasutada üleeuroopalist digiidentiteeti, mis isikukoodi abil sobitub Eesti e-teenustega. Palume isikukoodidega seonduvat seletuskirjas põhjalikumalt selgitada. Eelnõu seletuskirjas (vt eelpool toodud viidet) mainitakse läbivalt kodanikke. Palume täpsustada, kas kodanike all mõeldakse Eesti kodanikke või laiemalt eraisikuid.	hetkel ei ole planeeritud. Eestis planeeritakse kukrut pakkuda Eesti kodanikele ja residentidele, kuid mitte e-residentidele.
8.		EUTS §-i 5 lisatakse lõige 12, mis sätestab digikukru pakkuja õiguse teha isikutuvastusandmete digikukrusse kandmiseks ja nende ajakohasuse tagamiseks päringuid isikut tõendavate dokumentide andmekogusse (edaspidi ITDAK) ja rahvastikuregistrisse. Seletuskirjast ei selgu, milline isikuandmete töötlemise regulatsioon päringuga saadud isikuandmete osas pakkujale kohaldub, kas pakkujal on kohustus päringuga saadud andmed koheselt peale isikustamist kustutada või säilitatakse neid andmeid pakkuja poolt mingi perioodi jooksul. Palume hinnata, kas pakkuja poolset isikuandmete säilitamist tuleks reguleerida õigusaktis või piisab lepingus seatud kohustusest. Samuti palume selgitada isikuandmete ajakohasuse tagamise protsessi digikukru kasutamise vältel. Näiteks, millise ajaraami jooksul peab nime muutumise korral digikukru kasutaja isikuandmete ajakohasus tagatud olema, kelle kohustus see on ning kas selle täitmata jätmisel tunnistatakse digikukkur kehtetuks? Isikuandmete töötlemise põhimõtetest tulenevalt leiame, et eelnõus või vähemalt seletuskirjas peaks olema välja toodud, milliseid isikuandmeid digikukru andmiseks töödeldakse ja riiklikest andmekogudest küsitakse ning milline on nende andmete kasutamise õiguslik alus. Palume välja tuua nii siseriiklikud kui ka Euroopa Liidu	**Selgitame**, et andmetöötluseks on kavandatud, et digikukru pakkuja sõlmib lepingu andmeandjaga, kellega lepitakse kokku täpsed reeglid. Andmetöötlus toimub analoogiana ID-kaardi ning mobiil-ID-ga, kus erasektori teenusepakkuja töötleb isikuandmeid riigi tellimusel teenuse pakkumiseks. 1. ITDAK-st on planeeritud küsida teatud juhtudel isiku pilti. Õiguslik alus pildi töötlemiseks on andmetöötlusleping digikukru pakkuja ja andmeandja vahel ning EL komisjoni rakendusmääruse **(EL) 2026/1731** tabel 1 kooskõlas IKÜM Art 6 lg 1 p b-ga. 2. Rahvastikuregistrist on planeeritud küsida teisi EL rakendusmääruse **2026/1731** tabel 1-s loetletud isikuandmeid. Õiguslik alus on andmetöötlusleping ning RRS § 46 lg 2 p 2 kooskõlas IKÜM Art 6 lg 1 punktidega b ja c.

		õigusaktidest tulenevad alused ja täpne andmekoosseis. Seletuskirja kohaselt tuleneb rahvastikuregistrisse päringu tegemise vajadus digikukru kohustuslikust andmeväljast, milleks on sünnikoht. Samas ei ole välja toodud muid kohustuslikke andmeid, millest tulenevalt tekib samuti andmevahetusvajadus riiklike andmekogudega. Samuti palume lisada põhjenduse, mis eesmärgil on vaja teha päringuid ITDAK-isse ja lisada seletuskirja mõjude peatükki ka ITDAK-ile kaasnev mõju. ITDAK-i päringute mahu kasv omab olulist mõju ITDAK-i toimepidavusele tekitades täiendava koormuse. ITDAK-i töökindluse tagamine on riigi vaatest äärmiselt oluline, kuna ITDAK-i peamine eesmärk on avaliku korra ja riigi julgeoleku tagamine isikute tuvastamisel ja isikusamasuse kontrollimisel ning isikut tõendavate dokumentide väljaandmise teenuse tagamine. Selle tagamiseks võib ITDAK-i vastutav töötleja ITDAK-i põhimääruse § 152 lõige 6 kohaselt piirata kolmandatele isikutele andmetele juurdepääsu mahus, mis ei takista vastutavale töötlejale pandud ülesannete täitmist.	Selgitame täiendavalt, et kukru kasutamine on isikule vabatahtlik ning andmetöötlus toimub igakordselt tema algatusel. Lisaks kohustab EIDAS2 määrus kukrupakkujat võimaldama kasutajal valida, milliseid andmevälju ta soovib jagada e-teenusega. Päringute mahud mõlemasse andmekogusse on veel selgumisel. Lisaks selgitame, et andmepäringud nii ITDAk-isse kui RR-i on mõeldud ühekordsena PIDi väljastamisel ning salvestuvad digikukrusse isiku enda seadmes. Pildi edasisel kasutamisel võetakse pilt seadmest ning sellega ei kaasne koormust ITDAK-ile. Lisaks teadvustame ITDAK-i põhimääruse § 152 lõiget 6.
9.		Eelnõu § 1 punktiga 16 täiendatakse EUTS paragrahvi 6 lõikega 5, mis sätestab, et digikukru pakkumise luba kehtib kuni viis aastat. Palume selgitada kuidas mõjutab loa kehtivusaja lõppemine selle kehtivusajal välja antud digikukrute kasutamist.	**Selgitame,** et üldine põhimõte on sama mis usaldusteenuse osutajate puhul. Loa lõppemise ajaks peab olema uus kehtiv luba ja seejärel kehtivad väljastatud kukrud edasi. Kui mingil põhjusel uut luba ei väljastata, tunnistatakse kõik väljastatud kukrud kehtetuks.
10		Eelnõu § 1 punktiga 36 täiendatakse EUTS § 19 lõiget 2 punktiga 4, mille kohaselt tunnistab usaldusteenuse osutaja sertifikaadi kehtetuks, kui seda taotleb isikut tõendavate dokumentide väljaandja ITDS § 2 lõikes 2 nimetatud dokumendile kantud sertifikaatide osas ja samas seaduses sätestatud alustel. Viidatud ITDS-i sättes on loetletud ka isikut tõendavad dokumendid, millele kõnesolev EUTS-i regulatsioon ei peaks kohalduma (reisidokumendid). Palume sätet täpsustada, et see viitaks üksnes ID-1 formaadis dokumentidele, millele EUTS	**Arvestatud,** eelnõu § 1 punkti 36 (lisaks samadele sätetele viitavat punkti 38 muudetud selliselt, et viidatakse ITDS § 2 lõike 2 punktidele 1 – 1^2.

		kohaldub. Nendeks on ITDS § 2 lõige 2 punktides 1-1^2 nimetatud dokumendid. Palume eelnõu sellest tähelepanekust tulenevalt läbivalt üle vaadata.	
11		Eelnõu § 1 punktiga 38 muudetakse paragrahvi 19 lõiget 5, millega lisatakse usaldusteenuse osutajale kohustus teavitada enne ITDS § 2 lõikes 2 nimetatud dokumendile kantud sertifikaadi kehtetuks tunnistamist sellest isikut tõendava dokumendi väljaandjat. Palume seletuskirjas täpsustada, milliseid dokumendile kantud sertifikaate (vahe- ja juursertifikaate või isikusertifikaate) antud sättes käsitletakse, mis on selle teavitamise eesmärk. Kas väljaandja teavitamise all on mõeldud CRL teenust, kus info on kättesaadav või ligipääsu usaldusteenuse osutaja sertifikaatide andmetele? Isikusertifikaatide kehtetuks tunnistamisest teavitab usaldusteenuse osutaja dokumendi kasutajat, mitte selle väljaandjat. Termin „eelnev teavitamine“ või „enne kehtetuks tunnistamist teavitamine“ ei loo osapooltele õigusselgust, mis tähtaja jooksul enne kehtetuks tunnistamist tuleb teavitus saata, kas vahetult enne või tuleb jätta sinna vahele ajaline lõtk ning kas dokumendi väljaandjal võib tekkida selles osas vaidlustusõigus või võiks teavitamine toimuda ka kehtetuks tunnistamisel/selle järgselt (viivitamata)?	**Arvestatud. Seletuskirja täiendatud,** et mõeldud on isikusertifikaate, mitte juur- ega vahesertifikaate. Eesmärk on tagada, et dokumendi väljaandja saaks teha omapoolsed sammud sertifikaatide kehtetuks tunnistamise korral (nt on dokument varastatud ja sellest antakse teada usaldusteenuse osutajale ja ka füüsiline dokument tuleb kehtetuks tunnistada). Teavitamine võib toimuda ka tehniliste lahenduste kaudu. Tähtaja all on mõeldud mõistlikku aega, täpse tähtaja sätestamist ei peetud eelnõu koostamisel vajalikuks.
12		EUTS § 20 lõige 5 sätestab, et usaldusteenuse osutaja teavitab sertifikaadi kehtetuks tunnistamisest viivitamata sertifikaadi omajat. Käesoleva seaduse § 19 lõike 4 punktis 4 nimetatud juhul teavitab usaldusteenuse osutaja sertifikaadi kehtetuks tunnistamisest pärijat või surnuks tunnistamist taotlenud huvitatud isikut. Palume selgitada, kuidas usaldusteenuse osutaja teab, kes on pärija või huvitatud isik.	**Selgitame**, et antud küsimust eelnõu ei käsitle. Praktikas pöördub pärija surmatunnistuse ja pärimistõendiga usaldusteenuse osutaja poole ning palub usaldusteenuse konto kehtetuks tunnistada.
13		Eelnõu terminoloogia EUTS-is kasutatakse läbivalt terminit "sertifikaadi omaja", samas kui usaldusteenuse dokumentatsioonis (ID-1 dokumentide vaates) on kasutusel termin "sertifikaadi omanik". Mõisted on küll samatähenduslikud, kuid õigusselguse huvides võiks valdkondliku terminoloogia kasutamine olla ühetaoline ning võiks	**Selgitame,** et nõustume põhimõtteliselt mõistete ühtsuse kasulikkusega ning eelistame lahendust, kus usaldusteenuse dokumentatsioon viiakse kooskõlla seaduse mõistetega.

