

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

1. Sissejuhatus

1.1. Sisukokkuvõte

Eelnõuga viiakse Eesti õigus kooskõlla Euroopa Liidu uuendatud e-identimise ja usaldusteenuste raamistikuga (nn eIDAS 2), millega luuakse Euroopa digiidentiteedi raamistik ja selle keske elemendina Euroopa digiidentiteedikukkur.

Euroopa Liidu määrus on vahetult kohaldatav, kuid selle terviklik rakendamine eeldab riigisiseste rollide, menetluste ja karistuste kindlaksmääramist. Eelnõu peamine eesmärk on viia Eesti seadused Euroopa digiidentiteedi raamistikuga kooskõlla, tagada Euroopa digiidentiteedikukru (edaspidi ka *digikukkur* ja *kukkur*) turvaline kasutuselevõtt Eestis ning sätestada selleks vajalikud riigisisised reeglid, rollid ja sanktsioonid.

Kehtiv õigus ei reguleeri Euroopa digiidentiteedi raamistiku rakendamist piisavalt, kuna riigisisest rollid, menetlused ja järelevalve ei ole selgelt kindlaks määratud. Seetõttu on vaja seadust kooskõlas Euroopa Liidu uute nõuetega ajakohastada.

Kõige olulisemad muudatused on järgmised:

- Euroopa digiidentiteedikukru pakkumine tuuakse e-identimise ja e-tehingute usaldusteenuste seaduse reguleerimisalasse; riigil on kohustus teha elanikele kättesaadavaks vabatahtlikult kasutatav riiklikult tagatud Euroopa digiidentiteedikukkur;
- Riigi Infosüsteemi Amet määratakse peamiseks pädevaks asutuseks (järelevalve, load, register, teavitamine ja muud liikmesriigi ülesanded);
- luuakse Euroopa digiidentiteedikukrule tuginevate isikute registreerimise korraldus;
- Euroopa digiidentiteedikukru pakkuja kehtestatakse loamenetlus ja selle eest riigilõiv;
- kvalifitseeritud usaldusteenuse osutaja vastutuskindlustuse aastane koondsumma suureneb ühelt miljonilt kahe miljoni euroni;
- Eestis väljaantavasse Euroopa digiidentiteedikukrusse kantakse lisaks kohustuslikele isikutuvastusandmetele ka isikukood, mis on Eesti jaoks valikuline, kuid kukru praktiliseks kasutatavuseks oluline otsus;
- kehtestatakse Euroopa Liidu nõuetele vastavad trahvimäärad (kuni 5 000 000 eurot või 1 protsent üleilmsest aastasest kogukäibest) ning sunniraha igakordne ülemmäär (500 000 eurot või 1 protsent üleilmsest aastasest kogukäibest);
- karistusseadustikus lisatakse Euroopa digiidentiteedikukkur tähtsate isiklike dokumentide loetellu;

- mitu senist sätet tunnistatakse kehtetuks, kuna need on asendunud Euroopa Liidu otsekohaldavate rakendusmäärustega;
- Euroopa digiidentiteedikukru rakendustarkvarale kehtestatakse avatud lähtekoodi nõue koos Eestile lubatud erandi võimalusega;
- andmekaitsealases järelevalves ja kaebuste lahendamisel isikuandmete kaitse üldmääruse raames saab olulise rolli ka Andmekaitse Inspeksioon, kes tegutseb pädeva riikliku andmekaitseasutusena.

Mõjud on lühidalt järgmised: kodanikud saavad võimaluse kasutada üleeuroopalist digiidentiteeti, mis isikukoodi abil sobitub Eesti e-teenustega; ettevõtjatele luuakse selgemad reeglid usaldusteenuste osutamiseks ja Euroopa digiidentiteedikukru pakkumiseks; kahe paralleelse riikliku e-identimise vahendi (ID-kaart ja teised senised vahendid ning Euroopa digiidentiteedikukur) olemasolu suurendab e-riigi kerksust. Seaduse rakendamisega kaasnevad riigieelarvele lisakulud, mis jagunevad rakendamiskuludeks ja järelevalve tugevdamise kuludeks. Tegemist on õiguslikult olulise, kuid sisult eelkõige kohustusliku kohandamisega Euroopa digiidentiteedikukru raamistiku elluviimiseks Eestis, kusjuures Eesti valib aktiivse lähenemise, et kukkur oleks laialdaselt kasutatav ka Eesti e-teenuste puhul.

Halduskoormusele avalduva mõju kokkuvõte

Ettevõtjate halduskoormus ajutiselt suureneb, kuna osa teenuseosutajaid peavad digiidentiteedikukru kasutuselevõtuks oma süsteeme kohandama. Mikro- ja väikeettevõtjad on sellest kohustusest vabastatud. Samas aitab ühtne Euroopa digiidentiteedi lahendus ja digitaalsete tõendite kasutamine edaspidi vähendada kliendituvastuse ja asjaajamisega seotud kulusid. Inimeste halduskoormus väheneb, sest isiku ja vajalike andmete tõendamine muutub lihtsamaks nii Eestis kui ka teistes Euroopa Liidu liikmesriikides. Avaliku sektori töökoormus suureneb seoses digiidentiteedikukru arendamise, registri pidamise, järelevalve ja sertifitseerimisega seotud ülesannetega.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Justiits- ja Digiministeeriumi IT-õiguse talituse nõunik Mait Heidelberg (mait.heidelberg@justdigi.ee) koostöös Riigi Infosüsteemi Ameti ekspertidega. Eelnõu on keeleliselt toimetanud Justiits- ja Digiministeeriumi õigusloome korralduse talituse toimetaja Inge Mehide (inge.mehide@justdigi.ee).

Valdkonna eest vastutav asekancler on Tõnu Grünberg.

1.3. Märkused

Eelnõu on seotud Euroopa Liidu õiguse rakendamisega: sellega tagatakse kooskõla Euroopa Parlamendi ja nõukogu määrusega (EL) nr 910/2014¹ (edaspidi ka *eIDAS-määrus*), mida on

¹ Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.08.2014, lk 73–114). <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32014R0910>

muudetud Euroopa Parlamendi ja nõukogu määrusega (EL) 2024/1183² seoses Euroopa digiidentiteedi raamistiku kehtestamisega (edaspidi ka *eIDAS 2 määrus*), ning nende alusel antud Euroopa Komisjoni rakendusmäärustega.

Eelnõuga muudetakse järgmiste seaduste redaktsioone: e-identimise ja e-tehingute usaldusteenuste seadus³ (redaktsioon jõustumiskuupäevaga 01.01.2026), riigilõivuseadus⁴ (redaktsioon 01.08.2026–31.10.2026) ja karistusseadustik⁵ (redaktsioon jõustumiskuupäevaga 01.01.2026).

Eelnõu ei ole seotud muu menetluses oleva eelnõuga. Eelnõu täidab koalitsioonileppe 2025–2027 valdkonna 07.1 Digiriik koalitsioonileppe punkti „Teeme andmetega seotud õiguslikus raamistikus asjad selgeks ja ühte moodi tõlgendatavaks ning lihtsustame andmetöötlust“ tegevust „ELi digikukruga seotud selgete rollide määramiseks E-identimise ja e-tehingute usaldusteenuste seaduse muutmise“.

Eelnõu seadusena vastuvõtmiseks on vajalik Riigikogu poolthääle enamus.

2. Seaduse eesmärk

Seaduse eesmärk on ajakohastada e-identimise ja e-tehingute usaldusteenuste seadus ning viia see kooskõlla Euroopa Liidu uuenenud õigusaktidega. Sellega luuakse Eestis Euroopa digiidentiteedikukru kasutuselevõtuks, järelevalveks ja õiguskaitseks selge, rakendatav ja usaldusväärne õiguslik raamistik. Valdkonda reguleerib eIDAS-määrus, mida muudeti eIDAS 2 määrusega seoses Euroopa digiidentiteedi raamistiku kehtestamisega. Kuigi tegemist on otsekohalduva määrusega, sisaldab see nõudeid riigisiseste mehhanismide loomiseks, et määrust terviklikult rakendada. Määruse alusel on vastu võetud vähemalt 30 otsekohalduvat rakendusmäärust, mis määruse (EL) nr 910/2014 nõudeid täpsustavad, ning uute rakendusaktide ettevalmistamine ja olemasolevate muutmine jätkub. Euroopa Komisjon kavandab rakendusmääruste ajakohasena hoidmist pideva protsessina, et sünkroniseerida neis olevaid tehnilisi nõudeid pidevalt uuenevate standarditega. Kehtiva regulatsiooni peamine kitsaskoht on, et see ei kajasta Euroopa digiidentiteedi raamistikku: seaduses puuduvad Euroopa digiidentiteedikukru pakkumise, järelevalve ja asjaomaste karistuste normid ning mitu sätet dubleerivad nõudeid, mis on nüüdseks kehtestatud Euroopa Liidu otsekohalduvate rakendusmäärustega. Praktikas on tõlgendamiskursi tekitanud ka sertifikaatide kehtetuks tunnistamise aluste senine sõnastus (vt seletuskirja § 1 punktide 37–40 selgitusi).

E-identimise ja e-tehingute usaldusteenuste seaduse ajakohastamine on vajalik eelkõige järgmistel põhjustel:

– uuendatud eIDAS-määrusega võetakse kasutusele Euroopa digiidentiteedikukru kontseptsioon, millega seotud rollide ja vastutuse jaotus Eestis ning järelevalve korraldus tuleb reguleerida seadusega;

² Euroopa Parlamendi ja nõukogu 11. aprilli 2024. aasta määrus (EL) 2024/1183, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega (ELT L, 2024/1183, 30.04.2024). <http://data.europa.eu/eli/reg/2024/1183/oj>

³ RT I, 30.12.2025, 16. <https://www.riigiteataja.ee/akt/130122025016>

⁴ RT I, 11.07.2026, 166. <https://www.riigiteataja.ee/akt/111072026166>

⁵ RT I, 09.07.2026, 27. <https://www.riigiteataja.ee/akt/109072026027>

– uuendatud eIDAS-määrus ja selle rakendusaktid kirjeldavad varasemast detailsemalt mitmeid usaldusteenuse ja selle osutamisega seotud nõudeid, mistõttu on mitu e-identimise ja e-tehingute usaldusteenuste seaduse sätet kaotanud aktuaalsuse ja tuleb dubleerimise vältimiseks kehtetuks tunnistada;

– uuendatud eIDAS-määrus näeb ette konkreetsed karistuste ülemmäärad rikkumiste eest, millele vastavad sanktsioonid tuleb Eesti õigusruumis kehtestada.

Lisaks kehtestatakse loamenetlus Euroopa digiidentiteedikukru pakkumisele ja selle menetluse kulude katmiseks tehakse vastav täiendus riigilõivuseadusesse. Kuna Euroopa digiidentiteedikukkur kujuneb oluliseks digitaalseks isikutuvastusvahendiks, on otstarbekas käsitleda seda ka karistusseadustikus võrdväärselt teiste isikut tõendavate vahenditega, nagu ID-kaart ja digitaalne isikutunnistus. Nende muudatustega soovitakse saavutada, et Euroopa digiidentiteedikukkur oleks Eestis kasutatav kooskõlas Euroopa Liidu nõuetega, sobituks Eesti olemasolevate e-teenuste ja e-identimise lahendustega ning et riigil oleks olemas vajalikud järelevalve- ja õiguskaitsevahendid. Kaalutud lahendusvariandid ja nende valiku põhjendused on esitatud eelnõu sisu peatükis iga muudatuse juures ning kaalutlusotsuste (muu hulgas isikukoodi kandmine digikukrusse ja avatud lähtekoodi erand) mõjud seletuskirja 6. peatükis.

Eelnõule ei eelnenud väljatöötamiskavatsust. See tugineb hea õigusloome ja normitehnika eeskirja § 1 lõike 2 punktile 2, mille kohaselt ei ole väljatöötamiskavatsus nõutav, kui eelnõu käsitleb Euroopa Liidu õiguse rakendamist ning eelnõu aluseks oleva Euroopa Liidu õigusakti eelnõu menetlemisel on sisuline analüüs tehtud Eesti seisukohtade kujundamise käigus. Kaalutlusruumi kasutamise analüüs tehti Eesti seisukohtade kujundamise käigus (vt seletuskirja 6. ja 10. peatükki).

3. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kolmest paragrahvist:

– esimene paragrahv sisaldab e-identimise ja e-tehingute usaldusteenuste seaduse muudatusi, mis lisaks uuenenud eIDAS-määruse rakendamisele tingitud lisandustele sisaldavad muu hulgas ka lisandunud ülesannetega seotud rollijaotust valitsusasutuste vahel. Toodud rollijaotus põhineb ametkondadevahelise elektroonse identiteedi juhtrühma arvamusel;

– teine paragrahv näeb ette lisandunud loamenetluse eest riigilõivu riigilõivuseaduses;

– kolmas paragrahv lisab karistusseadustiku tähtsate isiklike dokumentide loetellu Euroopa digiidentiteedikukru.

Eelnõu §-ga 1 muudetakse e-identimise ja e-tehingute usaldusteenuste seadust.

§ 1 punkt 1. Paragrahvi 1 lõigete 1 ja 2 muudatustega tuuakse seaduse reguleerimisalasse Euroopa digiidentiteedikukru pakkumine, mis lisandus uue mõistena eIDAS-määrusesse selle eIDAS 2 määrusega muutmise tulemusena. Ühtlasi täpsustatakse reguleerimisala sõnastust, lisades sinna e-identimise süsteemi usaldusvärsuse hindamise. Seda toimingut reguleeris seadus ka varem, kuid reguleerimisalas oli see eraldi välja toomata.

§ 1 punkt 2. Paragrahvi 1 lõike 5 täiendusega lisatakse nende e-identimise süsteemide hulka, mille suhtes ei rakendata kõnesolevas seaduses sätestatud usaldusvärsuse taseme hindamist, ka Euroopa digiidentiteedikukkur. Vastavalt eIDAS-määruse artikli 5a lõikele 11 saab Euroopa

digiidentiteedikukkur olla ainult usaldusväärsuse tasemega „kõrge“, mis leiab kinnitust sertifitseerimise kaudu.

§ 1 punkt 3. Paragrahv 2 muudetakse ja sõnastatakse tervikuna uuesti, kuna uuenenud eIDAS-määrus tingib pädevuse jaotuse mitme asutuse vahel; paragrahvi uus pealkiri on „Asutuste pädevus“. Paragrahvi 2 täiendatakse lõigetega, mis määravad eri rollide jaotuse vastavalt uuenenud eIDAS-määruse nõuetele.

Lõikega 1 lisatakse viited uuendatud eIDAS-määruse sätetele, kus kirjeldatakse liikmesriigi kohustusi või toiminguid, mis on liikmesriigi pädevuses. Ametkondadevahelise elektroonse identiteedi juhtrühma arvamuse kohaselt nähakse pädeva asutusena ette Riigi Infosüsteemi Amet.

Pädeva asutuse ülesandeid täidab Riigi Infosüsteemi Amet mitmes eristatud rollis: järelevalveasutusena, kes teeb järelevalvet Euroopa digiidentiteedikukru pakkuja üle; hankijana, kes korraldab digikukru teenusepakkuja hankemenetluse riigi nimel, ning taristu haldajana, kes korraldab digikukru infrastruktuuri loomist ja haldamist. Rollide lahusus tagatakse Riigi Infosüsteemi Ameti sisese ülesannete jaotusega, mille kohaselt järelevalvet tegevad töötajad ei osale digikukru hanke korraldamises ega infrastruktuuri haldamises. Digikukruga seotud detailsem rollijaotus on läbi räägitud ja kokku lepitud töörühma tasandil (nt digiidentiteedi juhtrühmas mh 19.06.2024 ja 16.07.2024).

Lõige 2 puudutab liikmesriigi kohustust teha isikutele kättesaadavaks Euroopa digiidentiteedikukkur. Vastavalt eIDAS-määrusele võib seda teha vahetult liikmesriik, seda võib teha liikmesriigi volituse alusel või sõltumatult, kuid liikmesriigi tunnustatuna. Kui eelmise lõikega omistati see kohustus pädevale asutusele, siis lõikega 2 antakse pädevale asutusele võimalus Euroopa digiidentiteedikukru pakkumist ja selleks vajalikke tegevusi allhankida.

Lõige 3 määrab kindlaks, et eIDAS-määruse artikli 5a lõike 4 punkti d alapunktis iii ja lõike 5 punkti a alapunktis x sätestatud pädeva riikliku andmekaitseasutuse rolli täidab Andmekaitse Inspeksioon. Nimetatud sätete kohaselt peab Euroopa digiidentiteedikukkur võimaldama kasutajal andmete saamiseks esitatud väidetavalt ebaseadusliku või kahtlase taotluse korral hõlpsasti teatada digiidentiteedikukrule tuginevast isikust pädevale riiklikule andmekaitseasutusele. Sisuliselt on tegemist teavituskanaliga, mille kaudu Andmekaitse Inspeksioon saab teavet võimalikest andmekaitsealastest rikkumistest; teate saamisel menetleb Andmekaitse Inspeksioon seda oma tavapärase pädevuse piires isikuandmete kaitse üldmääruse alusel. Kooskõlastusringil esitatud Andmekaitse Inspeksiooni märkuste alusel koondati Andmekaitse Inspeksiooni rolli käsitlev regulatsioon sellesse lõikesse ning eelnõust jäeti välja seda dubleerinud ja Andmekaitse Inspeksioonile eIDAS-määruse artikli 46a kohast järelevalvepädevust andnud sätted, sest määruse artikli 46a kohane järelevalveasutus on üksnes pädev asutus (Riigi Infosüsteemi Amet).

