

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.	Eesti Linnade ja Valdade Liit	Seletuskirjas (lk 22) on märgitud, et „teenuste liidestamine digikukruka ja tõendite koostalitlusvõime tagamine on iga haldusala ülesanne" ning et Euroopa digiidentiteedi kukruka liidestuvate ministeeriumide (haldusalade) kulud on kokku 2 000 000 eurot. Seletuskirjast (lk 22) ei selgu, kuidas on vastav kulu välja arvatud ning palume seletuskirja vastavalt täiendada. Euroopa digiidentiteedi kukruka liidestuvad ka omavalitsuste e-teenused, mistõttu on koostalitlusvõime tagamise kulu katmine põhjendatud ka omavalitsustele. Seletuskiri tunnistab (lk 22), et „asutused, kes kesket 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 TARAgas 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 teise liikmesriigi kodanikul see puudub), tuleb sellega liidestatud infosüsteemi vastavalt kohandada. Kuna omavalitsused kasutavad teenuste osutamiseks laialdaselt erasektori pakutavaid infosüsteeme,	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 võimaluse kergemalt toetada rohkemate liikmesriikide eID läbi

	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 kasutuselevõttuga. 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 infosüsteemide kohandamise kulude hinnanguga. Palume tagada riiklik rahastus.	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.
--	---	---

2.		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 pääsuserifikaadid 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.
3.		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.
4.		Juhime ka tähelepanu, et eelnõus on kasutatud nii mõistet „Euroopa digiidentiteedi kukkur“ kui ka „Euroopa digiidentiteedikukkur“ ning palume see ühtlustada.	Arvestatud , mõisted eelnõus ühtlustatud.
5.	Eesti Infotehnoloogia ja Telekommunikatsiooni Liit	Rollide koondumine RIA-sse ja täiendav järelevalveku ITL juhü tähelepanu Riigi Infosüsteemi Ameti (RIA) rollide ulatuslikule koondumisele kavandatavas regulatsioonis. Eelnõu kohaselt hakkab sama asutus täitma samaaegselt mitut kesket 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	Mittearvestatud. Selgitame, et kuigi tavapärast 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 piiriülealt. Kuna eIDAS määrusena on otsekohalduv, ei tohi Eesti riikliku otsusega selle kohustusi kitsendada.

	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. 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.	
6.		Digikukru, e-identimise süsteemide usaldusväarsuse taseme hindamine ja sertifitseerimine ning loa andmine. Euroopa digiidentiteedikukru (edaspidi: digikukkur) sertifitseerimise, usaldusväarsuse taseme hindamise ja pakkumise loa andmise protsessid ei ole eelnõus piisavalt selgelt reguleeritud. Näiteks ei selgu, kes ja millises menetluses hindab ning kinnitab digikukru usaldusväarsuse 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 usaldusväarsuse 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 usaldusväarsuse 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.	Arvestatud osaliselt. Seletuskirjas selgemalt kirjeldatud, et sertifitseerimise skooobi määrab ära 2981 rakendusakt, samuti alused millised asutused võivad seda teostada. Plaan on digikukru hankega leida sobilik lõplik sertimise skeem ja sertifitseerimine. Digikukru usaldusväarsuse 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-infosusteem/elektroonilise-identiteediteenused/digikukkur-eudi-wallet#analusid:~:text=Tegevuste%20tabel%20EUDIW%20v%C3%A4ljaandmiseks%20%7C%2087.65%20KB%20%7C%20xlsx.
7.		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	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

		võrreldes teiste teenuseliikidega. Nii e identimise kui ka usaldusteenuste puhul kehtib luba 2 aastat. Iseenesest ei pea olema loa andmine vaikselt 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.	väljastatud sertifikaadi kehtivusega (mis on usaldusteenuste puhul 2 aastat). Kukurule 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 RIAI kui pädeval asutusel alati võimalik tegevusluba kehtetuks tunnistada.
8.		Digikurku pakumise 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 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	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. Ka EUTS § 7 lõikes 3 punktis 1¹ 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

		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?	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.
9.		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 intsidenti 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	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.

		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.	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).
10		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:	Arvestatud, seletuskirja täiendatud.

		„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.	
11		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.
12		Erasektorit puudutavate kohustuste tähtsajad 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	Arvestatud, seletuskirja täiendatud. Samuti selgitame, et kohustus aktsepteerida teiste liikmesriikide kukruid kehtib sõltumata Eesti digikukru valmimisajast.

		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.	
13		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. 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,	Arvestatud, sunniraha ülemmäära vähendatud 5 000 000 pealt 500 000ni (10 korda). Summat ei vähendatud 50 000ni, et säilitada efektiivne võimalus mõjutada digikukru pakkuja õiguskäitajale 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 pakkuja. Samas otsustati eelnõu koostamise käigus, et digikukru pakkuja ei määrata trahve selliselt, nagu seda on tehtud usaldusteenuse pakkuja

		kus maksimaalne trahv on direktiivist tulenevalt 7 miljonit eurot, kuid sunniraha oluliselt madalam (70 000 eurot).	suhtes (eelnõu järgne EUTS § 23²). 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 <i>gold-plating</i>). 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.
14		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	Mitte arvestatud. Nõustume, et digikukru regulatsiooni võiks paigutada seaduses 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.

		digikukrut käsitlevad sätted paigutada e-identimist reguleerivasse peatükki.	
15		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.
16		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.	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 audiitori vastavushindamisaruande koondjärelدusest 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.

17	Sertifikaadi kehtetuks tunnistamise aluste ammendavus Teeme ettepaneku jätta eelnõust välja eelnõu § 1 punktiga 37 EUTS-i lisatava § 19 lõike 4 punkt 16. Leiam, 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: <i>„16) sertifikaadi väljastamise järel ilmnenu 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.“.</i> 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.	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 <u>võib</u> sertifikaadi kehtetuks tunnistamist taotleda. Seega järelevalveasutusele jääb diskretsiooniõigus, kui tõepoolest on tegu väga väikese eksimusega.
----	---	---