		otsustada, millist terminit eelistada tehes vastavad muudatused kas eelnõuga või usaldusteenuse dokumentatsioonis.	
14		Eelnõu §-iga 3 muudetakse karistusseadustiku § 350, mille kohaselt sätestatakse edaspidi tähtsa isikliku dokumendina ka e-identimise ja e-tehingute usaldusteenuste seaduse § 21[1] hindamise positiivselt läbinud e-identimise süsteemi e-identimise vahend ja digikukkur. ITDS-i muutmise EN (905 SE) kooskõlastamisel andis JDM soovituse kasutada terminit e identimisvahend, selgitades et kui kasutada tegusõna identima, saab loomulikumalt moodustada sõnaühendi või liitsõna: elektrooniliselt ehk e-identima > elektroonilise ehk e identimise vahend > e-identimisvahend. Soovitame selguse huvides ka siin kasutada sama terminit.	**Selgitame,** et eelnõu koostamisel on lähtutud EIDAS2 määruse ametlikust eestikeelsest tõlkest.
15		Rakendusaktid Hädaolukorra seaduse (edaspidi HOS) § 36 lõige 1 punkti 8 kohaselt on elektrooniline isikutuvastamine ja digitaalne allkirjastamine elutähtis teenus. HOS-i alusel kehtestatud määruse[1] kohaselt on elutähtsaks teenuseks elektrooniline isikutuvastamine ja digitaalne allkirjastamine isikut tõendavate dokumentide seaduse alusel välja antud dokumentidega elektroonilises keskkonnas isiku tõendamiseks, isikusamasuse kontrollimiseks ja digitaalallkirja andmiseks vajalike sertifikaatide kehtivusinfo kättesaadavuse tagamine isikut tõendavate dokumentide seaduse § 94 lõikes 31 nimetatud sertifitseerimisteenuse osutaja poolt. Leiame, et elutähtsa teenuse regulatsioon peaks laienema ka digikukrule, kuna tegemist on uue paralleelse riikliku eID vahendiga, mille kasutusele võtmine ja elutähtsa teenusena defineerimine aitab tõsta kriisideks valmisolekut ja e-riigi kerksust. [1] Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektroonilise isikutuvastamise ja digitaalse allkirjastamise tagamisel-Riigi Teataja	**Selgitame,** et nõustume põhimõttega, kuid antud küsimus pole selle eelnõu käsitlusalas.

16	**Regionaal- ja Põllumajandusministeerium**	Palume täiendavalt hinnata ja vajaduse korral täpsustada eelnõu § 1 punktiga 6 lisatava e identimise ja e-tehingute usaldusteenuste seaduse § 3^1 lõikes 1 sätestatud avalikustamise ulatust. Komisjoni rakendusmääruse (EL) 2025/848 artikli 3 lõike 4 kohaselt tuleb registreeringut omavate kukrule tuginevate isikute kohta teha internetis avalikult kättesaadavaks nimetatud määruse I lisas loetletud teave inim- ja masinloetaval kujul. Eelnõu § 3^1 lõike 1 sõnastus, mille kohaselt tehakse avalikult kättesaadavaks „nende kohta esitatud teave", on tõlgendatav laiemalt kui rakendusmääruses nõutud avalikustamise ulatus ning hõlmata ka andmeid, mille avalikustamine ei tulene Euroopa Liidu õigusest või millele võib kohalduda juurdepääsupiirang, sealhulgas isikuandmed, ärisaladus või turvalisusega seotud teave. Ka seletuskirja kohaselt tuleb põhimääruses eristada avalikustatav teave rakendusmääruse I lisa kohaselt juurdepääsupiiranguga andmetest, kuid selline eristus ei nähtu eelnõu tekstist. Seetõttu palume kaaluda sätte täpsustamist selliselt, et avalikult tehakse kättesaadavaks rakendusmääruse (EL) 2025/848 I lisas nimetatud teave ning muu teave üksnes juhul ja ulatuses, milles selle avalikustamiseks on selge õiguslik alus ja puudub juurdepääsupiirang.	**Osaliselt arvestatud.** Eelnõus andmetöötlust reguleerivasse §-i 3^1 lisatud uus lõige (5), mis täpsustab registrisse kantava teabe avalikustamise ulatust. Teabepiirangut vaikimisi eeldusena ei võimalda ette näha AvTS § 3 lõikes 2 viidatud avalikkuse põhimõte, mille järgi võib avalikule teabele juurdepääsu piirata vaid seaduses sätestatud korras. Sama põhimõte on sõnastatud ka eelnõus. Registri osas on tõenäolisemad näited selliseks teabepiiranguks teabe määramine ärisaladuse kaitse (AvTS § 35 lg 1 p 17) näiteks tugineva isiku klientide registrisse kandmisel ning eraelu kaitse (AvTS § 35 lg 1 p 12), näiteks (EL) 2025/848 artikli 3 lõike 4 alla mittekuuluvad isikuandmed.
17		Palume täpsustada ka eelnõu § 1 punktiga 6 lisatava e-identimise ja e-tehingute usaldusteenuste seaduse § 3^1 lõiget 2, mille kohaselt Riigi Infosüsteemi Amet kehtestab ja avalikustab oma veebilehel registrisse teabe esitamiseks korra. Seletuskirja punktis 8 on märgitud, et registri põhimääruses sätestatakse muu hulgas andmete esitamise ja registreeringu menetlemise kord ning et registreerimistaotluste esitamise tehniline kord tehakse kättesaadavaks tuginevate isikute registri kaudu põhimääruses sätestatud korras. Eelnõu tekstist selline piirang siiski ei nähtu. Kui RIA veebilehel avaldatav kord reguleerib üksnes tehnilisi küsimusi, nagu andmete esitamise vorming, kasutatavad kanalid, vormid või masinliidese tehniline kirjeldus, palume see seaduse tekstis selgelt	**Arvestatud.** Rakendusakti kavandisse lisatud eraldi paragrahv, "Andmete esitamise kord". Selgitame, et andmete esitamine toimub sarnaselt MTRi sisestatavate majandustegevusteadetega, ehk andmete esitamisel nende vastuvõtmisest ei keelduta. Küll võiks olla kirjas, mis aja jooksul RIA andmed üle vaatab ja vajadusel annab tähtaja andmete parandamiseks/täiendamiseks. Registreerimise tähtaega ega menetlemise

		selliselt piiritleda. Kui aga kord puudutab isikute õigusi või kohustusi, sealhulgas andmete esitamise tähtaegu, registreerimistaotluse menetlemist, puuduste kõrvaldamist, registreeringu tegemist, sellest keeldumist, muutmist, peatamist, tühistamist või registreeringu kehtivust, peab vastav regulatsioon olema sätestatud seaduses või seaduse alusel antavas ministri määrusega kehtestatavas registri põhimääruses. Haldusorgani veebilehel avaldatava korraga ei saa kehtestada isikutele õigusi ja kohustusi mõjutavaid üldnorme	tähtaega ei ole. Registreeringu tühistamise ja peatamise alus on EUTSi eelnõus juba olemas, seega seda määruses ei pea eraldi sätestama.
18		Täpsustamist vajab eelnõu § 3^1 lõigete 5 ja 6 sõnastus ning seletuskiri põhjenduste osas, milles käsitletakse registriandmete säilitamist. Komisjoni rakendusmääruse (EL) 2025/848 artikli 10 kohaselt säilitavad registripidajad kümne aasta vältel teavet, mille kukrule tuginevad isikud on esitanud ja mis on registreeritud vastavalt määruse I lisale kukrule tugineva isiku registreerimiseks ning kukrule tugineva isiku pääsusertifikaatide ja registreerimissertifikaatide väljastamiseks, sealhulgas selle teabe hilisemaid muudatusi. Eelnõu § 3^1 lõige 6 näeb seevastu ette, et kümme aastat pärast registrikande kehtetuks muutmist säilitatakse kõik „registrisse kantud või registriga seotud andmed". Selline sõnastus on rakendusmääruse artikliga 10 võrreldes oluliselt laiem, kuna võib hõlmata ka menetlusandmeid, kontaktisikute isikuandmeid, logisid, tehnilisi andmeid ja muud teavet, mille kümneaastane säilitamine ei tulene nimetatud rakendusmäärusest. Samuti ei ole eelnõus üheselt selge säilitamistähtaja alguspunkt ega selle seos rakendusmääruse artiklis 10 nimetatud teabega.	**Arvestatud.** Eelnõud ja seletuskirja täiendatud selliselt, et töödeldav teave eristatakse neljaks grupiks: 1) EL) rakendusmääruse (EL) 2025/848 artiklis 10 nimetatud andmed (isikuandmed ja muud andmed) - säilitatakse 10 aastat vastavalt rakendusmäärusele. 2) Muud isikuandmeid mittesisaldavad andmed - säilitatakse 10 aastat ühtseks toimimiseks muude kogutavate andmetega. Seaduseelnõus ei käsitleta, kuna puudub põhiõiguste riive. 3) Isikuandmeid sisaldavad logiandmed - säilitatakse 10 aastat. Selle eesmärk on võimalike intsidentide lahendamine (nt andmete väärkasutus, mis selgub aastaid hiljem). Intsidentide lahendamisel on vajalik alles hoida ka kõiki nende andmetega seotud tehnilisi andmeid (nt logid, kontaktisikute nimed ja muud menetlusandmed), kuna