Lõige 4 määrab valdkonna eest vastutava ministeeriumi korraldama Euroopa digiidentiteedikukru sertifitseerimise kava väljatöötamist, Euroopa Komisjoni teavitamist sertifitseerijast ja avaliku sektori asutustest, kes väljastavad eIDAS-määrusele vastavaid tõendeid.

§ 1 punkt 4. Peatüki 2 pealkirja täiendatakse, lisades sinna ka Euroopa digiidentiteedikukru pakkuja.

§ 1 punkt 5. Paragrahvi 3 lõikes 2 täpsustatakse eIDAS-määruse sätte viidet, kuna säte on jäänud samaks, kuid numeratsioon on määruse uues versioonis muutunud. Pädeva asutusena mõeldakse § 1 p 3 kohast pädevat asutust ehk RIA-t.

§ 1 punkt 6. Lisanduva paragrahviga 3¹ luuakse Eestis eIDAS-määruse artikliga 5b ja komisjoni rakendusmäärusega (EL) 2025/848⁶ ette nähtud digiidentiteedikukrule tuginevate isikute registreerimiseks vajalik register. eIDAS-määruse artikkel 5b ja nimetatud rakendusmäärus näevad ette, et liikmesriigid loovad vähemalt ühe Euroopa digiidentiteedikukrule tuginevate isikute riikliku registri, mis sisaldab teavet selles liikmesriigis asutatud ja registreeringut omavate digiidentiteedikukrule tuginevate isikute kohta. Paragrahviga nähakse ette vastava andmekogu loomine, sinna esitatavate andmete koosseis, andmete esitamise korra kehtestamine, andmete säilitamise tähtaeg ning registreeringu peatamine ja kehtetuks tunnistamine.

Andmekogu asutamisel on järgitud avaliku teabe seaduse § 43⁵ nõudeid: paragrahvi lõikes 1 sätestatakse andmekogu pidamise eesmärk, lõikes 2 registrisse teabe esitamise korra kehtestamine ja avalikustamine, lõikes 3 registris isikuandmetena töödeldavate andmete koosseis, lõikes 4 andmete säilitamise tähtajad, lõikes 5 registriandmete avalikkus, lõikes 6 andmekogu vastutav töötleja (Riigi Infosüsteemi Amet), lõikes 7 volitusnorm registri põhimääruse kehtestamiseks ning lõikes 8 registreeringu peatamine ja kehtetuks tunnistamine. Registri liidestamisel teiste andmekogudega järgitakse avaliku teabe seaduse § 43⁹ lõiget 5 (andmevahetus X-tee kaudu).

Lõikes 3 sätestatakse registris isikuandmetena töödeldavate andmete koosseis: digiidentiteedikukrule tugineva isiku esindaja ees- ja perekonnanimi, isikukood, kontaktandmed ning logiandmed. Isikuandmete töötlemine registris piirdub seega peamiselt juriidiliste isikute esindajate ja kontaktisikute andmetega. Töödeldavate isikuandmete kategooriad lisati seadusesse kooskõlastusringil Andmekaitse Inspeksiooni ning Siseministeeriumi infotehnoloogia- ja arenduskeskuse esitatud märkuste alusel, et andmekoosseis ei jääks õigusselguse seisukohalt liiga avatuks.

Lõikes 4 sätestatakse andmete säilitamise tähtajad kolme andmekategooria kaupa. Punkti 1 kohaselt säilitatakse rakendusmääruse (EL) 2025/848 artiklis 10 nimetatud andmeid vastavalt rakendusmääruse kohaselt kümme aastat. Seda tähtaega seaduses korratakse, et tagada ülevaade andmete säilitamise tähtaegadest. Punkti 2 kohaselt säilitatakse logiandmeid kümme aastat. Selle eesmärk on võimalike intsidentide lahendamine (näiteks andmete väärkasutus, mis selgub aastaid hiljem). Intsidentide lahendamise korral on vaja alles hoida ka kõiki nende andmetega seotud tehnilisi andmeid (näiteks logid, kontaktisikute nimed ja muud menetlusandmed), kuna ka need võivad intsidentide lahendamisel vajalikuks osutuda. Punkti 3 kohaselt säilitatakse muid isikuandmeid, kuni digiidentiteedikukrule tuginev isik muudab registrikannet. Silmas peetakse digiidentiteedikukrule tugineva isiku esindaja kontaktandmeid (näiteks e-posti aadress), mis kustutatakse kohe pärast vastava registrikande muutmist. See võib toimuda näiteks siis, kui digiidentiteedikukrule tugineva isiku esindaja vahetub ning registrisse on vaja kanda uue esindaja kontaktandmed. Lisaks eelnimetatud kolmele andmekategooriale säilitatakse ka muid registri pidamise eesmärgi täitmiseks vajalikke isikuandmeid mittedisaldavaid andmeid (kõnesoleva seaduse § 3¹ lõike 3 punkt 5) kümme aastat, mis on

⁶ Komisjoni 6. mai 2025. aasta rakendusmäärus (EL) 2025/848, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad kukrule tuginevate isikute registreerimise kohta (ELT L, 2025/848, 7.5.2025). http://data.europa.eu/eli/reg_impl/2025/848/oj

vajalik nende ühtseks toimimiseks muude kogutavate andmetega. Seaduses seda andmekategooriat eraldi ei käsitleta, kuna sellega ei kaasne põhiõiguste riivet.

Lõike 5 kohaselt on registrisse kantud andmed avalikud, välja arvatud avaliku teabe seaduse alusel määratud piiratud juurdepääsuga teave. Andmete avalikkuse nõue tuleneb eIDAS-määruse artikli 5b lõikest 5 ja rakendusmääruse (EL) 2025/848 artikli 3 lõikest 4, mille kohaselt tuleb digiidentiteedikukrule tuginevate registreeritud isikute kohta käiv nimetatud rakendusmääruse I lisas loetletud teave teha internetis avalikult kättesaadavaks nii inim- kui ka masinloetavas vormingus. Juurdepääsu piiramise alus peab tulenema seadusest: avaliku teabe seaduse (AvTS) § 3 lõikes 2 väljendatud avalikkuse põhimõtte kohaselt võib avalikule teabele juurdepääsu piirata üksnes seaduses sätestatud korras, mistõttu ei saa registriandmetele vaikumisi teabepiirangut ette näha. Praeguse teadmise kohaselt on piiratud juurdepääsuga näiteks digiidentiteedikukrule tugineva isiku ärisaladuseks määratud vahendaja ja kontaktisiku andmed, kui need määratakse ärisaladuseks AvTS-i § 35 lõike 1 punkti 17 alusel. Lisaks AvTS-i § 35 lõike 1 punktile 17 võib teabele juurdepääsu piiramise aluseks olla ka sama lõike punkt 12 (eraelu puutumatust kahjustav teave), näiteks rakendusmääruse (EL) 2025/848 artikli 3 lõike 4 alla mittekuuluvate isikuandmete puhul. Seetõttu tuleb registri põhimääruses eristada avalikustatav teave (rakendusmääruse I lisa) juurdepääsupiiranguga andmetest.

Lõikega 6 määratakse andmekogu vastutavaks töötlejaks Riigi Infosüsteemi Amet. Vastutava töötleja ülesandeid täpsustatakse andmekogu põhimääruses.

Lõikega 7 antakse volitusnorm registri põhimääruse kehtestamiseks valdkonna eest vastutavale ministrile. Põhimääruses sätestatakse andmete täpne koosseis, andmeandjad ja nende esitatavad andmed, registritoimingute ja andmete säilitamise täpsemad tingimused, registri rahastamine ning registriga seotud muud korralduslikud nõuded.

Lõike 2 kohaselt kehtestab ja avalikustab Riigi Infosüsteemi Amet oma veebilehel registrisse teabe esitamise korra. See kord hõlmab üksnes registreerimise tehnilisi ja korralduslikke üksikasju (näiteks andmete esitamise vorming ja kanalid); isikute õigusi ja kohustusi puudutavad registreerimiskorra elemendid, sealhulgas andmete esitamise ja menetlemise täpsem kord, sätestatakse seaduses ja lõike 7 alusel antava registri põhimääruse §-s 8. Lõike 8 kohaselt võib pädev asutus teha otsuse digiidentiteedikukrule tugineva isiku registreeringu peatamiseks või kehtetuks tunnistamiseks rakendusmääruse (EL) 2025/848 artikli 9 lõikes 2 loetletud juhtudel.

§ 1 punkt 7. Paragrahvis 4¹ sätestatakse digiidentiteedikukru pakkuja ja usaldusteenuse osutaja kohustus teavitada pädevat asutust turvaintsidentidest. eIDAS-määrus ning komisjoni rakendusmäärus (EL) 2025/847 näevad ette liikmesriikide kohustuse reageerida Euroopa digiidentiteedikukruga seotud turvarikkumistele ning teavitada vajaduse korral Euroopa Komisjoni ja teisi liikmesriike, kuid ei pane Euroopa digiidentiteedikukru pakkujale otsest kohustust teavitada riigisisest pädevat asutust. Kuna Euroopa digiidentiteedikukru pakkuja ei ole Euroopa Liidu õiguse kohaselt automaatselt direktiivi (EL) 2022/2555 ega selle Eesti rakendusakti, küberturvalisuse seaduse kohaldamisalasse kuuluv subjekt, on vaja kehtestada vastav riigisisene teavitamiskohustus.

Usaldusteenuse osutajate puhul sisuliselt taastatakse teavituskohustus, mis kehtis kuni 1. jaanuarini 2026, arvestades et küberturvalisuse seaduses sätestatud küberintsidendi määratlus ei hõlma täies ulatuses usaldusteenuse osutamisel ega Euroopa digiidentiteedikukru pakkumisel tekkida võivaid turvaintsidente. Küberturvalisuse seaduse § 2 punkti 19 kohaselt on küberintsident võrgu- ja infosüsteemis toimuv sündmus, mis ohustab või kahjustab võrgu- ja

infosüsteemi turvalisust. Näiteks kui usaldusteenuse osutaja või tema partner väljastab sertifikaate auditeeritud protsessi tingimusi rikkudes, ei ole tegemist küberintsidendiga küberturvalisuse seaduse ega direktiivi (EL) 2022/2555 tähenduses, vaid turvaintsidendiga eIDAS-määruse tähenduses; ka sellistest intsidentidest tuleb pädevat asutust teavitada.

Lõikes 1 sätestatakse Euroopa digiidentiteedikukru pakkuja ja usaldusteenuse osutaja kohustus teavitada pädevat asutust 24 tunni jooksul turvaintsidendist, mis oluliselt mõjutab või võib mõjutada usaldusteenuse, Euroopa digiidentiteedikukru või selle kaudu osutatava teenuse turvalisust, töökindlust või usaldusvärsust; säte hõlmab nii tegelikke kui ka olulise mõjuga võimalikke turvaintsidente. 24 tunni tähtaeg tuleneb eIDAS-määrusest; see täpsustati kooskõlastusringil Riigi Infosüsteemi Ameti ettepanekul.

Lõikes 2 määratakse kindlaks teate sisu, mis võimaldab pädeval asutusel hinnata turvaintsidendi mõju ning otsustada vajalike meetmete üle.

Lõikes 3 antakse pädevale asutusele õigus nõuda täiendavat teavet ja dokumente, kui see on vajalik turvaintsidendi mõju hindamiseks või Euroopa Liidu õigusest tulenevate kohustuste täitmiseks.

§ 1 punkt 8. Paragrahvi 5 pealkirja täiendatakse, lisades sinna ka Euroopa digiidentiteedikukru pakkuja ja pakkumise.

§ 1 punkt 9. Paragrahvi 5 lõikega 1 lisatakse nõuete subjektiks ka Euroopa digiidentiteedikukru pakkuja ja objektiks Euroopa digiidentiteedikukru pakkumine. Samas jäetakse välja viide avalikult heakskiidetud ja kättesaadavatele spetsifikatsioonidele. Selle asemel viidatakse eIDAS-määruse rakendusaktidele, mis praeguseks määravad täpselt kindlaks, milliseid standardeid ja spetsifikatsioone tuleb järgida.

Lõikes 2 muudetakse kvalifitseeritud usaldusteenuse osutajalt nõutava kindlustuskatte summa suurust kõigi kindlustusjuhtumite kohta aastas. Senise ühe miljoni euro asemel nõutakse kahe miljoni euro suuruse kindlustuskatte olemasolu. Summa on olnud üle kümne aasta muutumatu ega suhestu enam praeguse hinnatasemega. Samas jääb iga üksiku kindlustusjuhtumi kohta nõutav kindlustuskate endiseks.

§ 1 punkt 10. Paragrahvi 5 lõikega 3 pikendatakse kvalifitseeritud usaldusteenuse osutaja tegevuslogi säilitamise tähtaega kümnele aastalt kaheteistkümnele aastale kirje loomisest arvates. Lõiget 3 muudetakse Politsei- ja Piirivalveameti ettepanekul. 2026. aasta kevadel tehtud eIDAS-i auditi raames andis audiitor hinnangu, et eIDAS-määruse ja rahvusvahelise ETSI standardi (ETSI EN 319 411-1, nõuded OVR-6.4.6-01 ja REG-6.3.4-17) kohaselt peavad logid ja tõendid sertifikaatide kasutustingimustega nõustumise kinnituse kohta olema kättesaadavad kuni 12 aastat. Kvalifitseeritud sertifikaadi maksimaalne kehtivusaeg on kuni viis aastat ja ETSI standardi kohaselt tuleb sertifikaatidega seotud sündmusi logida vähemalt seitse aastat pärast sertifikaadi kehtivuse lõppu. Tsiviilseadustiku üldosa seaduse (TsÜS) § 146 lõike 4 kohaselt on tahtliku rikkumise korral nõuete aegumistähtaeg kümme aastat. Kuna vaidlused võivad tekkida vahetult enne seda tähtaega 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 punkt 11. Senine paragrahvi 5 lõige 4 tunnistatakse kehtetuks, kuna üksikasjalikud nõuded tegevuse lõpetamise kavale on praeguseks kehtestatud eIDAS-määruse otsekohalduva rakendusaktiga.

§ 1 punkt 12. Paragrahvi 5 lõike 5 täiendus on vajalik, kuna isiku tuvastamist käsitlevad sätted on eIDAS-määruses muutunud. Viidatud artikli 24 lõike 1a punkt d käsitleb isiku tuvastamist füüsilise kohaloleku korral vastavalt riigisisesele õigusele. Lõikega täpsustatakse, kuidas sellises olukorras Eestis isikut tuvastatakse.

§ 1 punkt 13. Paragrahvi 5 lõikega 9 laiendatakse karistatuse puudumise nõuet ka usaldusteenuse osutaja alltöövõtjale. Täiendus on vajalik, et viia seaduse tekst kooskõlla uuenenud eIDAS-määruse ja komisjoni rakendusmääruse (EL) 2025/2530⁷ nõuetega.

§ 1 punkt 14. Paragrahvi 5 lisatakse lõiked 10–12, mis käsitlevad Euroopa digiidentiteedikukru pakkumist.

Lõige 10. Vastavalt eIDAS-määruse artikli 5a lõikele 2 peab Euroopa digiidentiteedikukru rakendustarkvara komponentide lähtekood olema avatud lähtekoodi litsentsiga. Samas antakse liikmesriikidele võimalus näha ette erand. Kõnesoleva sättega nähakse selline võimalus Eesti jaoks ette.

Lõige 11 näeb ette, et Euroopa digiidentiteedikukru pakkuja lisab kukru kasutaja isikutuvastusandmete hulka ka isikukoodi, mis komisjoni rakendusmääruse (EL) 2024/2977⁸ kohaselt on valikuline parameeter. Selle kaalutusotsuse mõju on käsitletud seletuskirja 6. peatükis.

Euroopa digiidentiteedikukru sihtrühm on Eesti isikukoodi omavad isikud: Eestis planeeritakse kukrut pakkuja Eesti kodanikele ja Eesti isikukoodi omavatele residentidele. Lõikes 11 nimetatud isikukood on Eesti isikukood. Teiste liikmesriikide digikukrud Eesti isikukoodi üldjuhul ei sisalda.

Lõige 12 sätestab Euroopa digiidentiteedikukru pakkuja õiguse teha päringuid isikut tõendavate dokumentide andmekogusse (ITDAK) ja rahvastikuregistrisse, kui see on vajalik isikutuvastusandmete kukrusse kandmiseks või nende ajakohasuse kontrollimiseks. Mõju nendele andmekogudele on kavandatud järgmiselt. Isikut tõendavate dokumentide andmekogust on planeeritud küsida teatud juhtudel isiku näokujutist (pilti). Rahvastikuregistrist on planeeritud küsida muid komisjoni rakendusmääruse (EL) 2026/1731 (millega muudetakse rakendusmäärust (EL) 2024/2977) tabelis 1 loetletud isikutuvastusandmeid, sealhulgas kasutaja sünnikohta. Kõik kohustuslikud isikutuvastusandmed peale näokujutise saadakse rahvastikuregistrist selle alusel, millega inimene ennast isikutuvastusandmete väljastamiseks tuvastas. Samuti nõuab eIDAS-määruse artikli 5a lõike 9 punkt c, et liikmesriigid tagavad võimaluse tunnistada Euroopa digiidentiteedikukru kasutaja surma korral kehtetuks. Andmeid päritakse isiku enda algatusel kukru väljastamisel või andmete ajakohasuse kontrollimisel ühekordselt ning need salvestatakse konkreetse inimese seadmes olemasse kukrusse; näokujutise hilisemal kasutamisel võetakse see seadmest, seega ei kaasne püsivat päringukoormust isikut tõendavate dokumentide andmekogule. Praeguse teadmise kohaselt ei eelda eelnõu rakendamine rahvastikuregistri ega isikut tõendavate dokumentide andmekogu arendusi, sest kasutatakse nende olemasolevaid teenuseid X-tee kaudu.

⁷ Komisjoni rakendusmäärus (EL) 2025/2530 (ELT L, 2025/2530).

⁸ Komisjoni 28. novembri 2024. aasta rakendusmäärus (EL) 2024/2977 (ELT L, 2024/2977, 4.12.2024).

Isikuandmete töötlemise õiguslikud alused on järgmised. Näokujutise saamiseks isikut tõendavate dokumentide andmekogust on aluseks Euroopa digiidentiteedikukru pakkuja ja andmeandja vaheline andmetöötlusleping ning komisjoni rakendusmääruse (EL) 2026/1731 tabelis 1 sätestatud isikutuvastusandmete koosseis kooskõlas isikuandmete kaitse üldmääruse (IKÜM) artikli 6 lõike 1 punktiga b. Rahvastikuregistrist andmete saamise alus on andmetöötlusleping ning rahvastikuregistri seaduse § 46 lõike 2 punkt 2 kooskõlas IKÜM-i artikli 6 lõike 1 punktidega b ja c. Andmetöötlus toimub analoogselt ID-kaardi ja mobiil-ID-ga, mille puhul erasektori teenusepakkuja töötleb isikuandmeid riigi tellimusel teenuse osutamiseks.

Põhiseaduse ja IKÜM-i valguses riivab Euroopa digiidentiteedikukru pakkumisel toimuv isikuandmete töötlemine põhiseaduse §-ga 26 tagatud eraelu puutumatust ja § 19 lõikest 1 tulenevat informatsioonilist enesemääramist, kuid riive on põhiseaduspärane. Töötlemise juhud ja kord on sätestatud vahetult kohalduvas eIDAS-määruses ja selle rakendusaktides, mis sisaldavad erandlikult üksikasjalikke ja siduvaid kaitsemeetmeid: andmete valikuline avaldamine ja kasutaja ainukontroll (artikli 5a lõike 4 punkt a), keeld koguda teenuse osutamiseks mittevajalikku teavet ja kohustus hoida kukru pakkumisega seotud isikuandmeid muudest andmetest loogiliselt lahus (artikli 5a lõige 14), jälgimis- ja seostamiskeeld (artikli 5a lõige 16) ning kasutamise vabatahtlikkus (artikli 5a lõige 15). Kukru kasutamine on vabatahtlik ja andmetöötlus toimub iga kord kasutaja algatusel; lisaks kohustab eIDAS-määrus kukru pakkujat võimaldama kasutajal valida, milliseid andmevälju ta soovib e-teenusega jagada. Isikutuvastusandmeid ja tõendeid säilitatakse kasutaja seadmes kasutaja kontrolli all, mitte riigi keskses andmekogus. Töötlemise õiguslik alus on IKÜM-i artikli 6 lõike 1 punkt c (õiguslik kohustus, mis tuleneb eIDAS-määrusest ja selle rakendusaktidest) ning punkt e koosmõjus artikli 6 lõikega 3 (avalikes huvides olev ülesanne). Liikmesriigi poolt või nimel toimuva töötlemise vastavust IKÜM-ile tuleb eIDAS-määruse artikli 5a lõike 17 kohaselt tõendada; selleks koostab Riigi Infosüsteemi Amet enne kukru kasutuselevõttu andmekaitsealase mõjuhinnangu (IKÜM-i artikkel 35). Riive eesmärk (identiteedikindlus ning teiste isikute õiguste ja vabaduste kaitse digikeskkonnas) on legitiimne ning valitud vahendid on sobivad, vajalikud ja mõõdukad, sest töödeldavate andmete ring piirdub eIDAS-määruses ja selle rakendusaktides sätestatud koosseisuga ning kasutajal säilib tegelik võimalus töötlemisest hoiduda, kasutades seniseid e-identimise vahendeid.

§ 1 punkt 15. Paragrahvi 6 pealkirja täiendatakse, lisades sinna ka Euroopa digiidentiteedikukru pakkuja.

§ 1 punkt 16. Kuna muudetav paragrahv 6 hõlmab kahte eri luba, täpsustatakse lõike 2 sõnastust nii, et see käib usaldusteenuse osutamise kohta. Samuti lisatakse loa kehtivuse aja kohta sõna „kuni“, sest luba tugineb auditi aruandele, mille aktuaalsus piirneb küll kahe aastaga, kuid audit võib olla tehtud ka oluliselt enne loataotluse esitamist.

§ 1 punkt 17. Paragrahvi 6 täiendatakse lõigetega 4 ja 5, kuna eIDAS-määruse kohaselt peab Euroopa digiidentiteedikukru pakkuja läbima sertifitseerimise, kus vastavushindamisasutus kinnitab määrusega ettenähtud nõuete täitmist ja väljastab selle kohta sertifikaadi. Sertifikaadi kehtivus on kuni viis aastat, misjärel tuleb sertifitseerimine uuesti läbida. Otstarbekas on ka loa kehtivusaeg hoida sünkroonis sertifikaadi kehtivusega. Lõikega 4 kehtestatav loakohustus laieneb Euroopa digiidentiteedikukru pakkumisele samamoodi nagu paragrahvi 6 lõikes 1 sätestatud loakohustus usaldusteenuse osutamisele. Nõue tuleneb eIDAS-määruse artikli 46a lõike 3 punktist a, mille kohaselt teeb järelevalveasutus Euroopa digiidentiteedikukru pakkujate üle järelevalvet nii ex ante kui ka ex post, tagamaks pakkujate ja nende pakutavate Euroopa

digiidentiteedikukrute vastavus määruse nõuetele. Loakohustus võimaldab pädeval asutusel veenduda kukru pakkuja nõuetele vastavuses enne pakkumise alustamist. Loakohustus riivab põhiseaduse §-s 31 sätestatud ettevõtlusvabadust, kuid riive on põhiseadusega kooskõlas. Riivel on legitiimne eesmärk: tagada, et isikutuvastuse ja isikuandmete töötlemise seisukohalt eriti tundlikku teenust pakub üksnes nõuetele vastav isik. Meede on sobiv ja vajalik, sest kukru nõuetele vastavust ei ole võimalik sama tõhusalt tagada üksnes tagantjärele tehtava järelevalvega, ning mõõdukas, kuna loa saamise tingimused piirduvad eIDAS-määrusest tulenevate nõuete täitmise kontrolliga ja loakohustus järgib sama loogikat, mis kehtib juba kvalifitseeritud usaldusteenuse osutajate suhtes.

Luba kehtib kuni viis aastat: loa kehtivusaeg on kooskõlas sertifikaadi kehtivusega ning kui sertifikaat mingil põhjusel kaotab kehtivuse (näiteks kui eIDAS-määruse artikli 5c lõikes 4 nimetatud korralist nõrkuste hindamist ei tehta või tuvastatud puudusi ettekirjutusest hoolimata ei kõrvaldata), tunnistab pädev asutus ka loa kehtetuks. Sätte eesmärk ei ole kehtestada, et luba kehtib igal juhul viis aastat.

§ 1 punktid 18 ja 19. Paragrahvi 7 lõike 3 punkti 1 muudetakse ja lõiget 3 täiendatakse punktiga 1¹, et loetleda täpsemalt dokumendid, mis on vajalikud loataotluse menetlemiseks. Vastavushindamiselt oodatakse ka kinnitust vastavuse kohta küberturvalisuse seaduse nõuetele, kuna eIDAS-määrus kohustab usaldusteenuse osutajat järgima ka Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555⁹ nõudeid, mis ei rakendu otse, vaid on Eestis üle võetud küberturvalisuse seadusega.

Punktis 1 täpsustati kooskõlastusringil Siseministeeriumi infotehnoloogia- ja arenduskeskuse märkuse alusel, et taotlusele lisatakse usaldusnimekirja lisatav teenuse sertifikaat selle olemasolu korral. Silmas peetakse usaldusnimekirja lisatavat teenuse sertifikaati, mitte vastavushindamisasutuse väljastatud sertifikaati; kuna kõigil teenustel sellist sertifikaati ei ole, esitatakse see üksnes olemasolu korral.

Punktis 1¹ nimetatud põhjendatud järeldus (koondjäreldus) usaldusteenuse ja selle osutaja vastavuse või mittevastavuse kohta tähendab audiitori kokkuvõtvat hinnangut usaldusteenuse ja selle osutaja eIDAS-määruse nõuetele ja seotud riigisisestele nõuetele vastavuse kohta. See võib sisalduda sertifikaadil või aruande põhidokumendis ning olla esitatud paari lausega või näiteks tabeli kujul. Samasisuline nõue oli varem majandus- ja taristuministri 26. oktoobri 2016. a määruse nr 64 „Usaldusteenuse osutaja ja usaldusteenuse vastavushindamise kord“ § 3 lõike 2 punktis 7; kuna nimetatud määrus muutub eelnõu kohaselt kehtetuks, tõstetakse nõue seadusesse. Vastavushindamisasutus peab kontrollima usaldusteenuse osutaja vastavust muu hulgas ka küberturvalisuse seadusele, millega on riigisiselt üle võetud direktiiv (EL) 2022/2555. Praktikas ei ole see nõue probleeme tekitanud.

§ 1 punkt 20. Paragrahvi 7 lõike 3 punktiga 3 lisatakse taotlemisel esitatavate dokumentide hulka ka teenuse riskianalüüs. Küberturvalisuse seadusest tulenevalt on kvalifitseeritud usaldusteenuse osutaja ülioluline üksus, kellel on kohustus teha riskianalüüs. Lisatud sättega nähakse loamenetlejale ette võimalus selle riskianalüüsiga tutvuda.

⁹ Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152).

Punktiga 4 lisatakse taotlemisel esitatavate dokumentide hulka tõend kindlustuse olemasolu kohta. Punktiga 5 nähakse ette Euroopa digiidentiteedikukru pakkuja loataotluse menetlemiseks vajalikud dokumendid: eIDAS-määruse artikli 5c lõike 2 kohaselt tuleb liikmesriigil edastada Euroopa Komisjonile selle e-identimise süsteemi kirjeldus, mille alusel Euroopa digiidentiteedikukrut pakutakse, Euroopa digiidentiteedikukru sertifikaat ja sertifitseerimise hindamise aruanne.

§ 1 punkt 21. Paragrahvi 7 lõige 4 tunnistatakse kehtetuks, kuna eIDAS-määruse rakendusaktid kirjeldavad ammendavalt standardeid, mille kohaselt tuleb usaldusteenuse osutamise põhimõtteid kirjeldada.

§ 1 punkt 22. Paragrahvi 8 punkti 1 lisatakse ka Euroopa digiidentiteedikukru pakkumine. Kuna loamenetlus käsitleb kahte eri luba, täpsustatakse punktiga 2, et seal peetakse silmas just usaldusteenuse osutaja auditit.

§ 1 punkt 23. Kuna loamenetlus käsitleb kahte eri luba, lisatakse punktiga 2¹ paragrahvi 8 viide eIDAS-määrusele, mille kohase sertifitseerimise peab Euroopa digiidentiteedikukkur olema läbinud. Kooskõlastusringil täpsustati Tarbijakaitse ja Tehnilise Järelevalve Ameti ettepanekul sätte sõnastust selliselt, et sertifitseerimise objektina nimetatakse Euroopa digiidentiteedikukrut, mitte selle pakkujat, ning viidatakse eIDAS-määruse artiklile 5c tervikuna. Nii Euroopa digiidentiteedikukru kui ka usaldusteenuse loa taotlemisel peab esitatav sertifikaat olema kehtiv.

§ 1 punkt 24. Paragrahvi 9 lõike 1 punkti 1 ehk loa andmisest keeldumist kirjeldavasse sättesse lisatakse ka Euroopa digiidentiteedikukru pakkuja luba puudutav.

§ 1 punkt 25. Paragrahvi 9 lõikesse 1 lisatud punkt 4 annab võimaluse loa andmisest keelduda, kui taotleja vastavushindamise aruandes või sertifitseerimise hindamise aruandes esineb olulisi vastuolusid. Tegemist on lõike 1 punktist 1 erineva alusega: punkt 1 kirjeldab olukorda, kus audiitor märgib selgesõnaliselt, et teenus või teenuse osutaja ei vasta nõuetele, punkt 4 aga olukorda, kus aruande järgi teenus või teenuse osutaja küll vastab nõuetele, kuid aruandes kirjeldatu alusel jõuab pädev asutus järeldusele, et esineb olulisi vastuolusid, mille kõrvaldamiseni ei ole võimalik luba väljastada. Olulise vastuoluga on tegemist näiteks siis, kui aruandes ei ole hinnatud riigisisesele õigusele vastavust, vastavust on hinnatud valede või aegunud nõuete alusel või nähtub aruandest, et seda on kopeeritud teise aruande pealt sisse süvenemata. Need näited pärinevad tegelikust järelevalvepraktikast. Üksnes vormiline või tähendust mittemuutev ebatäpsus loa andmisest keeldumise alust ei anna. Selline piiritus tagab kooskõla põhiseaduse §-st 10 ja § 13 lõikest 2 tuleneva õigusselguse põhimõttega: loa taotleja jaoks on ettenähtav, millise puuduse korral võib loa andmisest keelduda.

§ 1 punkt 26. Paragrahvi 9 lõiget 2 täiendatakse, selgitamaks, et majandustegevuse seadustiku üldosa seaduse §-s 37 sätestatud loa kehtetuks tunnistamise alused kehtivad ka kõnesoleva seaduse loamenetluse korral.

§ 1 punkt 27. Paragrahvi 9 lõike 2 punktide 1–3 sõnastust muudetakse nii, et hõlmatud ei oleks ainult kvalifitseeritud usaldusteenused, vaid ka Euroopa digiidentiteedikukru pakkumise teenus.

§ 1 punkt 28. Paragrahvi 9 lõike 3 sõnastust muudetakse nii, et hõlmatud ei oleks ainult kvalifitseeritud usaldusteenused, vaid ka Euroopa digiidentiteedikukru pakkumise teenus.

§ 1 punkt 29. Paragrahvi 9 lõike 4 sõnastust muudetakse, et kajastada olukorda, kus usaldusnimekirja kirjeid ei kustutata, vaid neid muudetakse, et need peegeldaksid tegelikku kehtivuse seisu.

§ 1 punkt 30. Paragrahvi 10 muudetakse, sõnastades lõike 3 selliselt, et kvalifitseerimata usaldusteenuse osutaja ja usaldusteenus kantakse usaldusnimekirja kuni kaheks aastaks. Sõna „kuni“ lisati kooskõlastusringil Riigi Infosüsteemi Ameti ettepanekul, et viia sätte sõnastus kooskõlla usaldusnimekirja kandmise üldise loogikaga: usaldusnimekirja kandmine peab olema kooskõlas väljastatud vastavushindamise sertifikaadiga. Vastavushindamise sertifikaat, tegevusluba ning usaldusnimekirja andmed peavad olema omavahel alati kooskõlas. Vastavushindamise sertifikaat väljastatakse kaheks aastaks, kuid tegevusloa menetlus võib toimuda mõnevõrra hiljem ning seetõttu võib ka usaldusnimekirja lisamise periood olla mõnevõrra lühem.

§ 1 punkt 31. Paragrahvi 12 pealkiri muudetakse, asendades selles sõna „vastavushindamise“ sõnaga „sertifitseerimise“. Uuenenud eIDAS-määrus ja selle rakendusaktid kirjeldavad detailselt usaldusteenuste vastavushindamist, kuid lisandunud on Euroopa digiidentiteedikukru sertifitseerimise protseduur, milleks vajaliku kava peab iga liikmesriik ise looma.

§ 1 punkt 32. Paragrahvi 12 lõige 2 tunnistatakse kehtetuks, sest viide usaldusteenuse osutaja ja usaldusteenuse vastavushindamise korra määrusele on muutunud ebavajalikuks. Uuendatud eIDAS-määruse alusel vastu võetud komisjoni rakendusmäärus (EL) 2025/2162¹⁰ seab nõuded vastavushindamisele, muutes seega Eesti määruse ebavajalikuks. Samas eeldab uuendatud eIDAS-määrus, et liikmesriigid loovad riigipõhise Euroopa digiidentiteedikukru sertifitseerimise kava.

§ 1 punkt 33. Paragrahvi 12 täiendatakse lõigetega 2¹–2³, mis käsitlevad Euroopa digiidentiteedikukrute sertifitseerimist.

Lõige 2¹. Uuendatud eIDAS-määrus ja komisjoni rakendusmäärus (EL) 2024/2981¹¹ näevad ette, et Euroopa digiidentiteedikukrute sertifitseerimine toimub vastavalt liikmesriikide loodud kavadele. Sättega pannakse selliste kavade loomise, ajakohasena hoidmise ja läbivaatamise kohustus valdkonna eest vastutavale ministeeriumile. Sertifitseerimise ulatuse, sealhulgas sertifitseeritavate komponentide ja nõuete ulatuse, määrab komisjoni rakendusmäärus (EL) 2024/2981. Euroopa digiidentiteedikukru väljaandmise etappide kohta on Riigi Infosüsteemi Amet avaldanud analüüsi oma veebilehel.¹²

Lõikega 2² nähakse ette, et valdkonna eest vastutav ministeerium avaldab nende kavade ajakohased versioonid internetis.

Lõige 2³. Vastavalt eIDAS-määrusele sertifitseerivad Euroopa digiidentiteedikukruid liikmesriikide määratud vastavushindamisasutused. Selle sättega määratletakse, millised vastavushindamisasutused tulevad sertifitseerimiseks kõne alla. Konkreetne vastavushindamisasutus leitakse hankeprotsessi käigus.

§ 1 punkt 34. Paragrahvi 13 pealkirja täiendatakse, kuna muudatustest teavitamine peab hõlmama ka Euroopa digiidentiteedikukrut.

¹⁰ Komisjoni rakendusmäärus (EL) 2025/2162 (ELT L, 2025/2162).