			ka need andmed võivad intsidentide lahendamisel osutuda vajalikuks. Selgitame, et füüsiliste isikute kontaktandmed kustutakse kohe peale tugineva isiku poolt nende muutmist. 4) muud isikuandmed kustutatakse viivitamatult pärast tugineva isiku poolt nende muutmist.
19		Eeltoodust tulenevalt palume kaaluda, kas eelnõus tuleks eristada rakendusmääruse (EL) 2025/848 artiklis 10 nimetatud teave muudest registri pidamisega seotud andmetest ning sätestada kümneaastane säilitamistähtaeg üksnes nimetatud määruses ette nähtud ulatuses, kui pikema või laiema säilitamise vajadust ei põhjendata eraldi. Muude registriandmete, sealhulgas menetlus-, logi- ja tehniliste andmete säilitamise tingimused tuleks määrata lähtuvalt nende töötlemise eesmärgist ning isikuandmete puhul ka Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 artikli 5 lõike 1 punktides c ja e sätestatud võimalikult väheste andmete kogumise ja säilitamise piirangu põhimõtetest. Samuti palume täiendada eelnõu § 3^1 lõike 5 punktis 3 antud volitusnormi selliselt, et registri põhimääruses oleks võimalik selgelt reguleerida eri andmekategooriate säilitamise, arhiveerimise ja kustutamise täpsemad tingimused, nagu see on nõutav kõigi riigi andmekogude puhul, jäädes seejuures eelnõus ja rakendusmääruses sätestatud piiridesse.	**Arvestatud,** vt eelmist vastust.
20		Eelnõu § 1 punktiga 6 täiendatakse EUTS-i §-ga 3^1, milles kehtestatakse tuginevate isikute registri regulatsioon. Palume seletuskirjas täpsemalt ja näidete varal avada „tugineva isiku“ mõistet. Kas tuginevate isikute registri puhul on plaanis pärida andmeid ka rahvastikuregistrist? Kui jah, siis palume see rakendusakti kavandis välja tuua koos andmekoosseisuga. Osad asutused võivad digikukruga seonduvalt olla mitmes rollis, näiteks võib PPA täita nii isikutuvastusandmete andja kui tugineva isiku rolli.	**Selgitame,** et tuginevate isikute all mõeldakse asutusi ja ettevõtteid. Tuginevate isikute mõiste on defineeritud eIDASes ja eelnõu koostamisel ei peetud vajalikuks dubleerida seda seaduses. Kuidagi peab ütlema selle ka välja, et täpsemad detailid (kust ja mida päritakse) selgub hiljem töö käigus.

		Kas eelnõu väljatöötamisel on õiguslikult ja tehniliselt läbi mõeldud, kuidas on sellisel juhul korraldatud andmevahetus teiste riiklike registritega, sh isikuandmete töötlemise vastutuse ja andmetele juurdepääsu küsimused teenusepakkujatele ning andmesubjektidele? Selged õiguslikud määratlused on vajalikud, et vältida võimalikke andmeedastuse puudusi ja konflikte, kaitsta kasutajate põhiõigusi ning kontrollida õiguslikult ja läbipaistvalt digitaalsete volitustega tehtud toiminguid.	**Selgitame täiendavalt**, et tuginevate isikute registri puhul ei ole plaanis pärida andmeid rahvastikuregistrist.
21		Lisaks märgime, et seletuskiri ei ole kooskõlas eelnõu tekstiga. Seletuskirja § 1 punkti 6 selgituses on märgitud, et andmekogu pidamise eesmärk ja vastutav töötleja sätestatakse lõikes 1, säilitamistähtaeg lõikes 7 ning volitusnorm lõigetes 5 ja 6, kuid eelnõu tekstis on vastutav töötleja sätestatud lõikes 4, säilitamistähtaeg lõikes 6 ning lõige 7 käsitleb registreeringu peatamist ja tühistamist. Samuti on seletuskirja punktis 8 (rakendusaktid) märgitud, et registri põhimäärus kehtestatakse § 3^1 lõigete 5 ja 6 alusel, kuigi lõige 6 ei sisalda volitusnormi. Ka on seletuskirjas öeldud, et registri andmed on eelnõu § 3^1 lõike 4 kohaselt osalise juurdepääsupiiranguga, kuid eelnõu lõige 4 määrab üksnes andmekogu vastutava töötleja. Seetõttu ei selgu eelnõust üheselt, millised registriandmed on avalikud ja millistele kohaldatakse juurdepääsupiirangut. Palume eelnõu ja seletuskirja vastavalt parandada ning vajaduse korral lisada seadusesse selge regulatsioon avalikustatavate ja juurdepääsupiiranguga andmete eristamiseks.	**Arvestatud,** eelnõud ja seletuskirja parandatud.
22		Seletuskirja punktis 6.6 märgitakse, et kõik avaliku sektori asutused, sealhulgas kõik 78 kohaliku omavalitsuse üksust, peavad Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 5f lõike 1 kohaselt aktsepteerima Euroopa digiidentiteedikukrut nendes internetipõhistes teenustes, mille kasutamiseks nõutakse e-identimist ja e-autentimist. Samas on seletuskirja punktis 7.4 märgitud, et kohaliku omavalitsuse üksustele ei panda eelnõuga uusi iseseisvaid	**Arvestatud,** seletuskirja täiendatud. Vaata ka vastust ELVL ettepanekule.

		ülesandeid ega rahastamiskohustusi ning eelnõu rakendamisega ei kaasne neile lisakulusid, kuna digikukru tugi lisatakse riigi kesksesse autentimisteenusesse TARA. Palume seda hinnangut täpsustada, arvestades, et seletuskirja punktis 6.6 on samas märgitud, et asutused, kes keskset autentimisteenust ei kasuta, peavad oma autentimislahendused ise kohandama. Seetõttu ei pruugi väide, et kohaliku omavalitsuse üksustele lisakulusid ei kaasne, olla piisavalt põhjendatud juhul, kui mõni kohaliku omavalitsuse üksus või tema hallatav infosüsteem ei kasuta TARA-t või vajab digikukru kasutuselevõtuks täiendavaid arendusi, testimist, teenuseprotsesside muutmist või juhendamist. Palume seletuskirjas täpsustada, kas ja millises ulatuses on analüüsitud kohaliku omavalitsuse üksuste kasutatavaid autentimislahendusi. Kui kohaliku omavalitsuse üksustel võib siiski tekkida vajadus teha eraldi arendusi või korralduslikke muudatusi, palume seletuskirjas kirjeldada nende võimalikku mõju, kulude katmise allikaid ja rahastamise põhimõtteid või täiendada mõjuanalüüsi vastava selgitusega.	
23		Seletuskirja punktis 6.6 (mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele) on märgitud, et riiklike andmekogude pidajatele, kelle andmekogu kvalifitseerub autentseks allikaks, tekib kohustus võimaldada elektrooniliste tõendite kvalifitseeritud usaldusteenuse osutajatel kasutaja taotlusel kontrollida vähemalt määruse (EL) nr 910/2014 VI lisas loetletud atribuute, sealhulgas näiteks aadressi, vanust, kvalifikatsioone ja esindusõigusi. Regionaal- ja Põllumajandusministeeriumi valitsemisalas on mitmeid andmekogusid ja infosüsteeme, mille andmeid võidakse edaspidi kasutada Euroopa digiidentiteedikukru ökosüsteemis elektrooniliste tõendite või atribuutide allikana, sealhulgas regionaal-, põllumajandus- või toetuste andmetega seotud andmekogud. Seetõttu palume seletuskirjas täpsustada, milliseid riiklikke andmekogusid või andmekogude liike käsitatakse eelnõu ja eIDAS-raamistiku rakendamisel võimalike autentsete allikatena ning kas Regionaal- ja	**Selgitame,** et määruse (EL) nr 910/2014 lisa VI on seotud EIDAS2 määruse artikliga 45e, mis seostub vaid tõendite verifitseerimisega (spetsiifilistel juhtudel pabertõendist digitaalse tõendi tekitamine). Sellist vajadust Eestis tänase seisuga analüüsides pole tuvastatud.