¹¹ Komisjoni 28. novembri 2024. aasta rakendusmäärus (ELT L, 2024/2981, 4.12.2024).

¹² <https://www.ria.ee/riigi-infosusteem/elektroonilise-identiteedi-teenused/digikukkur-eudi-wallet>

§ 1 punkt 35. Paragrahvi 13 lõike 1 muudatusega viiakse usaldusteenuse muudatustest teavitamise tähtajad kooskõlla uuendatud eIDAS-määruses sätestatuga. Ühtlasi laiendatakse muudatustest teavitamise kohustust ka Euroopa digiidentiteedikukru pakkujale.

§ 1 punkt 36. Paragrahvi 13 lõiked 3 ja 4 muudetakse. Lõikes 3 seatakse pädevale asutusele tähtaeg, mille jooksul tuleb teada anda taotluse uuesti esitamise vajadusest. Ühtlasi laiendatakse sätet ka Euroopa digiidentiteedikukru pakkujale.

Lõikes 4 asendatakse väljend „usaldusnimekirjas kajastatud andmete muutmise“ väljendiga „teenuse muutmise taotluse“. Ilma muudatuseta tuleks riigilõivu maksta ainult siis, kui muutuvad usaldusnimekirjas kajastatud andmed. Praktikas enamasti andmed usaldusnimekirjas ei muutu, kuid muudatuse läbivaatamine ja kinnitamine nõuab pädevalt asutuselt omajagu ressursi. Lisaks ei oleks senise sõnastusega kaetud Euroopa digiidentiteedikukru muudatused, mida usaldusnimekirja ei kanta. Muudatus tehti kooskõlastusringil Riigi Infosüsteemi Ameti ettepanekul.

§ 1 punkt 37. Paragrahvi 18 täiendatakse lõikega 5, kuna olenevalt tehnilisest teostusest ja teenuse osutamise korraldusest ei pruugi usaldusteenus võimaldada kord peatatud sertifikaatide kehtivust uuesti taastada. Sellises olukorras lähtub usaldusteenuse osutaja sertifikaatide kehtivuse peatamisel sertifikaatide kehtetuks tunnistamise kohta sätestatust.

§ 1 punkt 38. Paragrahvi 19 lõiget 2 täiendatakse punktiga 4, millega lisatakse sertifikaatide kehtetuks tunnistamise taotlejate loetellu ka isikut tõendavate dokumentide väljaandja, kuid teatud pädevusepiirangutega. Isikut tõendavate dokumentide väljaandja võib taotleda sertifikaatide kehtetuks tunnistamist ainult isikut tõendavate dokumentide seaduse § 2 lõike 2 punktides 1–1² nimetatud dokumendile kantud sertifikaatide puhul ja ainult neil alustel, mis on isikut tõendavate dokumentide seaduses sätestatud. Varem oli sama tähendus e-identimise ja e-tehingute usaldusteenuste seaduse § 19 lõikel 5, kuid senine sõnastus on tekitanud praktikas erinevaid tõlgendamisvõimalusi, eelkõige selle puhul, kas vastavad isikut tõendavate dokumentide seaduse normid on erinormid e-identimise ja e-tehingute usaldusteenuste seaduse § 19 normide suhtes. Selguse huvides nimetatakse isikut tõendavate dokumentide väljaandjat edaspidi teiste võimalike kehtetuks tunnistamise taotlejate loetelus. Kooskõlastusringil täpsustati Siseministeeriumi märkuse alusel, et säte viitab isikut tõendavate dokumentide seaduse § 2 lõike 2 punktides 1–1² nimetatud dokumentidele ehk dokumentidele, millele e-identimise ja e-tehingute usaldusteenuste seadus kohaldub; reisidokumendid jäävad sätte kohaldamisalast välja.

§ 1 punkt 39. Paragrahvi 19 lõike 4 punkti 5 muudetakse, täpsustades, et sertifikaadi kehtetuks tunnistamise alus on sertifikaadi omaja tegevuse lõpetamise tõttu tema kustutamine sertifitseerimise registrist. Täpsustatakse sõnastust (sertifitseerimise register), et eristada seda registrit eelnõuga asutatavast digiidentiteedikukrule tuginevate isikute registrist. Muudatus on täpsustav ega muuda sätte senist sisu.

§ 1 punkt 40. Paragrahvi 19 lõikega 4 lisatava sätte eesmärk on näha ette selge õiguslik alus sertifikaatide kehtetuks tunnistamiseks, kui on ilmnenu, et sertifikaatide väljastamine ei vasta usaldusteenuse loa tingimustele või eIDAS-määruses või kõnesolevas seaduses sätestatud nõuetele. Muus osas on sätte senine sõnastus laiahaardeline ega ole tekitanud praktikas küsitavusi ja vastuolulisi tõlgendamisvõimalusi.

§ 1 punkt 41. Paragrahvi 19 lõiget 5 muudetakse, jättes välja viite isikut tõendavate dokumentide seaduses loetletud sertifikaadi kehtetuks tunnistamise alustele ja korrale, kuna

samatähenduslik säte lisatakse selguse eesmärgil eelnõuga e-identimise ja e-tehingute usaldusteenuste seaduse § 19 lõikesse 2. Samas lisatakse usaldusteenuse osutajale kohustus teavitada enne sertifikaadi kehtetuks tunnistamist sellest isikut tõendava dokumendi väljaandjat.

Teavitamiskohustus puudutab isikusertifikaate, mitte juur- ega vahesertifikaate. Teavitamise eesmärk on tagada, et dokumendi väljaandja saaks vajaduse korral teha vajalikud otsused füüsilise dokumendi osas. Teavitamine võib toimuda ka tehniliste lahenduste kaudu. Eelneva teavitamise all peetakse silmas mõistlikku aega; täpse tähtaja sätestamist ei peetud eelnõu koostamisel vajalikuks. Ka selles sättes viidatakse isikut tõendavate dokumentide seaduse § 2 lõike 2 punktides 1–1² nimetatud dokumentidele.

§ 1 punkt 42. Lisanduva paragrahvi 23¹ kehtestatakse riikliku järelevalvemenetluse käigus ettekirjutuse täitmata jätmise korral rakendatava sunniraha igakordseks ülemmääraks 500 000 eurot või kuni 1 protsent usaldusteenuse osutaja eelmise majandusaasta ülemaailmsest kogukäibest, olenevalt sellest, kumb summa on suurem. Kooskõlastusringi tulemusel vähendati Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu ettepaneku tõttu sunniraha ülemmäär 5 000 000 eurolt 500 000 eurole ehk kümme korda. Samas on piisavalt suur piirmäär vajalik, et säilitada tõhus võimalus mõjutada Euroopa digiidentiteedikukru pakkujat õiguskuulekale tegevusele ning täita seeläbi eIDAS 2 määruse artikli 16 lõikes 1 sätestatud kohustus. eIDAS 2 määruse artikli 16 lõige 1 kohustab liikmesriike kehtestama mõjusad, proportsionaalsed ja hoiatavad normid eIDAS-määruse rikkumise eest kohaldatavate karistuste kohta; see säte kohaldub lisaks usaldusteenuse osutajatele ka Euroopa digiidentiteedikukru pakkujale. Samas otsustati eelnõu koostamise käigus, et Euroopa digiidentiteedikukru pakkujale ei nähta ette trahve selliselt, nagu seda on tehtud usaldusteenuse osutaja suhtes (eelnõukohane e-identimise ja e-tehingute usaldusteenuste seaduse § 23³). See lähtus kaalutlusest, et kuna eIDAS 2 määruse artikli 16 lõikes 2, mis näeb ette trahvimäärad, ei nimetata Euroopa digiidentiteedikukru pakkujaid, oleks trahvi ettenägemine kukru pakkujale ülereguleerimine (nn *gold-plating*; vt ka „Ametniku Euroopa Liidu käsiraamatu“ peatükki 8.3.5).¹³ Seega on piisavalt suur sunniraha ülemmäär (500 000 eurot) sobiv tasakaalupunkt eIDAS 2 määruse artikli 16 lõikes 1 sätestatud kohustuse täitmiseks Euroopa digiidentiteedikukru pakkuja suhtes olukorras, kus kukru pakkujale ei ole trahve ette nähtud. Pädev asutus peab sunniraha määramise korral hindama, millises määras on sunniraha rakendamine konkreetsel juhul proportsionaalne. Vähendamine puudutab ülemmäärade fikseeritud osa. Käibepõhine alternatiiv (kuni 1 protsent kogukäibest, kui see on suurem) säilib, mistõttu suure käibega kohustatud isiku puhul ülemmäär ei muutunud.

§ 1 punkt 43. Eelnõuga lisatava peatüki 3¹ „Teabevahetus“ ning § 23² „Teabevahetus teenuse osutajatega“ eesmärk on tagada Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 48a rakendamine, mille kohaselt tuleb liikmesriigil koguda ja Euroopa Komisjonile esitada statistilisi andmeid, sealhulgas Euroopa digiidentiteedikukru ja kvalifitseeritud usaldusteenuste toimimise kohta, ning avaldada need üleliiduliselt. Selleks kehtestatakse määras (EL) nr 910/2014 nimetatud teenuse osutajale statistika kogumiseks ja esitamiseks vajalik teabevahetuskohustus. Andmeid kogutakse teenuse osutajalt vajaduspõhiselt ja proportsionaalsuse põhimõttel.

§ 1 punkt 44. Lisanduva peatükiga 3² kehtestatakse trahvimäärade ülemmäärad seaduse nõuete rikkumise eest. Kohustus sellised trahvimäärad kehtestada tuleneb eIDAS-määruse artiklist 16. Peatükis nimetatud väärtegade kohtuväliseks menetlejaks määratakse Riigi Infosüsteemi Amet. Trahvimäärade ülemmäärad tuginevad eIDAS 2 määruse artikli 16 lõikele 2, mille punkti a

¹³ <https://riigikantselei.ee/el-poliitika-julgeolek-ja-riigikaitse/est-euroopa-liidus/ametniku-euroopa-liidu-kasiraamat/ulereguleerimine-ehk-direktiivis-satestatust-rangemate-nouete-kehtestamine>

kohaselt on füüsilisest isikust usaldusteenuse osutajale kohaldatava rahatrahvi ülemmäär 5 000 000 eurot ja punkti b kohaselt juriidilisele isikule 5 000 000 eurot või 1 protsent tema eelmise majandusaasta ülemaailmsest kogukäibest, olenevalt sellest, kumb on suurem. Karistusseadustiku § 47 üldmäärad (lõike 1 kohaselt füüsilisele isikule kuni 300 trahviühikut ja lõike 2 kohaselt juriidilisele isikule kuni 400 000 eurot) jäävad nendest määradest väiksemaks. Samas võib KarS-i § 1 lõike 1 järgi sätestada karistusseadustiku üldosast erisusi muudes seadustes, kui seda nõuab reguleeritava valdkonna eripära. Praegusel juhul on kõrgemad trahvimäärad sätestatud konkreetse valdkonna otsekohalduvas Euroopa Liidu määruses. Selliste trahvimäärade kehtestamine on kooskõlas Eesti Vabariigi põhiseaduse §-ga 23, kuna väärtekoosseisud (kõnesoleva seaduse § 5, § 6 lõige 1 ja § 13 lõige 1) on piisavalt selgelt sõnastatud ning trahvimäärade ülemmäärad on seaduses arvuliselt fikseeritud. Karistuste suurus on proportsionaalne põhiseaduse § 32 tähenduses, kuna trahvimäärade ülemmäärad on kooskõlas eIDAS 2 määrusest tuleneva kohustusega ning pädev asutus peab trahvi määra hindama iga üksikjuhtumi puhul karistuse proportsionaalsust.

§ 1 punkt 45. Paragrahvi 25 pealkirja täiendatakse pärast tekstiosa „tempel ning“ sõnaga „sertifitseerimise“, nii et pealkiri nimetab sertifitseerimise registrisse kantud sertifitseerimisteenuse osutajat. Täpsustatakse sõnastust (sertifitseerimise register), et eristada seda registrit eelnõuga asutatavast digiidentiteedikukrule tuginevate isikute registrist. Muudatus on täpsustav ega muuda sätte senist sisu.

Eelnõu §-ga 2 muudetakse riigilõivuseadust.

§ 2 punkt 1. Paragrahvi 116² pealkirja muudatus on vajalik, kuna loamenetlusse lisandub Euroopa digiidentiteedikukru pakkuja loa menetlemine.

§ 2 punktid 2 ja 3. Paragrahvi 116² lõigete 1 ja 2 muutmine ning lõike 3 täiendamine on vajalik, kuna loamenetlusse lisandub Euroopa digiidentiteedikukru pakkuja loa menetlemine. Riigilõivust kaetakse Euroopa digiidentiteedikukru pakkuja loataotluse menetlemise kulud, mis hinnanguliselt ei erine usaldusteenuse loataotluse menetlemisega kaasnevatest kuludest.

Eelnõu §-ga 3 muudetakse karistusseadustikku.

§ 3. Euroopa digiidentiteedikukkur pakub samasuguseid funktsioone või isegi enam kui mitu karistusseadustiku §-s 350 nimetatud dokumenti. Otstarbekas on näha ette võimalus käsitleda Euroopa digiidentiteedikukruga seotud süütegusid samadel alustel kui näiteks digitaalse isikutunnistusega seotud süütegusid. Selleks lisatakse tähtsa isikliku dokumendi loetellu ka Euroopa digiidentiteedikukkur. Otstarbekas on lisada loetellu ka e-identimise vahendid, mida ei ole küll välja antud isikut tõendavate dokumentide seaduse alusel, kuid mis on e-identimise ja e-tehingute usaldusteenuste seaduses sätestatud korras hinnatud samaväärseks vahendiga, mille usaldusväärsuse tase on „kõrge“.

4. Eelnõu terminoloogia

Eelnõuga võetakse kasutusele järgmised uued terminid, mis tulenevad eIDAS-määrusest: „Euroopa digiidentiteedikukkur“ (eIDAS-määruse artikli 3 punkt 42), „Euroopa digiidentiteedikukru pakkuja“ ja „digiidentiteedikukrule tuginev isik“ (eIDAS-määruse artikli 3 punkt 52 koostoimes artikliga 5b). Kooskõlas hea õigusloome ja normitehnika eeskirja § 18 lõikega 2 on eelnõus kasutatavad terminid kooskõlas Euroopa Liidu õigusakti eestikeelses tekstis kasutatud terminitega. Uue andmekogu nimetusena võetakse kasutusele „digiidentiteedikukrule tuginevate isikute register“. Rohkem uusi termineid ei looda. Eelnõus

kasutatavad terminid on kooskõlas e-identimise ja e-tehingute usaldusteenuste seaduses, riigilõivuseaduses ja karistusseadustikus juba kasutusel olevatega.

5. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu on kooskõlas Euroopa Liidu õigusega. Eelnõu on seotud eIDAS-määruse (mida on muudetud eIDAS 2 määrusega) ja selle alusel antud Euroopa Komisjoni rakendusmääruste rakendamisega. Euroopa Liidu toimimise lepingu artikli 288 kohaselt on määrus tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides, mistõttu määrust riigisisesele õigusesse üle ei võeta ega selle sätteid riigisiseses õiguses ei korrata. Eelnõu sisaldab üksnes riigisiseseid rakendusmeetmeid, mida määrus liikmesriigilt nõuab või võimaldab: pädevate asutuste määramine (eIDAS-määruse artikli 7 punkt f ning artiklid 5a–5e, 9, 12, 46a ja 46b), kükrule tuginevate isikute riikliku registri asutamine (artikkel 5b ja rakendusmäärus (EL) 2025/848), karistusnormide kehtestamine (artikkel 16) ning liikmesriigile jäetud kaalutlusruumi kasutamine (muu hulgas avatud lähtekoodi erand artikli 5a lõike 2 alusel, isikukoodi kandmine kukrusse rakendusmääruse (EL) 2024/2977 alusel ja isiku tuvastamise viis füüsilise kohaloleku korral artikli 24 lõike 1a punkti d alusel).

Kuna eelnõukohase seadusega ei võeta üle direktiivi, vaid rakendatakse määrust, ei lisata eelnõule normitehnilist märkust ega koostata direktiivi ülevõtmise vastavustabelit. Eelnõu ja eIDAS 2 määruse sätete seoste ülevaade on esitatud seletuskirja lisas 2 (vastavustabel). Eelnõu ei sisalda sätteid, mis läheksid kaugemale eIDAS 2 määruse nõuetest, välja arvatud liikmesriigile sõnaselgelt jäetud valikute kasutamine, mille põhjendused on esitatud seletuskirja 3. ja 6. peatükis.

6. Seaduse mõjud

Eelnõu on seotud eIDAS 2 määruse rakendamisega. Kuna Euroopa Liidu määrus on Euroopa Liidu toimimise lepingu artikli 288 kohaselt tervikuna siduv ja vahetult kohaldatav, tulenevad sihtrühmade põhilised õigused ja kohustused vahetult eIDAS 2 määrusest ning tekivad olenemata eelnõust. Eelnõu käsitleb üksnes määruse rakendamiseks vajalikke või lubatud riigisiseseid meetmeid: Justiits- ja Digiministeeriumi 2026. aasta kaasamisplaani kohaselt muudetakse e-identimise ja e-tehingute usaldusteenuste seadust, riigilõivuseadust ja karistusseadustikku ning muudatuste sisuks on eelkõige riigisiselised rollid, järelevalve ja karistused.¹⁴ Eelnõu põhilahendused on järgmised: Riigi Infosüsteemi Amet määratakse pädevaks asutuseks ja järelevalveasutuseks (eelnõu § 1 punkt 3), riigile luuakse võimalus Euroopa digiidentiteedikukru pakkumine ja selleks vajalikud tegevused allhankida (eelnõu § 1 punkt 3), asutatakse digiidentiteedikukrule tuginevate isikute register (eelnõu § 1 punkt 6) ning kehtestatakse Euroopa Liidu nõuetele vastavad sunniraha- ja trahvimäärad (eelnõu § 1 punktid 42 ja 44). Selguse huvides kirjeldatakse 6. peatükis nii eelnõu enda kui ka eIDAS 2 määruse kohaldamisega kaasnevaid mõjusid, sest sihtrühmade jaoks avalduvad need koos ja lahutamatu. Kavandatavad muudatused avaldavad mõju mitmes valdkonnas, hõlmates sotsiaalset mõju (sh e-teenuste kasutamise võimaluste laienemine), mõju riigi julgeolekule ja välissuhetele (digiidentiteedi taristu turvalisus ja piiriülene koostalitlusvõime), mõju majandusele (halduskoormus, ettevõtjate kohustused ja uute teenuste arendamise võimalused) ning mõju riigiasutuste ja kohaliku omavalitsuse korraldusele (uued ülesanded, järelevalve ja infosüsteemide arendamine).

¹⁴ Justiits- ja Digiministeeriumi kaasamisplaan: olulisemad algatused 2026. aastal. Justiits- ja Digiministeerium: 2026. <https://www.justdigi.ee/sites/default/files/documents/2026-03/JDM%20kaasamisplaan%202026.pdf>

Eelnõu kohta ei ole koostatud väljatöötamiskavatsust (vt seletuskirja punkt 2). Eesti seisukohad Euroopa Komisjoni ettepaneku COM(2021) 281 (final) kohta kiitis heaks Vabariigi Valitsus ja neid arutas Riigikogu Euroopa Liidu asjade komisjon.¹⁵ Euroopa Liidu tasandil on olemas ka põhjalik mõjuhindang. Komisjoni mõjuhindangu¹⁶ kohaselt oli kehtiva eIDAS-raamistiku põhiprobleem piiriülese e-identimise piiratud ja ebaühtlane kasutatavus – mõjuhindangu koostamise ajaks oli e-identimise süsteemist teavitanud vaid 14 liikmesriiki, teavitatud süsteemid (Eesti puhul muu hulgas ID-kaart ja mobiil-ID) katsid hinnanguliselt 59% liidu elanikkonnast ning teenusepakkujate vastuvõtuvõime oli ebaühtlane. Komisjoni mõjuhindangut toetavas uuringus¹⁷ hinnati eri poliitikavalikute kulusid ja tulusid avaliku sektori asutustele, internetiteenuste osutajatele, vastavushindamisasutustele, usaldusteenuse osutajatele ja e-identimise vahendite pakkujatele. Kuna väljatöötamiskavatsust ei koostatud, esitatakse 6. peatükis mõjude analüüs väljatöötamiskavatsuse tasemele vastava põhjalikkusega, tuginedes muu hulgas nimetatud Euroopa Liidu tasandi mõjuhindangule.

Mõjude hindamisel on ajaline raamistik järgmine. eIDAS 2 määrus jõustub 20. mail 2024. Määruse artikli 5a lõike 1 kohaselt peab iga liikmesriik tegema vähemalt ühe Euroopa digiidentiteedikukru kättesaadavaks 24 kuu jooksul artikli 5a lõikes 23 ja artikli 5c lõikes 6 osutatud rakendusaktide jõustumisest¹⁸, mis seab tähtajaks 24 detsembri 2026. Samast ajast muutub sisuliselt kohaldatavaks avaliku sektori asutuste kohustus aktsepteerida digikukrut e-identimist ja e-autentimist nõudvatele internetipõhistele teenustele juurdepääsul (artikli 5f lõige 1).¹⁹ Erasektori digiidentiteedikukrule tuginevatele isikutele, kellelt õigusakti või lepingulise kohustuse alusel nõutakse veebis kasutaja tugevat autentimist, muutub aktsepteerimiskohustus kohustuslikuks hiljemalt 36 kuu möödumisel nimetatud rakendusaktide jõustumisest ehk 2027. aasta lõpust (artikli 5f lõige 2).²⁰

Peamised sihtrühmad on:

- 1) füüsilised isikud ehk digikukru potentsiaalsed kasutajad – ligikaudu 1,36 miljonit Eesti elanikku²¹ ja teiste liikmesriikide kukrute kasutajad, kes soovivad Eesti teenustele juurde pääseda;
- 2) avaliku sektori asutused, kes osutavad e-identimist nõudvaid internetipõhiseid teenuseid, sealhulgas kõik 78 kohaliku omavalitsuse üksust;
- 3) erasektori digiidentiteedikukrule tuginevad isikud, kellelt õigusakti või lepingulise kohustuse alusel nõutakse veebis tugevat kasutaja autentimist, muu hulgas panganduse, finantsteenuste,

¹⁵ Eesti seisukohad Euroopa digiidentiteedi raamistiku määruse eelnõu (COM(2021) 281 final) kohta. EISI toimik 21-0812. <https://eelroud.valitsus.ee/main/mount/docList/30d59321-40e8-4d18-9e41-5676c2cbf811?activity=3>. Heaks kiidetud Vabariigi Valitsuse 30. septembri 2021. a istungil. Riigikogu toimik 1-2/21-365/6.

¹⁶ European Commission. Commission Staff Working Document. Impact Assessment Report. SWD(2021) 124 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0124>

¹⁷ European Commission. Study to support the impact assessment for the revision of the eIDAS regulation. 9.06.2021. <https://digital-strategy.ec.europa.eu/en/library/study-support-impact-assessment-revision-eidas-regulation>

¹⁸ Digikukkur ehk Euroopa Liidu digiidentiteedirakendus (EUDI Wallet). Riigi Infosüsteemi Ameti koduleht, 01.06.2026. <https://www.ria.ee/riigi-infosusteem/elektroonilise-identiteedi-teenused/digikukkur-eudi-wallet>

¹⁹ Cybernetica AS. Digikukru III etapi analüüs (Digiidentiteedikukru analüüside kogumik). Versioon 1.0, 8.04.2026. Tellija: Riigi Infosüsteemi Amet. Ptk 10 (Euroopa digiidentiteedikukrute aktsepteerimine avaliku sektori tuginevate isikute poolt). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuus.pdf>

²⁰ Vt viide 16. <https://www.ria.ee/riigi-infosusteem/elektroonilise-identiteedi-teenused/digikukkur-eudi-wallet>

²¹ Statistikaameti andmebaas [e-andmebaas]. RV021. <https://stat.ee/et/avasta-statistikat/valdkonnad/rahvastik/rahvaarv>

side, transpordi, energeetika, tervishoiu ja hariduse valdkonnas, välja arvatud mikro- ja väikeettevõtjad, kes on aktsepteerimiskohustusest vabastatud;

4) usaldusteenuse osutajad, sealhulgas kvalifitseeritud usaldusteenuse osutajad ja uut liiki usaldusteenuste (elektrooniliste tõendite väljastamine, e-allkirja kaugloomise vahendite haldamine) osutajad;

5) autentsete allikate eest vastutavad asutused ehk riiklike andmekogude pidajad, kelle andmeid kasutatakse elektrooniliste tõendite väljastamisel ja kontrollimisel, näiteks Siseministeerium rahvastikuregistri ning Politsei- ja Piirivalveamet isikut tõendavate dokumentide andmekogu vastutava töötlejana;

6) Euroopa digiidentiteedikukru pakkuja;

7) Riigi Infosüsteemi Amet kui pädev asutus, järelevalveasutus ja digikukru pakkumise korraldaja;

8) Andmekaitse Inspektsioon (AKI) andmekaitsealase järelevalve tegijana ning

9) Justiits- ja Digiministeerium kui sertifitseerimisskeemi väljatöötamise eest vastutaja.

6.1. Sotsiaalne mõju, sh demograafiline mõju

Mõju avaldub kõigile füüsilistele isikutele, kes hakkavad digikukrut kasutama avalikele ja erasektori teenustele juurdepääsuks nii Eestis kui ka mujal Euroopa Liidus. Digikukkur väljastatakse, seda kasutatakse ja see tunnistatakse füüsiliste isikute jaoks kehtetuks tasuta (eIDAS 2 määrusega kehtestatud artikli 5a lõige 13) ning kukkur peab pakkuma kõigile füüsilistele isikutele vaikimisi ja tasuta võimalust anda kvalifitseeritud e-allkiri mittekutselistel eesmärkidel (artikli 5a lõike 4 punkt g). Digikukkur on kavandatud täiendava riikliku isikutuvastusvahendina ID-kaardi ja teiste kehtivate eID-vahendite kõrval, mitte nende asendajana.²² Kasutajal on täielik kontroll oma andmete üle: ta saab andmeid valikuliselt avaldada, kasutada varjunimesid ning jälgida kõiki tehinguid ühise töölaua kaudu (artikli 5a lõiked 4 ja 14). Võrreldes kehtivate e-identimise vahenditega suureneb seega inimese teadlikkus ja kontroll selle üle, milliseid tema andmeid, kellele ja millal edastatakse – see on selgelt positiivne mõju eraelu puutumatusse ja informatsioonilisele enesemääramisele. Ka Euroopa Komisjon toob digikukru peamise kasuna kodanikele esile lihtsama juurdepääsu avalikele ja erasektori teenustele, asjaajamisele kuluva aja ja halduskoormuse vähenemise ning andmete valikulise avaldamise, mis vähendab oluliselt profileerimise võimalust; teatavates olukordades võimaldab kukkur identifitseerida end täiesti anonüümselt.²³

Eelnõuga tehtav oluline riigisisene kaalutusotsus on isikukoodi kandmine kukrusse. Kuigi eelnõuga korraldatakse otsekohalduva Euroopa Liidu määruse rakendamist Eestis, on siiski valikukohti, mida Euroopa Liidu määrus ette ei kirjuta. Eelnõus nähakse ette, et lisaks kohustuslikele isikutuvastusandmetele lisatakse Eestis väljaantavate Euroopa digiidentiteedikukrute isikutuvastusandmete hulka ka Eesti isikukood, mis rakendusmääruse (EL) 2024/2977 kohaselt ei ole kohustuslik, vaid valikuline parameeter. Isikukoodi lisamine annab Eesti inimestele võimaluse kasutada harjumuspäraseid e-teenuseid ka Euroopa digiidentiteedikukru abil. Vastasel juhul oleks Euroopa digiidentiteedikukru laialdane kasutuselevõtt Eestis raskendatud ning selle kasutamine jääks piiratud ulatusega, peamiselt piiriüleste teenuste kasutamisega seotud juhtudesse. See otsus puudutab kogu Eesti elanikkonda, kuid otsuse enda mõju tähtsus on mõõdukas, kuna e-teenuste kasutamiseks on inimestel ka alternatiivid. Isikukoodi digikukrusse kandmine on vajalik, sest Eesti e-teenuste isikutuvastus põhineb valdavalt isikukoodil ning ilma selleta ei oleks kukkur Eesti teenustes

²² Vt viide 16. <https://www.ria.ee/riigi-infosustem/elektroonilise-identiteedi-teenused/digikukkur-eudi-wallet>

²³ Benefits. EU Digital Identity Wallet. Euroopa Komisjoni veebileht, 23.10.2025. <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487811/Benefits>

seniste riiklike e-identimise vahenditega samaväärselt kasutatav. Meede on proportsionaalne: isikukood on avalik-õiguslikult reguleeritud ja laialdaselt kasutatav identifikaator, mille töötlemine digikukrus piirdub isikutuvastusandmete koosseisuga ega too kaasa uue andmekogu loomist. Kaalutud alternatiiv – digikukru väljaandmine ilma isikukoodita – jätkaks kukru kasutusala peamiselt piiriüleseks ega täidaks eesmärki. Andmekaitseriske, sealhulgas isikukoodi ülemäärase avaldamise riski, maandavad eIDAS-määruse nõuded andmete valikulise avaldamise kohta: kasutaja otsustab, milliseid andmeid ta digiidentiteedikukrule tuginevale isikule avaldab, ning digiidentiteedikukrule tuginev isik võib küsida üksnes oma registreeringus märgitud andmeid.

Digikukru kasutamine on vabatahtlik: määruse artikli 5a lõike 15 kohaselt ei tohi kukrut mittekasutavate isikute juurdepääsu avalikele ja erasektori teenustele ega tööturule mingil moel piirata ning juurdepääs peab jääma võimalikuks ka muude identimis- ja autentimisvahenditega. See maandab digilõhe riski: inimesed, kes nutitelefoniga ei kasuta või uut lahendust ei soovi, ei jää teenustest ilma. Rakendamisel tuleb siiski jälgida, et digikukru kasutamine ei muutuks praktikas kohustuslikuks alternatiivide puudumise tõttu. E-identimise vahendid ja nende kasutajaliidesed peavad ühtlasi vastama Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/882²⁴ ligipääsetavusnõuetele, mis toob kasu eakatele ja piiratud funktsionaalse võimekusega inimestele. Kasutaja privaatsust kaitseb ka see, et määrus keelab kasutajate jälgimise ja profiilianalüüsi eri teenuste vahel ning kukru kasutamise kohta tohib koguda üksnes teenuse osutamiseks vajalikke andmeid (artikli 5a lõiked 14 ja 16).²⁵

Positiivne sotsiaalne mõju avaldub ka alaealiste kaitsele: kuigi eIDAS 2 määrus alaealisi eraldi ei reguleeri, on digikukkur kavandatud toimima muu hulgas vanuse kontrollimise vahendina (nt digiteenuste määruse kohaste vanusepiirangute täitmisel), võimaldades tõendada vanust ilma muid isikuandmeid avaldamata; see eeldab kukru kättesaadavust ka alaealistele.²⁶ Negatiivse mõju riskina tuleb arvestada uute võimalike pettuseskeemide (nt õngitsus- ja QR-koodiründed) levikuga digikukru kasutuselevõtu algusfaasis. Seda riski aitavad maandada määruse ja rakendusaktide turvanõuded, kukru sertifitseerimine ning kasutajate teavitamise tegevused.²⁷

Mõju olulisus: mõju ulatus on keskmine (teenuste kasutamise viis muutub, kuid sihtrühma käitumisega ei kaasne kohanemiskulusi, sest kasutamine on vabatahtlik ja senised vahendid säilivad), avaldumise sagedus on suur (e-identimine on igapäevatoiming), sihtrühm on suur (potentsiaalselt kogu elanikkond) ning ebasoovitavate mõjude risk on väike kuni keskmine (pettuseriskid, digilõhe). Kuna vähemalt üks kriteerium on hinnatud suureks, on sotsiaalne mõju **oluline**. Demograafiline mõju puudub: eelnõu ei mõjuta rahvastiku koosseisu ega -protsesse.

6.2. Mõju riigi julgeolekule ja välissuhetele

²⁴ Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta direktiiv (EL) 2019/882 toodete ja teenuste ligipääsetavusnõuete kohta (ELT L 151, 07.06.2019, lk 70).

²⁵ Cybernetica AS. Digikukru II etapi analüüs (Digiidentiteedikukru ökosüsteem). Versioon 1.1, 02.07.2025. Tellija: Riigi Infosüsteemi Amet. Lisa 9 (Digikukrute monitoorimise aspektid). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuu.pdf>

²⁶ Vt viide 23, lisa 8 (Nõuded alaealistele kukruteenuse pakkumiseks). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuu.pdf>

²⁷ Vt viide 17, ptk 7 (QR-kood ründesaidi ründekaitse). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuu.pdf>

Digiidentiteedi taristu on Eesti e-riigi toimimise kriitiline osa, mistõttu mõjutab eelnõu kaudselt riigi sisejulgeolekut ja küberturvalisust. eIDAS 2 määrus nõuab digikukru pakkumist kõrge usaldusväärsuse tasemega e-identimise süsteemi alusel, lõimitud turvet ning kukru sertifitseerimist artikli 5c kohaselt; digikukru rakendustarkvara komponentide lähtekood on üldjuhul avatud (artikli 5a lõiked 3, 11 ja 12). Need nõuded tõstavad e-identimise ökosüsteemi turvalisuse taset tervikuna. Eelnõus valitud suund, mille kohaselt sisaldab Euroopa digiidentiteedikukkur isikut tuvastavate andmete seas ka Eesti isikukoodi, muudab kukru isikutuvastuse poolest samaväärseks Eesti seniste riiklike elektroonsete identimisvahenditega. Tänu sellele on Eesti inimestel võimalus kasutada kahte eri riiklikku elektroonset identimisvahendit ning kahe riikliku alternatiivi olemasolu annab võimaluse tagada teenuste toimivus ka ühe süsteemi tõrke korral, mis suurendab e-riigi kerksust. Samal ajal suureneb ründepind: digikukkur koondab isiku tuvastusandmed ja elektroonilised tõendid mobiilseadmesse, mistõttu on kukru ja selle tugisüsteemide turvaintsidentidel potentsiaalselt lai mõju. Identiteedivarguse riski maandamiseks tuleb muu hulgas tagada, et inimest teavitatakse alati, kui tema nimele on digikukkur väljastatud – see kaitseb ka neid, kes ise kukrut ei kasuta.²⁸ Kvalifitseeritud e-allkirja usaldusväärsuse seisukohalt on oluline, et allkirja kaugloomise korral oleks tagatud allkirjastaja ainukontroll, selgesõnaline tahteavaldus iga allkirjastamistoimingu suhtes ning võimalus allkirjastatavaid dokumente enne ja pärast allkirjastamist loodud tulemit kontrollida, vastasel juhul on allkirja õiguslik kehtivus ohus.²⁹ Määruse artikkel 5e näeb turvarikkumise korral ette digikukru kättesaadavuse peatamise ja kasutajate teavitamise kohustuse.