		Põllumajandusministeeriumi valitsemisala asutustele võib sellest tuleneda täiendavaid tehnilisi, korralduslikke või rahalisi kohustusi.	
24		Palume täpsustada, kas seletuskirja punktis 7.2 nimetatud „digikukruga liidestuvate ministeeriumide“ kulude hinnang 2 000 000 eurot hõlmab ka Regionaal- ja Põllumajandusministeeriumi valitsemisala võimalikke arendusvajadusi, sealhulgas andmekogude liidestamist, andmekvaliteedi parandamist, liideste loomist või elektrooniliste tõendite väljastamise ja kontrollimise võimekuse tagamist. Kui vastavad kulud või kohustused tulenevad vahetult Euroopa Liidu õigusest ega ole käesoleva eelnõuga täiendavalt reguleeritud, palume seda seletuskirjas selgelt eristada ning kirjeldada, millises edasises menetluses või rakendusplaanis valitsemisalade ülesanded ja rahastamine täpsustatakse.	**Selgitame,** et nimetatud summa viitab üldisele hinnangulisele kuluvajadusele. Konkreetsete kulude hüvitamise taotleb iga ministeerium eraldi riigieelarve protsessis vastavalt riigieelarve reeglitele.
25	**Eesti Linnade ja Valdade Liit**	Seletuskirjas (lk 22) on märgitud, et „teenuste liidestamine digikukruga ja tõendite koostalitlusvõime tagamine on iga haldusala ülesanne" ning et Euroopa digiidentiteedi kukruga liidestuvate ministeeriumide (haldusalade) kulud on kokku 2 000 000 eurot. Seletuskirjast (lk 22) ei selgu, kuidas on vastav kulu välja arvutatud ning palume seletuskirja vastavalt täiendada. Euroopa digiidentiteedi kukruga liidestuvad ka omavalitsuste e-teenused, mistõttu on koostalitlusvõime tagamise kulu katmine põhjendatud ka omavalitsustele. Seletuskiri tunnistab (lk 22), et „asutused, kes keskset autentimisteenust ei kasuta, peavad oma autentimislahendused ise kohandama" ning mitmed omavalitsuste e-teenused TARA-t ei kasuta. Seetõttu on ekslik väita, et omavalitsuste „koormus piirdub keskse autentimisteenuse kaudu lisanduvate võimaluste kasutuselevõtuga“, sest ka TARA kasutuselevõtt on lisakulu. Kohandusi tuleb aga teha mitte ainult TARA-s ja SIGA-s, vaid ka omavalitsuste kasutatavates TARAga liidestatud infosüsteemides (nt SPOKU, ARNO jne), et autenditud EL kodanik saaks iseteeninduses toiminguid jätkata. Liidestatud infosüsteemil on alati kaks poolt: kui TARA tagastatav andmekoosseis muutub (nt kui isikukood ei ole enam kindel väli, sest	**Arvestatud,** seletuskirjas täpsemalt kirjeldatud mõjusid kohaliku omavalitsuse üksuste eelarvele. Selgitame, et kulud jaotuvad kolmeks eri kategooriaks: - TARA –ga (või ka SIGA jt digikukru kasutamisega seotud süsteemid) liitumisega seotud kulud, nende KOV –de puhul kes TARA jt täna veel ei kasuta - SPOKU, ARNO jt süsteemid, mis täna kasutavad eID lahendusi, teevad ise vajalikud kohandused digikukru toetamiseks, võivad aga küsida sellest tulenevalt lisatasu, tõsta hinda vms - Need KOV –d kes tahavad rohkem panustada üleliidulisse digitaalsesse ühisturgu, näiteks need kes täna juba kasutavad TARA –s EU eID võimalust, saavad nüüd suurema

		teise liikmesriigi kodanikul see puudub), tuleb sellega liidestatud infosüsteemi vastavalt kohandada. Kuna omavalitsused kasutavad teenuste osutamiseks laialdaselt erasektori pakutavaid infosüsteeme, kaasnevad sellega vähemalt analüüsikulud ning muudatuse korral ka arenduskulud. Osa teenusepakkujaid võib analüüsi- ja arenduskulu enda kanda võtta, kuid tavaliselt küsitakse selle eest omavalitsustelt eraldi tasu. Seega kaasneb kohalikele omavalitsustele täiendav kulu. Kuigi EL liikmesriikide kodanike autentimise võimekus on juba TARA-sse ehitatud, ei ole seni selle kasutamine ja oma infosüsteemide vastav kohandamine olnud omavalitsustele kohustuslik. Olemasolevad infosüsteemid ei pruugi olla võimelised vastu võtma näiteks Rootsi kodaniku andmekoosseisu, kellel puudub 11-kohaline isikukood. Paljud infosüsteemid eeldavad isikukoodi olemasolu, kuid TARA tehnilise kirjelduse (https://e-gov.github.io/TARA Doku/TehnilineKirjeldus) kohaselt tagastatakse autenditud kasutaja identifikaator (sub) väljal kas isikukoodi või eIDAS-identifikaatorina, mis võib olla kuni 256 tähemärki pikk ja mis esitatakse koos riigikoodi eesliitega. Seega ei pruugi olemasolev infosüsteem, mis on üles ehitatud Eesti isikukoodi formaadile, sellist identifikaatorit ilma kohandamiseta vastu võtta. Iga infosüsteemi pakkuja peab eelnõu rakendamisel analüüsima, kas süsteem saab jätkuda olemasoleval kujul või kaasnevad täiendavad arenduskulud. See oleneb konkreetse süsteemi ülesehitusest. Kokkuvõtvalt – Euroopa digiidentiteedi kukruga liidestatakse kohalike omavalitsuste e-teenused, mistõttu ei ole õige väita, et kohalike omavalitsuste koormus piirdub keskse autentimisteenuse kaudu lisanduvate võimaluste kasutuselevõtuga. Kohalike omavalitsuste e-teenuste liidestamine Euroopa digiidentiteedi kukruga ja tõendite koostalitlusvõime tagamine peab olema sarnaselt keskvalitsuse institutsioonidega täielikult riiklikult rahastatud. Palume seletuskirja vastavalt täiendada, tunnistades omavalitsuste koostalitlusvõime tagamise kulu samamoodi nagu haldusalade oma ning täiendades mõjuanalüüsi kohalike omavalitsuste	võimaluse kergemalt toetada rohkemate liikmesriikide eID läbi digikukru ja potentsiaalselt ka lisakulud sellega seotud. Muud kuludega seotud: - Need, kes TARA juba kasutavad, siis plaan on, et olemasolevad TARA kasutajad saavad ilma lisaarenduseta digikukru kohustusliku osa (PID kasutamine online) kasutusele võtta, analoogselt kuidas 2019 lisandus Smart-ID TARA –sse.

		infosüsteemide kohandamise kulude hinnanguga. Palume tagada riiklik rahastus.	
26		Eelnõu § 1 punkti 6 (e-identimise ja e-tehingute usaldusteenuse seadus § 3[1]) kohaselt tuleb digiidentiteedikukrule tuginevate isikute registrisse registreerida ka avalike teenuste osutajad. Seletuskiri ei selgita, kas iga omavalitsus peab end eraldi registreerima ja pääsusertifikaadid taotlema või korraldatakse see keskselt. Palume seletuskirjas seda täpsustada. Kuna individuaalne registreerimine tähendaks omavalitsustele täiendavat töökoormust, siis palume see keskselt korraldada.	Seletuskirja täiendatud selgitusega, et kõik need, kes peavad digikukrut oma e-identimist nõudvates e-teenustes aktsepteerima, peavad end registreerima digikukrule tuginevate isikute riiklikus registris See hõlmab ka avaliku sektori asutusi, sealhulgas kohaliku omavalitsuse üksuseid ja riigiasutusi. Tänane kavatsus on TARA tänased kliendid saada digikukrut kasutama võimalikult lihtsalt (sh RP registri toimingud), et avaliku sektori asutustel oleks sellega seotud võimalikult väike halduskoormus.
27		Samuti märgime, et RIA-l tuleb vähemasti Euroopa digiidentiteedi kukru rakendamise esimesel aastal pakkuda Euroopa digiidentiteedi kukru kasutajatele kasutajatuge, sest kodanikel võivad Euroopa digiidentiteedi kukru teenuse kasutamisel tekkida küsimusi või probleeme.	**Teadmiseks võetud**.
28		Juhime ka tähelepanu, et eelnõus on kasutatud nii mõistet „Euroopa digiidentiteedi kukkur“ kui ka „Euroopa digiidentiteedikukkur“ ning palume see ühtlustada.	**Arvestatud,** mõisted eelnõus ühtlustatud.

29	**Tarbijakaitse ja Tehnilise Järelvalve Amet**	Eelnõu § 1 punktis 22 viidatakse, et üheks eelduseks pädevalt asutuselt loa saamiseks on Euroopa digiidentiteedi kukru ja selle pakkuja Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (edaspidi eIDAS määrus) artikli 5c lõikele 1 vastava sertifitseerimise läbimine. Kõnealuses eIDAS määruse artikli 5c lõikes 1 viidatakse, et sertifitseerimine toimub eIDAS määruse artikli 5a nõuetele vastavuse hindamiseks. TTJA hinnangul on oluline ka sertifitseeringu vastavus eIDAS määruse artikli 5c lõigetes 2 ja 3 toodud sertifitseerimise kavadele, mistõttu oleks asjakohane viidata üldiselt eIDAS määruse artiklile 5c. Samuti võiks TTJA hinnangul olla selguse mõttes välja toodud asjaolu, et loa saamise eelduseks on üksnes kehtiv sertifitseering. Samuti juhime tähelepanu, et eIDAS määruse artikli 5c kohaselt sertifitseeritakse digiidentiteedi kukrut, mitte selle pakkujat. Eeltoodut arvestades teeme ettepaneku muuta eelnõu § 1 punkti 22 ning sõnastada see järgmiselt: *„Euroopa digiidentiteedikukkur on läbinud Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 5c kohase sertifitseerimise ja asjaomane sertifitseering on kehtiv;“*.	**Arvestatud osaliselt.** Eelnõu § 1 punkt 22 sõnastatud ümber selliselt, et kustutatud väljendid “ja selle pakkuja” ning "lõikele 1”. Samas selgitame, et loa saamise eelduseks ei ole vaid sertifikaat, Vaja on tasuda ka riigilõiv. Lisaks võib pädeval asutusel olla vajadus täiendava teabe küsimiseks või täpsustamiseks. Väljendit “ja asjaomane sertifitseering on kehtiv” ei lisata eelnõusse. Selle asemel täiendatakse seletuskirja selliselt, et nii digikukru kui usaldusteenuse loa taotlemisel peab esitatav sertifikaat olema kehtiv.
30		Eelnõu § 1 punktis 16 tuuakse välja, et loa olemasolu tõendab sertifitseeringu kehtivust. TTJA hinnangul ei pruugi loa olemasolu aga käesoleva eelnõu sõnastuses sertifitseeringu kehtivust tõendada. Sertifitseering kehtib eIDAS määruse artikli 5c lõike 4 kohaselt kuni viis aastat, tingimusel, et iga kahe aasta järel viiakse läbi nõrkuste hindamine. Säte toob täiendavalt välja, et kui tuvastatakse nõrkus ja seda ei kõrvaldata tähtaegselt, siis sertifitseering tühistatakse. Eelnõus toodud EUTS § 6 lõike 5 kohaselt kehtib aga pädeva asutuse luba igal juhul viis aastat. Eeltoodut arvestades teeme ettepaneku muuta eelnõu § 1 punkti 16 ning sõnastada see järgmiselt:	**Selgitame**, et eelnõu kohaselt kehtib luba kuni 5 aastat, ehk see on sarnaselt tänase usaldusteenuste regulatsiooni ja praktikaga alati kooskõlas sertifitseeringu kehtivuse tähtajaga. Kui sertifitseering mingil põhjusel kaotab kehtivuse, tunnistab pädev asutus ka tegevusloa kehtetuks. Sätte eesmärk ei ole kehtestada, et tegevusluba kehtib igal juhul ja alati 5 aastat.