Välissuhete vaates tugevdab üleliiduline koostalitlusvõime Eesti positsiooni Euroopa Liidu digitaalsel siseturul: Eesti elanikud saavad kasutada digikukrut teiste liikmesriikide teenustes ja vastupidi. Kohustuste tähtaegne täitmine on ühtlasi oluline rikkumismenetluse riski vältimiseks – kui Eesti ei tee digikukrut tähtjaks kättesaadavaks või ei kehtesta nõutavaid rakendusmeetmeid, võib Euroopa Komisjon algatada Eesti suhtes rikkumismenetluse. Mõju olulisus: ulatus keskmine, sagedus väike, sihtrühm väike, ebasoovitavate mõjude risk keskmine. Mõju ei ületa olulisuse künnist, kuid küberturvalisuse riske tuleb rakendamisel järjepidevalt juhtida.

6.3. Mõju majandusele

Ettevõtjatele avaldub mõju kolmes rollis. **Esiteks peavad erasektoris digikukrule tuginevad isikud, kellelt õigusakti või lepingu alusel nõutakse veebis kasutaja tugevat autentimist** (muu hulgas pangad, sideettevõtjad, tervishoiu- ja transpordisektori teenuseosutajad), hiljemalt 2027. aasta lõpust kasutaja vabatahtliku taotluse korral aktsepteerima digikukrut (artikli 5f lõige 2). See toob kaasa ühekordsed liidestamis- ja arenduskulud ning autentimisvoogude kohandamise kulud. Mikro- ja väikeettevõtjad on sellest kohustusest vabastatud, mis piirab halduskoormuse kasvu väiksemate ettevõtjate jaoks. Väga suurte digiplatvormide aktsepteerimiskohustus tuleneb vahetult määruse artikli 5f lõikest 3 ega puuduta Eesti ettevõtjaid otseselt. Aktsepteerimiskohustus hõlmab kõiki eIDAS 2 määruse kohaselt pakutavaid digikukruid, mistõttu peavad Eesti teenusepakkujad olema valmis aktsepteerima ka teiste liikmesriikide kukruid. Peame arvestama, et osa liikmesriike võib oma digikukrud kasutusele võtta juba 2026. aasta lõpuks.³⁰

²⁸ Cybernetica AS. Digikukru I etapi analüüs. Versioon 1.0.1, 21.12.2023. Tellija: Riigi Infosüsteemi Amet. <https://www.ria.ee/sites/default/files/documents/2024-01/Digikukru-I-etapi-analuus.pdf>

²⁹ Vt viide 17, ptk 5 (Massallkirjastamise piirangud ja tingimused). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuus.pdf>

³⁰ Vt viide 16. <https://www.ria.ee/riigi-infosusteeim/elektroonilise-identiteedi-teenused/digikukkur-eudi-wallet>

Kohustuste rakendamisel tuleb arvestada ka ajaga, mis kulub riigil vajalike tehniliste ja organisatsiooniliste eelduste loomiseks. Ettevõtjatele peab pärast seda jääma mõistlik aeg lahenduste arendamiseks, testimiseks ja kasutuselevõtuks ning ettevõtjate valmisoleku hindamisel tuleb seda samuti arvesse võtta. Samas kehtib kohustus aktsepteerida teiste liikmesriikide kukruid sõltumata Eesti digikukru valmimise ajast. Seda selgitust täiendati kooskõlastusringil Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu ettepaneku alusel. Kooskõlastusringil palus Kliimaministeerium hinnata eelnõu mõju ühisveevärgi ja -kanalisatsiooni teenuse osutajatele, kes kasutavad klientidele suunatud iseteeninduskeskkondi. Digikukru aktsepteerimise kohustus tuleneb vahetult määruse artikli 5f lõikest 2 ja laieneb erasektoris üksnes neile teenuseosutajatele, kellelt liidu või liikmesriigi õigusakti või lepingu alusel nõutakse veebis kasutaja tugevat autentimist. Ühisveevärgi ja -kanalisatsiooni teenuse osutajatele ei tulene õigusaktist kohustust kasutada iseteeninduskeskkonnas kasutaja tugevat autentimist, mistõttu eelnõul puudub otsene mõju vee-ettevõtjatele ja veeteenuse osutamisele. Kui vee-ettevõtja on kasutaja tugeva autentimise iseteeninduskeskkonnas ette näinud lepingu alusel, võib aktsepteerimiskohustus teda puudutada samadel alustel kui teisi erasektori teenuseosutajaid. Kohustus ei puuduta mikro- ja väikeettevõtjaid.

Teiseks peavad kõik digikukrule tugineda soovivad ettevõtjad end registreerima digiidentiteedikukrule tuginevate isikute riiklikus registris (määruse artikkel 5b, komisjoni rakendusmäärus (EL) 2025/848³¹). Registreerimisprotsess peab olema kulutõhus ja riski suhtes proportsionaalne: rakendusmäärus nõuab veebipõhist ja võimaluse korral automaatset registreerimist ning taotluste menetlemist põhjendamatu viivitusega, samuti on registreerimisel esitatavate andmete maht piiratud (asukohaliikmesriik, nimi ja registrikood, kontaktandmed, kukru kavandatud kasutus ja taotletavad andmed), mistõttu on ühe ettevõtja halduskoormus registreerimisel väike. Ettevõtja ettevalmistavad tegevused hõlmavad kohustuse hindamist, protsesside analüüsi, registreerimist, pääsuserifikaatide taotlemist ja süsteemide integreerimist. Registri esmaversion koos juhenditega on kavandatud valmima 2026. aasta lõpus või 2027. aasta alguses ning registreerimine algab pärast selle valmimist.³² Eelnõuga ei kehtestata digiidentiteedikukrule tuginevate isikute registreerimise ega pääsuserifikaatide väljastamise eest riigilõivu: riigilõiv nähakse riigilõivuseaduse §-s 116² ette üksnes Euroopa digiidentiteedikukru pakkuja loa taotluse läbivaatamise eest. See hoiab ettevõtjate turule sisenemise barjääri madalal ja toetab Eesti konkurentsipositsiooni teiste liikmesriikide suhtes. Registreerimise võimaliku tasustamise mõju turule sisenemisele on käsitletud ka Eesti analüüsides³³ ning digikukru kasutuse majandusmudeli selgitamise vajadus tõstatati juba 2021. aasta kaasamisel.³⁴

Kolmandaks mõjutab eelnõu usaldusteenuse osutajaid. Eelnõuga täpsustatakse ja ajakohastatakse loamenetlust ning riigipõhiseid nõudeid usaldusteenuse osutaja jaoks ja kirjeldatakse vastavat menetlust ja nõudeid ka Euroopa digiidentiteedikukru pakkuja jaoks. Selgelt sõnastatud nõuded aitavad teenuseosutajatel loamenetlust läbida ning loovad õigusselgust nõuetele vastavuse suhtes; see mõju puudutab väikest ringi ettevõtjaid, kuid nende jaoks on mõju suur. eIDAS 2 määrus loob uued usaldusteenuse liigid, muu hulgas atribuutide elektroonilise tõendamise (elektroonilised tõendid) ja e-allkirja kaugloomise vahendite haldamise, mis avavad Eesti usaldusteenuse osutajatele uued turuvõimalused kogu Euroopa

³¹ Vt viide 6. http://data.europa.eu/eli/reg_impl/2025/848/oj

³² Vt viide 16. <https://www.ria.ee/riigi-infosusteeim/elektroonilise-identiteedi-teenused/digikukkur-eudi-wallet>

³³ Vt viide 17, ptk 9 (RP-dega seotud õiguslik ja menetluslik raamistik). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuus.pdf>

³⁴ Vt viide 29. http://data.europa.eu/eli/reg_impl/2025/848/oj

Liidus.³⁵ Elektrooniliste tõendite potentsiaalseid kasutusjuhte on Eestis analüüsitud juba alates 2022. aastast – näiteks töötajakaardi, kalastuslubade, perekaardi ja mobiilse juhiloa digiteerimine –, mis võimaldaks asendada paberil ja plastkaartidel põhinevad tõendid masinloetavate elektrooniliste tõenditega ning vähendada nii ettevõtjate kui ka riigi asjaajamiskulusid.³⁶ Samal ajal karmistuvad vastavusnõuded: kvalifitseeritud usaldusteenuse osutajaid auditeeritakse vähemalt iga 24 kuu järel (artikli 20 lõige 1) ning liikmesriigid peavad tagama, et määruse rikkumise eest saab usaldusteenuse osutajale määrata haldustrahvi, mille maksimummäär on vähemalt 5 000 000 eurot või juriidilise isiku puhul 1% üleilmsest aastasest kogukäibest, olenevalt sellest, kumb on suurem (artikkel 16). Eelnõu kohaselt e-identimise ja e-tehingute usaldusteenuste seaduses kehtestatavad karistusnormid (eelnõu § 1 punktid 41 ja 43) ning karistusseadustiku § 350 täiendamine (eelnõu § 3) suurendavad seega usaldusteenuse osutajate vastutusriski, kuid ühtlustavad selle teiste liikmesriikidega.

Euroopa Liidu tasandi mõjuhindang toob esile, et ühtse digiidentiteedi lahenduse kasutuselevõtt vähendab oluliselt ettevõtjate kliendituvastuse kulusid ja identiteedipettustest tulenevaid kahjusid: komisjoni hinnangul on tegevuskulude sääst olenevalt kasutuselevõtu ulatusest finantsteenuste sektoris liidus tervikuna 0,68–1,36 miljardit eurot aastas (kliendi tuvastamise ja hoolsusmeetmete kulud) ja tervishoiusektoris 1,26–2,51 miljardit eurot aastas ning identiteedipettuste kahjud vähenevad finantsteenuste sektoris 0,85–1,4 miljardi euro võrra aastas.³⁷ Komisjon rõhutab ühtlasi, et sertifitseeritud ja kogu liidus toimiv autentimislahendus vähendab iga üksikteingu kulu, võimaldab viia tundlikumaid tehinguid täielikult digitaalseks ning pakub ettevõtjatele neutraalse avaliku sektori autentimislahenduse alternatiivina eraõiguslikele lahendustele, mis võivad kasutada kasutajaandmeid profileerimiseks.³⁸ Need on liidu koondhinnangud; Eesti-spetsiifiline kvantitatiivne hinnang koostatakse eelnõu menetluse käigus (vt punkt 6.6).

Eesti kaalutusotsustest mõjutab ettevõtjaid ka kvalifitseeritud usaldusteenuse osutaja vastutuskindlustuse aastase koondsumma suurendamine ühelt miljonilt kahe miljoni euroni: see suurendab mõõdukalt kindlustusmakset, kuid tagab kannatanutele tegeliku kahju hüvitamise võimaluse ja vastab summa kehtestamisest möödunud aja jooksul muutunud hinnatasemele; iga üksiku kindlustusjuhtumi kohta nõutav kate ei muutu. Avatud lähtekoodi nõudest erandi tegemise võimalus (eelnõu § 1 punkt 13) annab riigile paindlikkuse juhaks, kui digikukru üksikute komponentide lähtekoodi avalikustamine ohustaks turvalisust; erandi kasutamata jätmise korral kehtib määruse üldreegel, mistõttu on selle otsuse vahetu mõju ettevõtjatele ja kasutajatele väike ning avaldub eelkõige riigi enda arendus- ja hankevalikutes.

Tarbijate jaoks väheneb asjaajamiskoormus: digikukkur võimaldab tõendada isikut ja atribuute (nt vanust, kvalifikatsiooni, lube) ühe vahendiga nii Eestis kui ka üleliiduliselt, vähendades paberdokumentide ja korduva andmete esitamise vajadust. Komisjoni mõjuhindangu kohaselt väheneks kodanike halduskoormus isikuandmete üleliidulise kasutamise korral liidus tervikuna

³⁵ Vt viide 23, ptk 2 (Digiidentiteedikukru ökosüsteem). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuus.pdf>

³⁶ A. Pankova, P. Laud, A. Kalu, R. Lillemets, M. Toomsalu, M. J. Liba, A. Kamenik. Tõend kui platvorm. Riigi Infosüsteemi Amet: 2022. <https://www.ria.ee/sites/default/files/documents/2022-11/Toend-kui-platvorm-12.05.2022.pdf>

³⁷ Vt viide 14, 3. lisa (joonis 18) ja 5. lisa (joonised 34 ja 35). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0124>

³⁸ Vt viide 21. <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487811/Benefits>

hinnanguliselt 350–400 miljoni euro võrra aastas.³⁹ Mõju olulisus: ulatus keskmine (kohustatud ettevõtjad peavad autentimislahendusi kohandama, kuid tegemist on ühekordse kohanemisega), sagedus keskmine, sihtrühm keskmine (aktsepteerimiskohustus puudutab piiratud, kuid majanduslikult olulisi sektoreid; mikro- ja väikeettevõtjad on vabastatud), ebasoovitavate mõjude risk väike. Kuna kaks kriteeriumi on hinnatud keskmiseks, on mõju majandusele **oluline**.

6.4. Mõju elu- ja looduskeskkonnale

Puudub. Eelnõu reguleerib digitaalset identiteeditaristut ega mõjuta keskkonnakvaliteeti, loodusvarasid ega ehitatud keskkonda. Kaudse vähese positiivse mõjuna võib digikukru ja elektrooniliste tõendite kasutuselevõtt vähendada paber- ja plastdokumentide kasutust, kuid see mõju ei ole mõõdetav ega siinses kontekstis oluline.

6.5. Mõju regionaalarengule

Otsene mõju puudub, sest eelnõu kohaldub kogu riigis ühetaoliselt. Kaudne vähene positiivne mõju avaldub selles, et digikukkur parandab avalike ja erasektori e-teenuste kättesaadavust olenemata asukohast, mis toetab teenuste tarbimist ka piirkondades, kus füüsiline teenusvõrk on hõredam. Mõju ei ületa olulisuse künnist.

6.6. Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele

Eelnõuga ei jagata ümber kohustusi keskvalitsuse struktuuris ega looda uusi struktuuriüksusi; lisanduvad ülesanded on jagatud asutuste vahel, kelle põhiülesanded juba hõlmavad sarnaseid funktsioone. Suurim koormus langeb RIA-le, kelle ülesanneteks on eelnõu kohaselt pädeva asutuse ülesanded, sealhulgas digikukru pakkumise korraldamine riigi nimel (sh võimalus pakkumine ja selleks vajalikud tegevused allhankida), digiidentiteedikukrule tuginevate isikute riikliku registri asutamine ja pidamine koos pääsuseritifikaatide väljastamise korraldamisega, Euroopa digiidentiteedikukru pakkuja loamenetlus, e-identimise süsteemide usaldusväärsuse taseme samaväärsuse hindamine e-identimise ja e-tehingute usaldusteenuste seaduse⁴⁰ § 21¹ kohases menetluses ning riiklik ja haldusjärelevalve koos väärtegade kohtuvälise menetleja rolliga. Kuna eIDAS 2 määrus loob uued usaldusteenuse liigid, laieneb ka usaldusteenuste järelevalve ulatus ning lisandub Euroopa digiidentiteedikukru raamistiku järelevalveasutuse roll (määruse artikkel 46a).⁴¹ Need ülesanded eeldavad püsivat lisaressurssi nii infosüsteemide arenduseks ja halduseks kui ka menetluste läbiviimiseks; kulud ja rahastamisallikad on esitatud seletuskirja 7. peatükis. Euroopa Liidu tasandil hinnati komisjoni mõjuhinnangus, et digikukru ühe lahenduse arendus- ja halduskulud on esimese kolme aasta jooksul kokku ligikaudu 10,5 miljonit eurot ja käitamine eeldab 25–30 töötajaga püsimeeskonda, ning e-identimise süsteemi teavitamisega seotud vastavushindamisaruande kulu on suurusjärgus 80 000 – 100 000 eurot. Kuna Eesti kasutab eID-vahendite turvasertifitseerimist juba praegu, ei tohiks sertifitseerimisnõuetest endist tuleneda märkimisväärsed lisakulusid.⁴² Andmekaitse Inspektsiooni töökoormus suureneb digikukru ja sellega seotud töötlemistoimingute andmekaitsealase järelevalve võrra, sealhulgas kasutajate teadete menetlemisega, mida saab esitada otse kukru ühise töölaua kaudu (artikli 5a lõike 4 punkt d).

³⁹ Vt viide 14, 3. lisa (joonis 18). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0124>

⁴⁰ Vt viide 3. <https://www.riigiteataja.ee/akt/130122025016>

⁴¹ Vt viide 23, ptk 2. <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuus.pdf>

⁴² Vt viide 14, 5. lisa. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0124>

Digikukru ökosüsteemi käivitamine eeldab lisaks mitme muu asutuse panust. Riiklik sertifitseerimiskava tuleb igal liikmesriigil kehtestada oma digikukrulahenduse ja selle aluseks oleva e-identimise süsteemi arhitektuuri kohta ning määrata kava omanik. Eelnõu kohaselt on kavade koostamine, ajakohasena hoidmine ja avaldamine valdkonna eest vastutava ministeeriumi ülesanne (eelnõu § 1 punkt 32). Digikukru vastavushindamisasutuse akrediteerimine on riikliku akrediteerimisasutuse (Eesti Standardimis- ja Akrediteerimiskeskus) uus akrediteerimisteenus, millest tuleb teavitada Euroopa Komisjoni.⁴³ Digikukkur kavandatakse eraldiseisva mobiilirakendusena. Kui digikukkur kavandatakse kombineerituna mõne muu mobiilirakendusega (nt riigiäpiga), muutub kukru sertifitseerimine keerukamaks ja EUDI-nõuded võivad laieneda rakenduse muudele funktsioonidele; seetõttu tuleb arhitektuurivalikul eraldi hinnata turvaperimeetrit, sertifitseerimise ulatust ja lisamoodulite mõju hindamisobjektile.⁴⁴ Digikukru kui kõrge usaldusväärsuse tasemega e-identimise vahendi väljaandmine eeldab isikutuvastusandmete väljastamisel koostööd rahvastikuregistri ja isikut tõendavate dokumentide andmekogu pidajaga.⁴⁵ Riiklike andmekogude pidajatele, kelle andmekogu kvalifitseerub autentseks allikaks, tekib kohustus võimaldada elektrooniliste tõendite kvalifitseeritud usaldusteenuse osutajatel kasutaja taotlusel kontrollida vähemalt määruse VI lisas loetletud atribuute (nt aadress, vanus, kvalifikatsioonid, esindusõigused) elektrooniliselt hiljemalt 24 kuu möödumisel rakendusaktide jõustumisest (artikkel 45e). See eeldab andmekogude liideste ja andmekvaliteedi ettevalmistamist ning kohustus on suunatud ka üleliidulisele kasutusele.⁴⁶

Kõik avaliku sektori asutused, sealhulgas kohaliku omavalitsuse üksused, peavad artikli 5f lõike 1 kohaselt aktsepteerima digikukrut nendes internetipõhistes teenustes, mille kasutamiseks nõutakse e-identimist ja e-autentimist. Asutuste individuaalset kohandamiskoormust vähendab oluliselt see, et valdavas osas avaliku sektori teenustes kasutatakse autentimiseks riigi kesket autentimisteenust (TARA): digikukru tugi lisatakse kesksesse teenusesse, misjärel jõuab see asutusteni ilma iga asutuse eraldi arendusteta. Samas tuleb keskse autentimisteenuse vahendajarolli kujundamisel arvestada määruse piiranguga, mille kohaselt digiidentiteedikukrule tuginevate isikute nimel tegutsevad vahendajad ei tohi salvestada andmeid tehingu sisu kohta (artikli 5b lõige 10).⁴⁷ Rakendamisel tuleb ühtlasi tagada, et digikukru andmevahetusloogika sobituks Eesti X-tee, ühendatud andmekogude ja ühekordse küsimise (once-only) põhimõttega ega tekitaks paralleelset, kasutaja käsitsi hallatavat tõendite vahendamise kanalit seal, kus automatiseeritud andmevahetus on otstarbekam; sellele riskile juhiti tähelepanu juba 2021. aasta kaasamisel.⁴⁸ Asutused, kes kesket autentimisteenust ei kasuta, peavad oma autentimislahendused ise kohandama. Kohaliku omavalitsuse üksustele ei panda eelnõuga uusi iseseisvaid ülesandeid, kuid Euroopa digiidentiteedikukruga liidestuvad ka kohaliku omavalitsuse üksuste e-teenused, mistõttu võivad neile kaasneda kohanemiskulud (vt seletuskirja punkt 7.5). Planeeritud on TARA teenuse laiendamine, et olemasolevate TARA

⁴³ Vt viide 23, lisa 1 (Liikmesriigi riiklik sertifitseerimiskava) ja lisa 3 (Euroopa Komisjonile tehtavad teavitused). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuus.pdf>

⁴⁴ Vt viide 17, ptk 2 (Superäpp). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuus.pdf>

⁴⁵ Vt viited 23 ja 26. <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuus.pdf> ja <https://www.ria.ee/sites/default/files/documents/2024-01/Digikukru-I-etapi-analuus.pdf>

⁴⁶ Vt viide 23, ptk 2 ja lisa 2 (Autentne allikas). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuus.pdf>

⁴⁷ Vt viide 17, ptk 11 (TARA kui digikukru liides). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuus.pdf>

⁴⁸ Vt viide 29. http://data.europa.eu/eli/reg_impl/2025/848/oj

klientide digikukru kasutuselevõttu lihtsustada. Esmalt laiendatakse autentimisvahendite hulka (lisatakse digikukkur). Digikukru lõplik tehniline lahendus sõltub hanke dialoogidest ja pakkujatest. Täpsem info edastatakse töö käigus mõjutatud osapooltele esimesel võimalusel.

Digiidentiteedikukrule tuginevate isikute registris peavad end registreerima kõik, kes peavad digikukrut oma e-identimist nõudvates e-teenustes aktsepteerima; see hõlmab ka avaliku sektori asutusi, sealhulgas kohaliku omavalitsuse üksusi ja riigiasutusi. Kavatsus on riigi keskse autentimisteenuse (TARA) praegused kliendid registreerida digiidentiteedikukrule tuginevate isikute registrisse ühekordselt ja võimalikult lihtsalt, et avaliku sektori asutuste halduskoormus oleks sellega seoses võimalikult väike.

Eelnõuga ei panda andmekogude pidajatele kohustust liidestada andmekogu digikukruga: autentse allika kohustus võimaldada elektrooniliste tõendite kvalifitseeritud usaldusteenuse osutajal kasutaja taotlusel määruse VI lisas loetletud atribuute (sealhulgas kvalifikatsioone) kontrollida tuleneb vahetult määruse artikli 45e lõikest 2 ning selle täitmise tehnilised nõuded ja liidesed kehtestatakse Euroopa Komisjoni rakendusaktidega. Avaliku sektori registritele suunatud rakendamise ajakava, liidestamise järjekorra ja tehniliste nõuete avaldamise põhimõtted kavandab RIA digikukru projekti raames koostöös asjaomaste haldusaladega ning avaldab need oma veebilehel koos digiidentiteedikukrule tuginevate isikute registreerimise juhenditega.

Mõju olulisus: ulatus on RIA jaoks suur (lisanduvad uued püsiülesanded ja infosüsteemid), teiste asutuste jaoks väike kuni keskmine; sagedus keskmine; sihtrühm keskmine; ebasoovitavate mõjude risk suur (tähtajaks valmimata jäämise risk). Mõju on **oluline**.

Järelhindamine

Järelhindamine on ette nähtud eIDAS 2 määruse artiklis 49 ja toimub Euroopa Liidu üleselt Euroopa Komisjoni algatusel. eIDAS 2 määruse artikli 48a kohaselt kogub liikmesriik statistikat digikukru ja kvalifitseeritud usaldusteenuste toimimise kohta – sealhulgas kehtiva kukru kasutajate arv, kukrut aktsepteerivate teenuste liik ja arv, kasutajate kaebused ning turvaintsidendid ja nende mõju – ning esitab statistilise aruande Euroopa Komisjonile igal aastal 31. märtsiks avatud ja masinloetavas vormingus.⁴⁹ Euroopa Komisjon hindab omakorda määruse artikli 5f lõike 5 kohaselt 24 kuu jooksul digikukrute kasutuselevõttust nende nõudlust, kättesaadavust ja kasutatavust. Riigisiselt seiravad Justiits- ja Digiministeerium ja RIA digikukru kasutuselevõttu jooksvalt vähemalt eelnimetatud artikli 48a näitajate alusel, millele lisanduvad digiidentiteedikukrule tuginevate registreeritud isikute arv ning digikukruga tehtud autentimiste ja allkirjastamiste maht. Et võimaldada nende ülesannete täitmist, lisatakse eelnõuga peatükk 3¹ „Teabevahetus“ ning § 23² „Teabevahetus teenuse osutajatega“, mis võimaldab valdkonna eest vastutaval ministeeriumil ja pädeval asutusel 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.

Halduskoormuse koondhinnang

– Ettevõtete halduskoormus ajutiselt mõõdukalt suureneb, pikemas vaates võimaldab ühtne üleliiduline identimisvahend ja tõendite digiteerimine kliendituvastuse ja asjaajamise kulusid vähendada. Halduskoormuse ajutine suurenemine tuleneb asjaolust, et

⁴⁹ Vt viide 23, lisa 9. <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuus.pdf>

aktsepteerimiskohustusega digiidentiteedikukrule tuginevad isikud peavad end registreerima ja autentimislahendused kohandama (ühekordne kulu, olemasolevad riigi keskse autentimisteenuse (TARA) kliendid võivad saada registreerimiseks lihtsustatud võimaluse). Mikro- ja väikeettevõtjad on kohustusest vabastatud.

– Kodanike halduskoormus väheneb – isiku ja atribuutide tõendamine muutub lihtsamaks nii Eestis kui ka üleliiduliselt. Näiteks hakkavad isikud juhiluba saada tulevikus digitaalsena digikukrusse ega pea enam füüsilise kaardina seda kaasas kandma. Digikukkur on füüsilistele isikutele tasuta ja selle kasutamine vabatahtlik. Muudatus võimaldab inimestel tõendada oma isikut ning erinevaid andmeid, näiteks vanust, õigusi ja lubasid, ühe turvalise digiidentiteedilahenduse abil nii Eestis kui ka teistes Euroopa Liidu liikmesriikides. Samuti võimaldab digikukkur jagada teenuse kasutamiseks vajalikke andmeid digitaalselt, mis võib vähendada vajadust hankida ja esitada tõendeid eraldi ning esitada samu andmeid korduvalt eri teenuseosutajatele. Kasutaja saab ise valida, milliseid andmeid ta teenuseosutajaga jagab. Digiidentiteedikukru kasutamine on füüsilistele isikutele vabatahtlik ja tasuta ning see täiendab seniseid isikutuvastusvahendeid.

– Avaliku sektori töökoormus suureneb – Riigi Infosüsteemi Ametile (RIA) lisanduvad püsivad arendus-, haldus-, registri- ja järelevalveülesanded, Andmekaitse Inspektsioonile järelevalve tegemise ja kaebuste menetlemise koormus, Justiits- ja Digiministeeriumile lisakohustused seoses sertifitseerimisskeemi loomise ning ajakohasena hoidmisega ning autentseid allikaid pidavatele asutustele atribuutide kontrolli võimaldamise kohustus. Teiste asutuste koormuse kasvu leevendab keskse autentimisteenuse kasutamine.

7. Seaduse rakendamisega seotud riigi ja kohaliku omavalitsuse tegevused, eeldatavad kulud ja tulud

Eelnõu rakendamine eeldab Andmekaitse Inspektsioonilt, Justiits- ja Digiministeeriumilt ning Riigi Infosüsteemi Ametilt lisategevusi, millega kaasnevad riigieelarvelised lisakulud. Kulud jagunevad rakendamiskuludeks (sealhulgas digikukru väljaarendamine) ja järelevalvekuludeks. Lisaks kaasnevad ministeeriumide haldusaladele kulud oma e-teenuste digikukruga liidestamisest. Käesolevas peatükis esitatud kulud tuginevad asutuste tegevuspõhistele eelarvestustele perioodiks 2027–2030. Samas tuleb arvestada, et projekt jätkub ja sellega kaasnevad kulud ka pärast 2030. aastat.

Kulude kogumaht aastatel 2027–2030 on 20 445 588 eurot. Kulud jagunevad asutuste vahel järgmiselt (vt tabel 1).

Tabel 1. eIDAS2 rakendamise kulud asutuste ja aastate lõikes 2027–2030 (eurodes).
Allikas: AKI, JDM ja RIA eelarvestused.

Asutus	2027	2028	2029	2030	Kokku 2027–2030
AKI	75 522	75 522	75 522	75 522	302 088
JDM	385 000	685 000	470 000	370 000	1 910 000
Liidestuvad ministeeriumid	-	-	1 000 000	1 000 000	2 000 000
RIA – järelevalve	75 000	75 000	75 000	75 000	300 000

Asutus	2027	2028	2029	2030	Kokku 2027–2030
RIA – digikukru arendus	4 483 500	4 902 000	3 431 000	3 117 000	15 933 500
Kokku	5 019 022	5 737 522	5 051 522	4 637 522	20 445 588

AKI – Andmekaitse Inspeksioon; JDM – Justiits- ja Digiministeerium; RIA – Riigi Infosüsteemi Amet.

Ministeeriumide real kajastatakse ministeeriumide haldusalade e-teenuste digikukru liidestamise kulud (1 000 000 eurot 2029. aastal ja 1 000 000 eurot 2030. aastal, kokku 2 000 000 eurot); iga haldusala liidestab oma teenused digikukruga ise. Haldusalade kulu tekib eelkõige nende e-teenuste ja andmekogude kohandamisest, mis keskset autentimisteenust ei kasuta või mis hakkavad toimima autentse allikana. Liidestuvate ministeeriumide kulud sisalduvad käesolevas peatükis esitatud perioodi 2027–2030 riigieelarve lisavajaduses ja taotletakse keskselt Justiits- ja Digiministeeriumi kaudu riigieelarve koostamise käigus.

7.1. Andmekaitse Inspeksioon

AKI-le tekivad eIDAS2 määrusest tulenevate uute järelevalveülesannete täitmiseks alates 2027. aastast iga-aastased lisakulud kokku 75 522 eurot aastas, sealhulgas tööjõukulu 68 206 eurot ja sellega seotud majandamiskulu 7316 eurot (vt tabel 2). Kulu aluseks on üks lisanduv ametikoht (1 FTE) eIDAS2 määrusest tulenevate järelevalvekohustuste täitmiseks; brutopalk 3600 eurot kuus, millele lisandub 18 protsenti tugifunktsiooni katteks, ja korruptustegur 1,338 tööjõumaksude ja muude palgalisandite katteks ($3600 \times 12 \times 1,18 \times 1,338 = 68\,206$ eurot aastas).

Tabel 2. AKI lisakulud eIDAS2 rakendamiseks 2027–2030 (eurodes). Allikas: AKI eelarvestus.

Kulutüüp	2027. a summa	2028. a summa	2029. a summa	2030. a summa	Selgitus
Investeeringud	-	-	-	-	Investeeringuid ei kavandata.
Tööjõukulud	68 206	68 206	68 206	68 206	1 FTE eIDAS2 määrusest tulenevate uute järelevalvekohustuste täitmiseks. Brutopalk 3600 eurot kuus, millele lisandub 18 protsenti tugifunktsiooni katteks ja korruptustegur 1,338 tööjõumaksude ja muude palgalisandite katteks ($3600 \times 12 \times 1,18 \times 1,338 = 68\,206$ eurot aastas).
Majandamiskulud, mis on seotud tööjõukuludega	7 316	7 316	7 316	7 316	Uue ametikohaga seotud majandamiskulu (töökoha loomine ja ülalpidamine).

Kulutüüp	2027. a summa	2028. a summa	2029. a summa	2030. a summa	Selgitus
Muud majandamiskulud	-	-	-	-	Ei kavandata.

Kulud on seotud eelnõuga kehtestatavate uute järelevalveülesannetega, mis on kirjeldatud seletuskirja punktis 6.6. Ilma lisaressursita ei ole AKI-l võimalik eIDAS2 määrusest tulenevaid ülesandeid täita, mis toob kaasa Euroopa Liidu õigusest tulenevate kohustuste täitmata jätmise riski.

7.2. Justiits- ja Digiministeerium

JDM-ile tekib eIDAS2 määrusest tulenevate ülesannete täitmiseks lisavajadus tööjõukulu, investeeringukulu ja majandamiskulu näol kokku 1 910 000 eurot aastatel 2027–2030 (vt tabel 3). Kulud on seotud kahe uue ametikoha (projektijuht, sertifitseerimise ekspert) loomisega, riikliku sertifitseerimisskeemi väljatöötamise, kinnitamise ja haldamisega ning digikukruga seotud kommunikatsioonitegevustega. Tööjõukulude arvestuse aluseks on avaliku sektori palgastatistika.

Tabel 3. JDM-i lisakulud eIDAS2 rakendamiseks 2027–2030 (eurodes). Allikas: JDM-i eelarvestus.

Kulutüüp	2027. a summa	2028. a summa	2029. a summa	2030. a summa	Selgitus
Investeeringud	-	300 000	-	-	Investeeringukulu on kavandatud 2028. aastasse, kuna sertifitseerimisskeemi tehniline infrastruktuur ja seonduvad IT-lahendused hangitakse pärast skeemi sisulist kinnitamist 2027. aastal, vastavalt kavandatud hanke- ja arendusetapi ajakavale.
Tööjõukulud	135 000	135 000	135 000	135 000	2 FTE-d (projektijuht, sertifitseerimise ekspert).
Majandamiskulud, mis on seotud tööjõukuludega	15 000	15 000	15 000	15 000	Uute ametikohtadega seotud majandamiskulu.
Muud majandamiskulud	235 000	235 000	320 000	220 000	Riikliku sertifitseerimisskeemi väljatöötamine, kinnitamine ja haldamine ning EUDI kommunikatsioonitegevused.

JDM-i eelarvestuse aastasummad kulutüüpide kaupa (tabel 3) annavad 2027. aastal kokku 385 000 eurot, 2028. aastal 685 000 eurot, 2029. aastal 470 000 eurot ja 2030. aastal 370 000 eurot.

7.3. Riigi Infosüsteemi Amet – järelevalve

RIA-le tekib alates 2027. aastast digiidentiteedikukru raamistiku järelevalvega seotud iga-aastane lisavajadus 75 000 eurot, sealhulgas tööjõukulu 67 500 eurot ja sellega seotud töökohakulu 7500 eurot (vt tabel 4). Kulud on seotud järgmiste ülesannetega: 1) autentsete allikate järelevalve eIDAS2 nõuetele vastavuse üle, tegevuslubade väljastamine, teenuseosutajate üle arvestuse pidamine ning nende usaldusväärseks tunnistamine ja sellest Euroopa Liidule teavitamine; 2) digikukru pakkujate ja tuginevate isikute järelevalve, sealhulgas järelevalve sihipärase kasutamise üle; 3) järelevalvetegevustest regulaarne aruandmine Euroopa Komisjonile ja Euroopa Liidu Küberturvalisuse Ametile (ENISA) – aruandluse maht võrreldes senisega kasvab.

Tabel 4. RIA järelevalve lisakulud eIDAS2 rakendamiseks 2027–2030 (eurodes). Allikas: RIA eelarvestus.

Kulutüüp	2027. a summa	2028. a summa	2029. a summa	2030. a summa	Selgitus
Investeeringud	-	-	-	-	Investeeringuid ei kavandata.
Tööjõukulud	67 500	67 500	67 500	67 500	1 FTE digikukru raamistiku järelevalveks.
Majandamiskulud, mis on seotud tööjõukuludega	7 500	7 500	7 500	7 500	Uue ametikohaga seotud töökohakulu.
Muud majandamiskulud	-	-	-	-	Ei kavandata.