		„(4) Euroopa digiidentiteedikukru pakkumiseks peab isikul olema kehtiv Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 5c kohane sertifitseering, mida tõendab asjaomane luba. *(5) Euroopa digiidentiteedikukru pakkumise luba kehtib sertifikaadi kehtivuse lõpuni, kuid mitte kauem kui viis aastat.*“.	
31	**Andmekaitse Inpektsioon**	Eelnõu § 1 p-ga 40 täiendatakse EUTS §-i 22 lg-ga 2 järgmises sõnastuses: „Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 5a lõike 4 punkti d alapunktis iii ja lõike 5 punkti a alapunktis x sätestatud pädeva riikliku andmekaitseasutuse ülesandeid täidab Andmekaitse Inspektsioon. Andmekaitse Inspektsioon teeb järelevalvet määruse artikli 46a lõike 4 punktis f sätestatud ülesannete täitmise üle.“ Sätte esimene lause on sisult asjakohane st digiidentiteedikukrud võimaldavad kasutajal andmete saamiseks saadetud väidetavalt ebaseadusliku või kahtlase taotluse korral hõlpsasti teatada tuginevast isikust pädevale riiklikule andmekaitseasutusele. Sisuliselt on tegemist teavituskanaliga, mille kaudu AKI saab teavet võimalikest andmekaitsealastest rikkumisest. Teate saamisel menetleb AKI seda tavapäraselt lähtudes IKÜM-i raamidest. Samas sätte esimene lause sisuliselt dubleerib juba kavandatava EUTS § 2 lg-s 3 sätestatut – mõlemad viitavad samadele eIDAS määruse (edaspidi määrus) sätetele ja annavad AKI-le sama rolli, mistõttu ei ole seda vajalik uuesti korrata. Probleemne on kavandatava EUTS § 22 lg 2 teine lause, mille kohaselt AKI teostaks järelevalvet määruse art 46a lg 4 p-s f sätestatud ülesannete täitmise üle. Säte üritab AKI-le anda ülesannet, mis eelnõu endaga on juba antud ainult RIA-le nii nagu seda määruses mõeldud ongi. Määruse art 46 a lg 4 p f sätestab, et lõike 1 kohaselt määratud järelevalveasutusel on ülesandeks mh peatada või tühistada tuginevate isikute registreerimine ja kaasamine art 5b lg-s 7 osutatud mehhanismi Euroopa digiidentiteedikukru ebaseadusliku või petturliku kasutamise korral. Esmalt, määruse art 46a lg 1 kohaselt	**Arvestatud.** Eelnõust eemaldatud viide AKI järelevalvele määruse artikli 46a lõike 4 punktis f sätestatud ülesannete täitmise üle ning dubleeriv viide.

		määratud järelevalveasutuseks ehk pädevaks asutuseks on ainult RIA (vt kavandatav EUTS § 2 lg 1)1 ehk kõiki määruse art 46a nimetatud järelevalveasutuse ülesandeid saab täita ainult RIA. Seega ei ole AKI järelevalveasutus määruse art 46a tähenduses ega saa kuidagi teostada järelevalvet määruse art 46a ükskõik millise lõike või punkti osas. Eelnõu seletuskirja lisas 2 toodud vastavustabelis on teisel real AKI roll rakendava riigisisese sättena õigesti märgitud EUTS § 2 lg 3, kuid asjakohatult on märgitud lisaks juurde EUTS § 22 lg.	
32		Seda kinnitavad ka samal real olevad EL-i õigusakti sätted, mis räägivad AKI rollist, mitte järelevalvepädevuse määramisest nagu ekslikult sama rea kommentaaris on märgitud. AKI täidab pädeva riikliku andmekaitseasutuse rolli, mitte määruse üle järelevalvet teostava järelevalveasutuse rolli (vt kavandatav EUTS § 2 lg 3). Eelnõus on pädeva asutuse ja pädeva andmekaitseasutuse rollid seoses pädeva asutuse ühe ülesandega kokku liidetud ja segamini aetud. AKI teostab järelevalvet andmekaitsealaste normide üle IKÜM raamistikus ja määruse üle teostab järelevalvet siiski ainult RIA (sh on ta EUTS-is nimetatud ka ainsana kohtuväliseks menetlejaks). Küll aga peab olema määruse kohaselt tagatud, et AKI-le oleks võimalik esitada hõlpsasti teateid võimalike andmekaitsealaste rikkumiste kohta, mis on seotud digiidentiteedikukru ebaseadusliku või petturliku kasutamise kahtlusega. RIA kui pädeva asutuse üheks ülesandeks on mh teha koostööd AKI-ga ning teavitada AKI-t võimalikest isikuandmetega seotud rikkumistest (määruse art 46a lg 4 p g). Teisalt ei saa AKI pädevuse puudumise tõttu ka peatada või tühistada tuginevate isikute registreerimist ja kaasamist, sest selline pädevus on pädeva asutusena samuti ainult RIA-l (vt kavandatav EUTS § 2 lg 1 ja 31 lg 7). Lisaks ei ole AKI-l pädevust tuvastada määruse art 46a lg 4 p-s f nimetatud „ebaseaduslikku või petturlikku kasutamist“, mis on juba oma olemuselt laiem mõiste kui isikuandmetega seotud rikkumine ja hõlmab endas ka muid rikkumisi (nt volitamata kasutus vms), mis ei kujuta endast IKÜM-i rikkumist.	**Arvestatud.** Vaata ka eelmist vastust.

33		Eelnõu seletuskirja p-s 7.2 kajastatud AKI aastane lisavajadus on kooskõlas AKI tegeliku, IKÜM raamistikuga seotud koormuse kasvuga, mis tuleneb kasutajate (andmesubjektide) esitatud digikukruga seotud teadete menetlemisest kahtlaste või ebaseaduslike andmepäringute kohta, mida AKI hindab oma tavapärase pädevuse piires. Lisavajaduse suhteliselt tagasihoidlik suuruski viitab, et AKI-le ei ole määruse mõttes kavandatud iseseisvat määruse üle järelevalvet teostava asutuse rolli koos sellega kaasneva lisavajadusega. Juhul kui seadusandja sooviks siiski määrata Eestis määruse art 46a tähenduses mitu järelevalveasutust (nt osaliselt mõne ülesande osas RIA ga kõrvuti ka AKI), tuleks see selgelt eelnõus välja tuua ning kehtestada selleks vajalikud normid. Sellisel juhul oleks AKI tegelik lisavajadus praegu kavandatust oluliselt suurem. Lisaks tuleb arvestada, et määruse art 46a lg-s 3 kirjeldatud järelevalveasutuse rollid moodustavad ühtse, omavahel seotud terviku, millest art 46a lg-s 4 nimetatud üksikuid ülesandeid ei saa sisuliselt lahus käsitleda. Näiteks selle sama kõnesoleva määruse art 46a lg 4 p-s f toodud ülesande täitmine eeldab paratamatult ligipääsu ja arusaamist laiemast kontekstist – pakkuja tegevusloa tingimustest, vastavushindamise tulemustest, tehnilisest infrastruktuurist jms – mida haldab RIA. Juhul kui AKI määrataks järelevalveasutuseks kitsalt määruse art 46a p-i f ulatuses, peaks AKI selle ülesande täitmiseks sisuliselt dubleerima osa RIA-l olemasolevast järelevalvevõimekusest, mis ei ole otstarbekas ega ka kooskõlas RIA ja AKI rollidega. RIA-le seatud ülesannete osas saab AKI vajadusel anda andmekaitsealast sisendit (vt nt määruse art 20 lg 3b). Seega ei ole AKI määruse ega EUTS-i täitmise üle järelevalve teostajaks ega peaks seetõttu olema ka EUTS §-s 22 nimetatud järelevalveasutus. AKI töökoormus suureneb digikukru ja sellega seotud töötlemistoimingute andmekaitsealase järelevalve võrra, kuid seda siiski vastavalt IKÜM i ja IKS-i raamistikule. Kokkuvõttes tuleb kavandatav EUTS § 22 lg 2 eelnõust tervikuna välja jätta ning	**Arvestatud,** eelnõud muudetud.

		seetõttu pole vajalik sellega seotult ka eelnõu § 1 p-s 39 nimetatud muudatus.	
34		Teabevahetus ja aruandlus Eelnõu § 1 p-ga 43 täiendatakse EUTS § 234 lg 1 järgmiselt: „Valdkonna eest vastutaval ministeeriumil, pädeval asutusel ja Andmekaitse Inspektsioonil on õigus nõuda Eesti jurisdiktsiooni alla kuuluvalt Euroopa Parlamendi ja nõukogu määruses (EL) nr 910/2014 sätestatud teenuse osutajalt määruse artikliga 48a pandud ülesannete täitmiseks vajalikku teavet.“ Sisuliselt kordub sama põhimõtteline probleem. Määruse art 48a pandud ülesanded on kavandatava EUTS § 2 lg 1 kohaselt RIA ainupädevuses. Seletuskirja lisas 2 olevas vastavustabelis on määruse art 48a kajastatud kahel korral. EUTS § 234 peaks olema üksnes menetluslik teabe nõudmise mehhanism asutuse jaoks, kellele on pandud sisuline ülesanne täita määruse art-t 48a (RIA). Kuna AKI ei täida määruse art-ga 48a pandud ülesandeid, siis ei ole vajalik ega saa ka AKI le anda õigust nõuda teenuse osutajalt nimetatud ülesande täitmiseks vajalikku teavet. AKI roll statistika kogumisel saab olla vaid vajadusel enda menetluste osas sisendi andmises RIA-le.	**Arvestatud.** Eelnõu § 1 punktist eemaldatud viide AKI-le.
35		Digiidentiteedikukrule tuginevate isikute register Eelnõu § 1 p-ga 6 täiendatakse seadust §-ga 31, mille lg 3 loetleb andmekogusse kantavate andmete kategooriad, nähes muu hulgas ette, et andmekogusse kantakse ka muud registri pidamise eesmärgi täitmiseks vajalikud isikuandmeid mittesisaldavad andmed. Kuigi lisatud on piirang, et need andmed ei sisalda isikuandmeid, jääb andmekategooria ise siiski ebaselgeks. Leiame, et tegemist on liiga avatud volitusega. JDM juhise järgi on probleemne olukord, kus töödeldavate andmete kategooriad üldse puuduvad või on liiga laiad ja üldised. Ka andmekogude juhendis on selgitatud, et seadusega võib täpse andmete koosseisu kehtestamise delegeerida täitevvõimule, kuid täitevvõim ei saa väljuda seaduse ja volitusnormi raamidest. Antud juhul isikuandmete välistamine küll vähendab riski, kuid ei kõrvalda siiski õigusselguse probleemi. Soovitame asendada p-i 3 sõnastus konkreetse	**Arvestatud,** eelnõusse lisatud töödeldavad isikuandmete kategooriad (EUTS § 3^1 lõige 3)

		andmeliikide loeteluga või siis täpsustada vähemalt, millist liiki isikuandmeid mittesisaldavaid andmeid võib registrisse kanda. Kui silmas on näiteks peetud tehnilisi metaandmeid, registreeringu menetlusandmeid või avalikustamise vormingut puudutavaid andmeid vms, siis võiks normis sellele ka viidata.	
36		Rakendusakti kavand Kuigi tuginevate isikute registri põhimäärus tuleb eelduslikult täiendavalt arvamuse avaldamiseks peale selle lõpliku sõnastuse kujundamist, toob AKI välja järgmised tähelepanekud, mida põhimääruse koostamisel tuleks arvesse võtta. Põhimääruse kavandis on vastutava töötleja ülesanded kirjeldatud liiga kitsalt (põhimääruse § 2 lg 2). Vastutav töötleja ei ole üksnes n-ö tehniline majutaja, vaid AvTS-st tulenevalt on vastutavaks töötlejaks see, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist, vastutades andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest ehk täidab nende kohustustega seotud ülesandeid. Seega tuleks põhimääruses selgelt sätestada RIA kui vastutava töötleja ülesanded. Põhimääruse § 4 lg 2 on olemuselt sisutu. AvTS järgi on andmekogu infosüsteemis töödeldavate korrastatud andmete kogum, infosüsteem on defineeritud KüTS-s ning selle järgi infosüsteem kujutabki endast digitaalset andmete töötlust. Sama sätte lg-s 4 tuleks lisada üksnes need juhud, kus andmekogu andmetel on õiguslik tähendus ja mitte märkida, et andmetel on üksnes informatiivne tähendus. Põhimääruse § 6 osas märgime, et põhimääruses tuleb loetleda nii andmeandjad kui ka nende poolt esitatavad andmed ehk millistest andmekogudest või kelle käest milliseid andmeid saadakse. Läbi selle määratakse kindlaks, millised on selle konkreetse andmekogu unikaalsed põhiandmed. Põhimääruse § 8 lg 1 (registriandmete õigsus) osas märgime, et andmete teise andmekogusse edastamisel vastutab andmete edastaja edastatavate andmete õigsuse eest. Andmekogu terviku vaatest vastutab andmete õigsuse eest andmekogu vastutav töötleja, kelle andmekogusse andmed edastati. Selgitame, et IKÜM art 5 lg 2 kohaselt tagab vastutav	**Arvestatud.** Täiendame rakendusakti ametlikul kooskõlastusringil.

		töötleja sama artikli lõikes 1 sätestatud isikuandmete töötlemise põhimõtete järgimise. IKÜM art 5 lg 1 p-i d ja IKS § 14 p-i 4 kohaselt tagab vastutav töötleja ka andmete õigsuse ja asjakohasuse. Eelnevalt arvesse võttes vastutab andmekogu vastutav töötleja tervikuna andmekogu andmete õigsuse eest. Seega peaks põhimäärusest nähtuma RIA kui andmekogu vastutava töötleja osa registriandmete õigsuse tagamisel. Praegune sõnastus jätab mulje nagu RIA-l andmekogu vastutava töötlejana siin üldse mingit vastutust ei ole. Põhimääruse § 10 (registriandmete arhiveerimine) osas märgime, et juhul kui andmekogus soovitakse eristada arhiivseid andmeid, siis peab põhimäärusest ka selguma, mida arhiiv sisuliselt tähendab (ehk millal ja millised andmed liiguvad arhiivi, kes nendele andmetele ja millistel tingimustel ligi pääsevad jne) ning miks seda üldse vaja on.	
37	**Siseministeeriumi infotehnoloogia- ja arenduskeskus**	EN § 1 p 6, millega lisatakse § 3^1 lg 6. Juhime tähelepanu, et jääb ebaselgeks mis on registriga seotud andmed mida registrisse ei kanta aga säilitatakse sellest olenemata 10 aastat. Mis andmed need on ja kus neid sellisel säilitatakse?	**Arvestatud.** Eelnõusse lisatud töödeldavad isikuandmete kategooriad (EUTS § 3^1 lõige 3).
38		EN § 1 p 6 millega lisatakse § 5 lg 12: A) Lg 12 viitab lg-le 11 mis omakorda viitab rakendusmääruses (EL) 2024/2977. Samas ei ole selge mis andmeid millisest andmekogust kogutakse. St millised isikutuvastusandmeid saab digiidentiteedikukru pakkuja isikut tõendavate dokumentide andmekogust (ITDAK) ja milliseid Rahvastikuregistrist (RR). Andmesubjektile peab olema selge kust ja konkreetselt milliseid andmeid tema kohta kogutakse. Kas soov on koguda andmeid topelt, kuidas oleks see sellisel juhul isikuandmete töötlemise põhimõtetega kooskõlas? Ka arendusvajadused võivad sõltuda küsitavate andmete koosseisust. Seejärel on võimalik hinnata millise andmekogu juures kas ja milliseid arendusi on vaja teha.	A) **Selgitame,** et 1. ITDAK-st on planeeritud küsida teatud juhtudel isiku pilti. 2. Rahvastikuregistrist on planeeritud küsida teisi EL rakendusmääruse 2026/1731 tabel 1-s loetletud isikuandmeid. Sünnikoht on selles tabelis loetletud. 3. Andmeid päritakse isikute initsiatiivil või vastususe hindamise ja andmeid hoiustatakse konkreetse inimese telefonis olevas kukrus.

		B) SK-s on RRi kohta toodud järgnev „Kehtiva rakendusmääruse (EL) 2024/2977 kohaselt on kohustuslik andmeväli ka digiidentiteedikukru kasutaja sünnikoht, mille digiidentiteedikukrusse kandmine võib eeldada päringut rahvastikuregistrisse.“ Kas RRi puhul ongi mõeldud tegelikult vaid sünnikoha päringuid? Kui jah, siis tuleks see ka eelnõusse selliselt sisse tuua. See aga eeldab, et sünnikoha päringu vajadus on eelnevalt selgeks tehtud, mitte tasandil „võib eeldada päringut“. Ehk et arvestades SK-s toodud sõnastust, siis seadusesse ei peaks looma aluseid andmete pärimiseks kui ei ole selge selle vajadus. C) Kehtiva rakendusmääruse (EL) 2024/2977 isikutuvastusandmed sisaldavad ka näokujutist. ITDAK saab isiku näokujutise automaatse biomeetrilise isikutuvastuse süsteemi andmekogust (ABIS) ning ITDAK-sse kantakse andmed isikut tõendavate dokumentide seaduse alusel läbiviidavate menetluste käigus (ITDAK pm § 12), st vastavalt menetluse eesmärgile. Juhul kui seda ei ole eelnevalt tehtud, siis palume eelnõu koostajal koostöös andmekogude vastutava töötlejaga analüüsida, kas näokujutise päring ITDAK-st on õiguspärane või vajab see ABIS andmekogu kaasamist ja eelnõusse toomist.	B) **Arvestatud**, seletuskirja täiendatud. Kõik PID kohustuslikud andmed (välja arvatud pilt) saadakse rahvastikuregistrist, selle alusel millega inimene ennast PID väljastamiseks tuvastas. C) **Teadmiseks võetud**, analüüsime ABIS kui andmeandja vajadust.
39		EN § 1 p 15. Ettepanek kaaluda, kas lisada eelnõusse, et millest sõltuvalt võib kehtivus olla lühem kui 2 aastat. Hetkel eelnõu tasandil võimalik mõista millest see sõltub. Sama põhimõte ka EN § 1 p 16 osas, millega lisatakse § 6 lg 5 - digiidentiteedikukru pakkumise loa kehtivus.	**Selgitame**, et need põhjendused on seletuskirjas põhjendatud. Eelnõu täiendamist ei peetud vajalikuks.
40		EN § 1 p 17. Vastavalt eelnõuga plaanitavale seaduse § 6 g-le 4 (EN § 1 p 16) peab sertifikaat olema. Seega igaks juhuks juhime tähelepanu sõnastusele, mille kohaselt tuleb eelnõu järgi sertifikaat esitada vaid olemasolul, st ei ole nõutud. Ehk et jääb ebaselgeks kas see on kohustuslik või tuleb esitada vaid olemasolul. Ühtlasi on	**Arvestatud**, eelnõus täpsustatud "usaldusnimekirja lisatav teenuse sertifikaat" (EN p 17).