7.4. Riigi Infosüsteemi Amet – digikukru arendus

RIA eID-tiimile tekib alates 2027. aastast digikukru väljaarendamise ja haldamisega seotud lisavajadus kokku 15 933 500 eurot aastatel 2027–2030 (vt tabel 5). Kulud jagunevad kuue tegevussuuna vahel: 1) digikukru teenusepakkuja hankimine; 2) digiidentiteedikukrule tuginevate isikute registri loomine ja haldamine; 3) tõendite vahendamise lüüsi loomine ja haldamine; 4) olemasoleva eID baasteenuse TARA API muutmine digikukruga liidestamiseks; 5) olemasoleva eID baasteenuse DigiDoc muutmine digikukruga liidestamiseks; 6) olemasoleva eID baasteenuse SiGa (Signature Gateway) muutmine digikukruga liidestamiseks.

Tabel 5. RIA digikukru arenduse lisakulud eIDAS2 rakendamiseks 2027–2030 (eurodes). Allikas: RIA eID-tiimi eelarvestus.

Kulutüüp	2027. a summa	2028. a summa	2029. a summa	2030. a summa	Selgitus
Investeeringud	1 290 000	1 000 000	350 000	350 000	Digikukru teenusepakkuja hankimine (1 250 000 eurot kokku), digiidentiteedikukrule tuginevate isikute registri loomine (420 000 eurot),

Kulutüüp	2027. a summa	2028. a summa	2029. a summa	2030. a summa	Selgitus
					tõendite vahendamise lüüsi loomine (420 000 eurot) ning TARA API, DigiDoc ja SiGa muutmine (kokku 900 000 eurot).
Tööjõukulud	606 000	687 000	716 000	752 000	10 FTE-d (4 digikukru teenusepakkuja hankimise ja halduse, 3 tuginevate isikute registri ning 3 tõendite vahendamise lüüsi tegevussuunas).
Majandamiskulud, mis on seotud tööjõukuludega	-	-	-	-	Ei kavandata eraldi realt; sisaldub muudes majandamiskuludes.
Muud majandamiskulud	2 587 500	3 215 000	2 365 000	2 015 000	Digikukru valdkonna kommunikatsioonitegevused (1 550 000 eurot kokku), üldised analüüsid ja uuringud, sealhulgas piiriülese koostoimelisuse korralduse tagamiseks vajalikud kohtumised (892 500 eurot kokku), digikukru teenusepakkuja hankimise korraldamise ja lepingu kulud (6 750 000 eurot kokku) ning digiidentiteedikukrule tuginevate isikute registri ja tõendite vahendamise lüüsi majanduskulu (kokku 990 000 eurot).

Digikukru arenduse ja haldamisega tekivad RIA-le uued tehnilised ja korralduslikud ülesanded, mille täitmine nõuab nii uut töötajaskonda kui ka olemasolevate eID baasteenuste (TARA, DigiDoc, SiGa) kohandamist.

7.5. Mõju kohaliku omavalitsuse üksuste eelarvetele

Kohaliku omavalitsuse üksustel tekivad kulud ulatuses, kus nad ei kasuta keskset TARA teenust. Kohalike omavalitsuste infosüsteemidest, mida kasutatakse teenuste osutamiseks, ei ole osa praegu TARA-ga liidestatud (nt lemmikloomaregister, ELIIS, Stuudium, huviregistrid), ning sama teenusepakkuja lahendusel võib eri omavalitsustes olla erinev autentimine (nt ARNO puhul Pärnul TARA, Saue Pikseli pass). Kõigi nende infosüsteemide TARA-ga liidestamise kuluks on Eesti Linnade ja Valdade Liidu esialgsel hinnangul 100 000–200 000 eurot, kuid praegu ei ole selge, millises ulatuses kataksid selle arendajad ja millises ulatuses jääks see

kohalike omavalitsuste kanda. Kui kohalike omavalitsustele lisanduvate kulude katmise vajadus peaks tekkima, siis taotletakse need välisrahastusest. Viimastel aastatel on Eesti Linnade ja Valdade Liidule valdkondlike digipöörete vahenditest vahendeid eraldatud igal aastal.

7.6. Kulude kokkuvõte

Kokku on eIDAS2 määruse rakendamisega seotud riigieelarve lisavajadus aastatel 2027–2030 20 445 588 eurot, millest AKI-le langeb 302 088 eurot, JDM-ile 1 910 000 eurot, RIA-le kokku 16 233 500 eurot (sealhulgas järelevalve 300 000 eurot ja digikukru arendus 15 933 500 eurot) ning ministriumide haldusalade EUDI-liidestumisele 2 000 000 eurot.

Täiendavaid vajadusi eelnõu rakendamiseks menetletakse iga-aastases riigieelarve ja riigi eelarvestrateegia protsessis. Alates 2028. aastast otsitakse võimalusi katta vajadusi uue perioodi Euroopa Liidu toetustest. Digikukru kasutuselevõtu tähtajad tulenevad otse eIDAS2 määrusest ja on liikmesriigile siduvad, seetõttu kaasneb määruse rakendamata jätmisel Euroopa Liidu õiguse rikkumise menetluse ja rahaliste sanktsioonide risk.

7.7. Tulud ja rahastamise allikas

Eelnõuga muudetakse ka riigilõivuseadust. Laekuva riigilõivu maht sõltub taotluste arvust, mida ei ole avalike allikate põhjal võimalik usaldusväärselt prognoosida; muid tulusid eelnõu rakendamisega ei kaasne.

8. Rakendusaktid

Eelnõuga antakse üks uus volitusnorm: e-identimise ja e-tehingute usaldusteenuste seaduse § 3¹ lõike 7 alusel kehtestab valdkonna eest vastutav minister määrusega digiidentiteedikukrule tuginevate isikute registri põhimääruse, milles sätestatakse andmete täpne koosseis, sealhulgas isikustamata andmed, andmeandjad ning nende esitatavad andmed, registritoimingute ja registrisse kantud andmete säilitamise täpsemad tingimused, registri rahastamine ning registriga seotud muud korralduslikud nõuded. Volitusnorm on vajalik, sest komisjoni rakendusmäärus (EL) 2025/848 jätab registri pidamise tehnilise ja korraldusliku täpsustamise liikmesriigile; seaduse tasandil sätestatakse andmekogu asutamine, eesmärk, vastutav töötleja, andmete koosseisu põhialused, avalikkus ja säilitustähtaeg ning määruse tasandile jääb üksnes rakenduslik täpsustus. Rakendusakti kavand on esitatud seletuskirja lisas 1. Rakendusakt tuleb kehtestada hiljemalt 24. detsembriks 2026, sest sellest kuupäevast kohaldub komisjoni rakendusmäärus (EL) 2025/848 ja registreerimine peab olema võimalik.

Eelnõu § 1 punktiga 31 tunnistatakse kehtetuks e-identimise ja e-tehingute usaldusteenuste seaduse § 12 lõige 2, mille tagajärjel muutub kehtetuks selle alusel antud majandus- ja taristuministri 26. oktoobri 2016. a määrus nr 64 „Usaldusteenuse osutaja ja usaldusteenuse vastavushindamise kord“.⁵⁰

Euroopa digiidentiteedikukru sertifitseerimise kava, mille koostamise kohustus pannakse eelnõuga valdkonna eest vastutavale ministriumile (eelnõu § 1 punkt 32), ei ole õigustloov akt ega rakendusakt hea õigusloome ja normitehnika eeskirja tähenduses, vaid haldusesisene dokument, mis avaldatakse ministriumi veebilehel. Samuti ei eelda eelnõu muud

⁵⁰ Usaldusteenuse osutaja ja usaldusteenuse vastavushindamise kord (RT I, 28.10.2016, 17).

rakendusakti: registreerimistaotluste esitamise tehniline kord tehakse kättesaadavaks digiidentiteedikukrule tuginevate isikute registri kaudu põhimääruses sätestatud korras.

9. Seaduse jõustumine

Seadus jõustub üldises korras ehk põhiseaduse § 108 kohaselt kümnendal päeval pärast Riigi Teatajas avaldamist. Eraldi jõustumissätet eelnõu ei sisalda. Üldkorras jõustumine on põhjendatud, sest sihtrühmade sisulised kohustused tulenevad valdavalt vahetult eIDAS 2 määrusest ja selle rakendusmäärustest, mille kohaldamise tähtajad on sätestatud Euroopa Liidu õiguses, ning eelnõu riigisisese rakendusmeetmed (pädeva asutuse määramine, loamenetlus, register, karistusnormid) ei nõua sihtrühmadelt sellist kohanemisaega, mis eeldaks pikemat jõustumistähtaega. Vastupidi, riigisiseste rollide ja menetluste võimalikult varane jõustumine on vajalik, et digiidentiteedikukrule tuginevate isikute registreerimine oleks võimalik hiljemalt 24. detsembrist 2026, mil kohaldub komisjoni rakendusmäärus (EL) 2025/848.

10. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitati eelnõude infosüsteemi (EIS) kaudu kooskõlastamiseks [26-0864](#) ning arvamuse avaldamiseks Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule, Eesti Linnade ja Valdade Liidule ning Rahvusarhiivile.

EIS-i kaudu toimuv kooskõlastamine on ühtlasi avalik konsultatsioon, sest eelnõu materjalid on infosüsteemis avalikult kättesaadavad ja igaühel on võimalik esitada eelnõu kohta arvamus.

Huvirühmi on sisuliselt kaasatud juba enne eelnõu koostamist, ja seda kahel tasandil. **Euroopa Liidu tasandil** korraldas Euroopa Komisjon eIDAS-määruse läbivaatamiseks avaliku konsultatsiooni 24. juulist kuni 2. oktoobrini 2020, et koguda tagasisidet e-identimise ja usaldusteenuste arengu ning kasutuselevõtu takistuste kohta⁵¹; konsultatsioonile laekus 318 vastust ning selle tulemusi on kajastatud komisjoni mõjuhinnaugut toetavas uuringus.⁵² Lisaks avalikule konsultatsioonile sai komisjon kirjalikku tagasisidet esialgse mõjuhinnaugu kohta (23. juulist 3. septembrini 2020), korraldas sihitatud sidusrühmauuringu (106 vastust) ning küsitles liikmesriikide esindajaid eIDAS-i koostöövõrgustikus. Avaliku konsultatsiooni tulemuste kohaselt toetas 60% vastanutest ühtse ja üldtunnustatud Euroopa digiidentiteedi süsteemi loomist riiklike e-identimise vahendite kõrvale; peamiste eelistena nimetati universaalset aktsepteeritavust (47% vastanutest), kasutusmugavust (43%) ja riigi tagatud usaldusväarsust (37%), peamise väljakutsena aga ühtse süsteemi ülesehituse ja juhtimise keerukust (52%); 49% vastanutest pidas kehtiva raamistiku peamiseks parandusmeetmeks selle laiendamist erasektorile.⁵³ Eesti seisukohtade kujundamisse komisjoni ettepaneku COM(2021) 281 (final) kohta kaasati asjaomased ministriumid, asutused ja huvirühmad; seisukohad kiitis heaks Vabariigi Valitsus ja neid arutas Riigikogu Euroopa Liidu asjade komisjon.⁵⁴ 2021. aasta kaasamise tabelist nähtub muu hulgas, et Siseministerium toetas eelnõu eesmäärke, huvirühmad tõstatasid küsimusi digikukru seosest olemasoleva eID-ökosüsteemi ja X-tee andmevahetusloogikaga, riigisisestest kuludest, majandusmudelid, erasektori vastutusest ja rakendamise tähtajast ning Eesti tegi ettepaneku näha kukru kasutuselevõtuks ette 24 kuud

⁵¹ Digital identity and trust: Commission launches public consultation on the eIDAS Regulation. Euroopa Komisjoni veebileht, 24.07.2020. <https://digital-strategy.ec.europa.eu/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation>

⁵² Vt viide 15.

⁵³ Vt viide 14, 2. lisa.

⁵⁴ Vt viide 13.

tehniliste nõuete jõustumisest – tähtaeg, mis kajastub ka määruse lõplikus tekstis (artikli 5a lõige 1).⁵⁵ Kaalutlusruumi kasutamise analüüs tehti Eesti seisukohtade kujundamise käigus, mistõttu ei koostatud eelnõu kohta väljatöötamiskavatsust (hea õigusloome ja normitehnika eeskirja § 1 lõike 2 punkt 2; vt ka seletuskirja punkt 2). Lisaks osales Eesti Euroopa Komisjoni kaasrahastatud suuremahulises pilootprojektis POTENTIAL, milles 19 liikmesriiki ja Ukraina katsetasid aastatel 2023–2025 digikukru kuut kasutusjuhtu; Eesti panustas RIA eestvedamisel digitaalse juhiloa tehnilise kontseptsioonilahenduse väljatöötamisse ning projekti tulemused andsid sisendi Euroopa digiidentiteedikukru arhitektuuriraamistiku (ARF) väljatöötamisse.⁵⁶ Määruse rakendusaktide eelnõude kohta on huvirühmadel olnud võimalik esitada tagasisidet Euroopa Komisjoni tagasisidekorje kaudu.

Eestis on kaasamine ja ettevalmistus toimunud järjepidevalt alates 2022. aastast. RIA on tellinud sõltumatud analüüsid digikukru ja elektrooniliste tõendite ökosüsteemi kohta – „Tõend kui platvorm“ (2022), digikukru I etapi analüüs (2023), II etapi analüüs (2025) ja III etapi analüüs (2026) – ning avalikustanud need oma kodulehel, kus on avaldatud ka teave digikukru ökosüsteemi, ettevõtjate kohustuste, digiidentiteedikukrule tuginevate isikute registri ajakava ja korduma kippuvate küsimuste kohta.⁵⁷ 2025. aasta mais kutsus RIA turuosalisi avalikult varakult kaasa mõtlema Euroopa Liidu digikukru järgmiste sammude üle.⁵⁸ Digiidentiteedikukrule tuginevate isikute registreerimise juhendid avaldatakse pärast registri esmaversiooni valmimist samuti RIA kodulehel, mis tagab ettevõtjatele jooksva teabe kohustuste täitmiseks.⁵⁹

Pärast EIS-i kooskõlastusringi uut kaasamisringi ei kavandata. EIS-i kaudu toimuv kooskõlastusring täidab ühtlasi Justiits- ja Digiministeeriumi 2026. aasta kaasamisplaanis kavandatud avaliku konsultatsiooni eesmärgi.⁶⁰ See on põhjendatud, sest eIDAS 2 määrus on vahetult kohaldatav ja eelnõu riigisisene otsustusruum on piiratud rakendusmeetmetega, mille sisulised valikud on läbi arutatud Euroopa Liidu tasandi õigusloomes, pilootprojektides ja Eestis toimunud ettevalmistava kaasamise käigus; sihtrühmadel on võimalik esitada arvamusi kooskõlastusringi jooksul EIS-i kaudu ning eelnõu menetlemisel Riigikogus. Kaasamisel ja ettevalmistavates analüüsides esile kerkinud põhiküsimused – sobitumine X-tee ja ühekordse küsimise põhimõttega, digikukru kasutuse majandusmudel, erasektori vastutusraamistik, digiidentiteedikukrule tuginevate isikute register, järelevalve ja karistused, sertifitseerimise ulatus – on käsitletud seletuskirja 6. peatükis ja eelnõu sisu peatükis (seletuskirja 3. peatükk).

Kooskõlastusringil esitasid eelnõu kohta märkusi ja arvamusi Eesti Linnade ja Valdade Liit, Eesti Infotehnoloogia ning Telekommunikatsiooni Liit. Iga märkuse sisu, esitaja ning arvestamine või arvestamata jätmine koos põhjendusega on esitatud seletuskirja lisa oleva kooskõlastustabelina (hea õigusloome ja normitehnika eeskirja § 50 lõiked 2 ja 3). Kooskõlastusringi tulemusel muudeti muu hulgas eelnõu §-s 1 kavandatud paragrahvide 3¹, 4¹, 5, 7, 8, 10, 13, 19 ja 23² puhul, jäeti eelnõust välja § 22 muudatused ning vähendati sunniraha ülemmäära; vastavad selgitused leiab seletuskirja asjakohastest osadest.

⁵⁵ Vt viide 29.

⁵⁶ Pilootprojekt POTENTIAL (digitaalne juhiluba). Riigi Infosüsteemi Ameti koduleht, 19.05.2026. <https://www.ria.ee/riigi-infosusteeim/elektronilise-identiteedi-teenused/pilootprojekt-potential>

⁵⁷ Vt viited 35, 26, 23 ja 17. Analüüsid on avalikustatud Riigi Infosüsteemi Ameti kodulehel (vt viide 16).

⁵⁸ EL digikukru järgmised sammud: kutsume turuosalisi varakult kaasa mõtlema. Riigi Infosüsteemi Ameti blogi, 30.05.2025.

<https://www.ria.ee/blogi/el-digikukru-jargmised-sammud-kutsume-turuosalisi-varakult-kaasa-motlema>.

⁵⁹ Vt viide 16.

⁶⁰ Vt viide 12.

Seletuskirja lisad

Lisa 1. Rakendusakti kavand (digiidentiteedikukrule tuginevate isikute registri põhimäärus).

Lisa 2. Vastavustabel (eIDAS 2 määruse ja eelnõu sätete seosed).

Lisa 3. Kooskõlastustabel (märkustega arvestamise tabel).

Algatab Vabariigi Valitsus 12. oktoobril 2026. a

Vabariigi Valitsuse nimel

(allkirjastatud digitaalselt)

Heili Tõnisson

Valitsuse nõunik