		kehtiv sõnastus jäigem. Kui on siiski vaid „olemasolul“, siis võiks selle muutuse kohta lisada täpsustuse ka seletuskirja.	Selgitame, et elnõuga peeti silmas usaldusnimekirja lisatavat teenuse sertifikaati, mitte vastavushindamisasutuse poolt väljastatud sertifikaati.
41		Seletuskiri EN § 1 p 6. Palume seletuskirja EN § 1 p 6 kohta käiva selgituse teine lõik üle vaadata. Hetkel tundub, et ei lähe EN tekstiga kokku.	**Arvestatud,** seletuskirja kohendatud.
42		Kulud ja ajaraam. Eelnõu rakendamine võib eeldada ITDAK-i ja/või RR-i täiendavaid arendusi ja liidestusi, et tagada vajalik andmevahetus ning toetada digiidentiteedikukru elutsükli haldamist. Seejuures ei ole täna teada milliseid konkreetseid arendusi on vaja teostada, mistõttu ei ole võimalik hinnata nende ajalist mahtu ega ka kulu. Arvestades, et vajalike arenduste osas puudub selgus, on ka praeguses ajaraamis püsimine küsitav. Seletuskirjas on hinnatud RIA, Andmekaitse Inspektsiooni, Justiits- ja Digiministeeriumi ning teiste ministeeriumide kulusid koondtasemel, kuid puudub hinnang üksikutele andmekogudele ja infosüsteemidele tekkiva mõju kohta. Seetõttu ei ole võimalik ka hinnata, kas seletuskirjas toodud arendus- ja liidestamiskulud katavad ITDAKi ja/või RRi arendamise ja kohandamise vajaduse. Arvestades andmekogude rolli ning võimalikku vajadust muuta olemasolevaid teenuseid, liideseid ja andmevahetuslahendusi, tuleks enne eelnõu lõplikku menetlemist analüüsida konkreetselt ITDAKile ja RR-le avalduvat mõju, hinnata vajalike arenduste mahtu ning tuua välja nende eeldatav maksumus ja rahastamisallikas. Seejuures tuleks arvestada nii ühekordset arenduskulu kui ka hilisemat püsikulu. Hetkel ei ole SK-st selge kuidas nende kuludega on arvestatud.	**Selgitame, et** hetkel meile teadaolevalt ei pole vaja RR ja ITDAK arendusi. Plaanitakse kasutada nende teenuseid üle x-tee.
43		TARA. Hetkel ei ole teada, kuid juhime tähelepanu, et kui TARA-sse lisandub digiidentiteedikukru autentimise võimalus, siis võib see	**Selgitame,** et kulude osa on vastatud real 25. Lahenduse juurutamisel lähtutakse

		andmekogudele tuua kaasa täiendavaid arendusvajadusi, millega kaasnevad omakorda kulud.	põhimõttest, et digikukru ülesehitamisega kaasneks võimalikult vähe kulusid.
44		Välismaalaste autentimise andmed. Kuhu on planeeritud salvestada digiidentiteedikukkur vahendusel tuvastatud välismaalaste autentimise andmed (PID)?	**Selgitame,** et autentmisel saadud andmed kasutab ja säilitab vastavalt nõuetele tuginev isik. See see ei muutu võrreldes tänasega, kus tuginevad isikud juba kasutavad TARA kaudu EU eID. Pikemas vaates on kavatsus riigis välja arendada lahendus, mis võimaldaks keskselt viia kokku inimese Eesti isikukoodi sama isiku teise liikmesriigi tunnusega (isikukoodiga).
45		Rakendusakt. Arvestades, et dokument on kavandi faasis ning ei ole toodud ammendavat andmeandjate loetelu, siis ei ole hetkel võimalik hinnata kas on puutumus andmekogudega, mille puhul SMIT on volitatud töötleja.	**Teadmiseks võetud.** Rakendusakti täiendatud andmeandjate paragrahvi kavandiga (§ 6), mis valideeritakse rakendusakti ametlikul kooskõlastusringil.
46	**Maa- ja Ruumiamet**	Kas digiidentiteedikukru lisandumine usaldusteenustesse, mida kasutavad olemasolevad andmekogud (riiklikud autentimise- ja allkirjastamise teenused), toob kaasa lisanõudeid usaldusteenusele tuginevatele süsteemidele? Näiteks, kas e-teenused peavad laiendama kasutajaskonda üle-Euroopaliseks, mille tulemusel ei piisa enam isikute valideerimisest rahvastikuregistris või äriregistris, vaid tuleb arvestada ka muude variantidega?	**Selgitame**, et Komisjoni eesmärk on tekitada (uuesti) digitaalset ühisturgu. See on aga relevantne nendele e-teenustele kes ka täna juba pakuvad teenuseid teiste liikmesriikide residentidele, näiteks läbi TARA eID võimaluse. Digikukkur annab siis lisavõimalused ja võimendab seda üleliidulist identimist.
47		Kui andmekogu või infosüsteem kasutab riiklikku autentimis- ja allkirjastamisteenust, siis kas selline andmekogu peab ise ennast digiidentiteedikukrule tuginevate isikute riiklikusse registrisse registreerima või lisatakse riiklikud andmekogud ja infosüsteemid sinna vaikimisi?	**Selgitame**, et tänane kavatsus on TARA tänased kliendid saada digikukrut kasutama võimalikult lihtsalt (sh RP registri toimingud), et avaliku sektori asutustel oleks sellega seotud võimalikult väike halduskoormus.
48		Kui riiklikku autentimisteenust kasutavat andmekogu kasutab asutus otsese avaliku teenuse läbi viimiseks, siis kas ka see asutus peab	**Selgitame**, et TARA olemasolevate klientide registreerimise detailid on täpsustamisel.

		ennast digiidentiteedikukrule tuginevate isikute riiklikus registris registreerima?	
49	**Eesti Infotehnoloogia ja Telekommunikatsiooni Liit**	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. 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	**Mittearvestatud.** Selgitame, et kuigi tavapäraselt teeb neid loetletud toiminguid vastavushindamisasutus, siis eIDAS määruse järgi saab järelevalve asutus igal hetkel ka ise vajadusel kõiki kontrolle teha (art. 20 lg 2). Selle sätte eesmärk on ühetaolise järelevalve tagamine piiriüleselt. Kuna eIDAS määrusena on otsekohalduv, ei tohi Eesti riikliku otsusega selle kohustusi kitsendada.

		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. 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.	
50		Digikukru, e-identimise süsteemide usaldusväärsuse taseme hindamine ja sertifitseerimine ning loa andmine. 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. EUTS-is sätestatud siseriiklikku e-identimise usaldusväärsuse	**Arvestatud osaliselt.** Seletuskirjas selgemalt kirjeldatud, et sertifitseerimise skoobi määrab ära 2981 rakendusakt, samuti alused millised asutused võivad seda teostada. Plaan on digikukru hankega leida sobilik lõplik sertimise skeem ja sertifitseerimine. Digikukru usaldusväärsuse kõrge tase on määratud määruses ja rakendusaktides, selle kontroll on osa sertifitseerimisest. Kukru väljaandmise etappidest on koostatud ka eraldi analüüs, mis sisaldab viiteid eIDAS määrusele. Veebis kättesaadav: https://www.ria.ee/riigi-

		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.	infosusteem/elektroonilise-identiteedi-teenused/digikukkur-eudi-wallet#analuusid:~:text=Tegevuste%20tabel%20EUDIW%20v%C3%A4ljaandmiseks%20%7C%2087.65%20KB%20%7C%20xlsx.
51		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. 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.	**Mittearvestatud.** Digikukrut ei saa võrdsustada usaldusteenustega - need on erinevad teenused. Lühem loa kehtivusaeg suurendab halduskoormust ning siiani on kõik tegevusload olnud sünkroonis neile vastavushindamisasutuse (*CAB*) poolt väljastatud sertifikaadi kehtivusega (mis on usaldusteenuste puhul 2 aastat). Kukrule tehtud sertifitseering hakkab kehtima 5 aastat ning sellest tulenevalt võiks ka tegevusluba kehtida sama kaua. Kui vahesertifitseerimist ei tehta (või leitakse vahepeal nt suured turvaaugud, mida ettekirjutuse peale korda ei tehta) - on RIAl kui pädeval asutusel alati võimalik tegevusluba kehtetuks tunnistada.
52		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	**Mittearvestatud.** Selgitame**,** et EUTS § 7 lõike 3 näol ei ole tegemist uute nõuetega, RIA on samasugust teavet ka siiani loamenetluste puhul juurde küsinud. Seega eelnõu täiendamise eesmärk on lahendada just ettepaneku eesmärki - luua selgust, mida tuleb taotlejal loamenetluse puhul esitada.

		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 11 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 11 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 11 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?	Ka EUTS § 7 lõikes 3 punktis 1^1 sätestatud nõue oli enne sätestatus EUTS rakendusaktis (majandus- ja taristuministri 26.10.2016 määrus nr 64 "Usaldusteenuse osutaja ja usaldusteenuse vastavushindamise kord" - § 3 lg 2 punkt 7). Kuna kõnealune määrus antud eelnõuga kaob, siis tõsteti selle säte seadusesse. Vastavushindamisasutus peab kontrollima usaldusteenuse osutaja vastavust muuhulgas ka kohalikule regulatsioonile, millega on siseriiklikult üle võetud NIS2 direktiiv (Eestis on selleks KüTS). Koondjärelduse all peame silmas audiitori kokkuvõtvat hinnangut usaldusteenuse ja selle osutaja eIDAS nõuetele ja seotud siseriiklikele nõuetele vastamise kohta. See võib olla sertifikaadil või rapordi põhidokumendis ning esitatud paari lausega või nt tabeli kujul. Praktikas ei ole siiani antud nõue probleeme tekitanud.

53		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. 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.	**Selgitame,** et eIDAS ja rakendusmäärused ei defineeri PID väljastuse ja elutsükli kontekstis eraldiseisvat "Registration Authority (RA)" rolli. Defineeritud on PID pakkuja ning määratud talle PID väljastamisega seotud kohustused, sealhulgas nõude tagada LoA kõrge nõuetele vastav kasutaja isiku tuvastamine jms. PID väljastamise ja elutsükli eest vastutab PID pakkuja, kes hangitakse teenusena digikukru hanke käigus. Rahvastikuregister ei ole PID pakkuja vaid pigem autentne allikas PID pakkujale. Digikukru pakkujate vastutusejaotust on küsitud Euroopa Liidu Komisjonilt ning saadud järgnev vastus - Digikukru pakkujate üle teostavad järelevalvet artikli 46a alusel määratud järelevalveasutused; artikli 46a lõike 3 punktid a ja b annavad neile asutustele selgesõnalised eel- ja järeljärelevalve volitused. Sertifitseerimisasutused peavad teatama järelevalveasutusele vastavussertifikaatide väljastamisest,

			peatamisest ja tühistamisest (komisjoni rakendusmäärus (EL) 2024/2981, artikkel 11).
54		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.“*. Muudatus ei muuda seletuskirja sisu, vaid viib selle sõnastuse paremini kooskõlla eIDAS artikli 5f lõikega 2 ning sama seletuskirja teistes osades juba kasutatud terminoloogiaga.	**Arvestatud,** seletuskirja täiendatud.
55		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.	**Selgitame,** et eelnõu koostamise raames kaaluti erinevaid variante. Äriregister ning mitmed teiste asutuste vastutusel registrid ei osutunud valituks, sest see oleks teinud keerulisemaks vastutuse jaotuse Riigi Infosüsteemi Ameti ning vastava registri vastutava töötleja vahel. Seega viimases

			valimis olid Riigi Infosüsteemi vastutusel teised andmekogud ning eraldi andmekogu loomine. Kuna EIDAS2 määrus näeb tuginevate isikute registri eraldi ette, otsustati määruse kõige selgema rakendamise huvides luua uus andmekogu.
56		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.	**Arvestatud**, seletuskirja täiendatud. Samuti selgitame, et kohustus aktsepteerida teiste liikmesriikide kukruid kehtib sõltumata Eesti digikukru valmimisajast.
57		Sunniraha ülemmäära vähendamine eIDAS 2 artikli 16 eesmärk on sätestada rikkumiste eest kohaldatavate haldustrahvide maksimaalne	**Arvestatud**, sunniraha ülemmäära vähendatud 5 000 000 pealt 500 000ni (10 korda). Summat

		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. Eelnõus on aga sama suur ülemmäär ette nähtud ka sunnirahale (eelnõu § 1 punktiga 41 lisatav EUTS § 231). 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 § 231 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).	ei vähendatud 50 000ni, et säilitada efektiivne võimalus mõjutada digikukru pakkujat õiguskuulekale tegevusele ning täita seeläbi eIDAS2 artikli 16 lõikes 1 sätestatud kohustus. Selgitame, et eIDAS2 artikli 16 lõige 1 kohustab liikmesriike kehtetama mõjusad, proportsionaalsed ja hoiatavad normid eIDAS määruse rikkumise eest kohaldatavate karistuste kohta. See säte kohaldub lisaks usaldusteenuse osutajatele ka digikukru pakkujale. Samas otsustati eelnõu koostamise käigus, et digikukru pakkujale ei määrata trahve selliselt, nagu seda on tehtud usaldusteenuse pakkuja suhtes (eelnõu järgne EUTS § 23^2). See lähtus kaalutlusest, et kuna eIDAS2 artikli 16 lõikes 2 (mis näeb ette trahvimäärad) ei nimetata digikukru pakkujaid, oleks trahvi ettenägemine digikukru pakkujale ülereguleerimine (n.ö *gold*-plating). Vaata ka „Ametniku Euroopa Liidu käsiraamat“ ptk 8.3.5. Seega on piisavalt suur (500 000) sunniraha määr sobiv tasakaalupunkt eIDAS 2 artikli 16 lõikes 1 sätestatud kohustuse täitmiseks digikukru pakkuja suhtes olukorras, kus digikukru pakkujatele pole ette nähtud trahve.
58		Digikukru regulatsiooni paigutus seaduses Teeme ettepaneku paigutada digikukrut reguleerivad sätted EUTS-is eraldi peatükki. See	**Mitte arvestatud.** Nõustume, et digikukru regulatsiooni võiks paigutada seaduses

		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.	mitmeti, muuhulgas vastavalt ettepanekule. Ettepanekut kaaluti eelnõu koostamise alguses, aga selle tulemus on mitmete samasisuliste sätete kordamine. Kuna ettepanekuga ei kaasne selget kvalitatiivset kasu võrreldes eelnõu lahendusega, ei hakata eelnõud muutma.
59		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.	**Selgitame,** et ettepanekut on kaalutud kuid eelnõud ei muudeta. Eesti isikukood on Eestis vajalik andmeatribuut, et teostada rahvastikuregistrist asjakohaseid päringuid ja valideerimisi. Samuti on see vajalik Eestis e-teenuste kasutamisel.
60		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	**Mitte arvestatud.** Selgitame, et tegemist on erinevate alustega. § 9 lg 1 p 1 kirjeldab olukorda, kus audiitor märgib selgesõnaliselt, et teenuse ja/või teenuse osutaja ei vasta nõuetele. Uus lg 4 kirjeldab olukorda, kus

		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.	audiitori vastavushindamisaruande koondjäreldusest võib välja lugeda, et teenus ja/või teenuse osutaja küll vastab nõuetele, kuid aruandes kirjeldatu alusel jõuab järelevalve järeldusele, et esineb olulisi puudusi, mille kõrvaldamata jätmiseni ei ole võimalik tegevusluba väljastada. Näiteks ei ole hinnatud siseriiklikule õigusele vastavust või hinnatud vastavust valede/aegunud nõuete alusel või on aruande alusel ilmne, et seda on kopeeritud teise aruande pealt ilma sisusse süvenemata. Need näited pärinevad tegelikust praktikast.
61		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:	**Mitte arvestatud.** Sertifikaadi ja ka kogu usaldusteenuste usaldusväärsus on üles ehitatud rangete reeglite järgimisele, eriti kvalifitseeritud teenuste puhul. Kui eIDAS või rakendusaktide nõudeid on rikutud, siis ei saa olla kindel, et sertifikaadid on usaldusväärsed. Sellist "halli ala" ei eksisteeri, et peaks eraldi hindama sisulist mõju teenusele. Usaldusteenuse maailmas on loogika selline, et vaja on kindlust usaldusväärsuses, mitte usaldusväärsuse puudumises. Lisaks täpsustame, et antud juhul on tegemist lihtsalt aluste loeteluga, millal võib sertifikaadi kehtetuks tunnistamist taotleda. Seega järelevalveasutusele jääb diskretsiooniõigus, kui tõepoolest on tegu väga väikese eksimusega.

		„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.“. 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.	
62	**Rahandusministeerium**	Teeme ettepaneku lüüa kõik selle õigusaktiga seotud kulud tabelis lahti järgmises lõikes: -investeeringud ; -tööjõukulud ; -majandamiskulud, mis seotud tööjõukuludega ; -majandamiskulud.	**Arvestatud**, seletuskirja kulude peatükki täiendatud.
63	**Riigi Infosüsteemi Amet**	Palume asendada EUTS § 4^1 lõikes 1 sõna „viivimatult“ väljendiga „"igal juhul 24 tunni jooksul pärast intsidenti". See tähtaeg tuleneb EIDAS määrusest.	**Arvestatud**, § 4^1 -s täpsustatud 24 tunnine tähtaeg turvaintsidendist.
64		Palume muuta ja täiendada EUTS §-i 10 lõikes 3 pärast sõnu „kantakse nimekirja“ sõnaga „kuni“ (kantakse nimekirja kuni kaheks aastaks). See viiks sätte sõnastuse kooskõlla ülejäänud loogikaga – usaldusnimekirja kandmine peab olema kooskõlas väljastatud vastavushindamise sertifikaadiga.	**Arvestatud**, EUTS § 10 lõiget 3 täiendatud sõnaga „kuni“.
65		Palume EUTS § 13 lõikes 4 asendada väljend „Usaldusnimekirjas kajastatud andmete muutmise „ väljendiga „Teenuse muudatuse“. Vastasel juhul peab riigilõivu tasuma ainult siis, kui muutuvad usaldusnimekirjas kajastatud andmed. Praktikas enamasti andmed usaldusnimekirjas ei muutu, kuid muudatuse läbivaatamine ja kinnitamine nõuab RIA-lt omajagu ressurssi. Lisaks ei ole sellise	**Arvestatud,** EUTS § 13 lõiget 4 muudetud.

		sõnastusega kaetud digikukru muudatused, mida usaldusnimekirja ei kanta.	