

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 turvaline kasutuselevõtt Eestis ning sätestada selleks vajalikud riigisisised reeglid, rollid ja sanktsioonid.

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

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 euron;
- 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 trahvi- ja sunnirahamäärad (kuni 5 000 000 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 otsekohalduvate rakendusmäärustega;
- Euroopa digiidentiteedikukru rakendustarkvarale kehtestatakse avatud lähtekoodi nõue koos Eestile lubatud erandi võimalusega;
- järelevalves ja kaebuste lahendamisel saab olulise rolli ka Andmekaitse Inspeksioon.

Mõjud on lühidalt järgmised: kodanikud saavad võimaluse kasutada üleeuroopalist digiidentiteeti, mis isikukoodi abil sobitub Eesti e-teenustega; ettevõtjatele luuakse selgemad reeglid usaldusteenuste ja Euroopa digiidentiteedikukru pakkumiseks; kahe paralleelse riikliku e-identimise vahendi (ID-kaart ja teised senised vahendid ning Euroopa digiidentiteedikukkur) 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.

Halduskoormuse koondkokkuvõte

- Ettevõtete halduskoormus suureneb mõõdukalt ja ajutiselt – aktsepteerimiskohustusega tuginevad isikud peavad end registreerima ja autentimislahendused kohandama (ühekordne kulu, olemasolevad TARA kliendid võivad saada lihtsustatud võimaluse registreerimiseks); mikro- ja väikeettevõtjad on kohustusest vabastatud; pikemas vaates võimaldab ühtne üleliiduline identimisvahend ja tõendite digiteerimine kliendituvastuse ja asjaajamise kulusid vähendada.
- Kodanike halduskoormus väheneb – isiku ja atribuutide tõendamine muutub lihtsamaks nii Eestis kui ka üleliiduliselt; digikukkur on füüsilistele isikutele tasuta ja selle kasutamine vabatahtlik.
- Avaliku sektori töökoormus suureneb – RIA-le lisanduvad püsivad arendus-, haldus-, registri- ja järelevalveülesanded, Andmekaitse Inspeksioonile järelevalve- ja kaebuste menetlemise koormus, Justiits- ja Digiministeeriumile täiendavad kohustused seoses sertifitseerimisskeemi loomise ning ajakohasena hoidmisega ning autentseid allikaid pidavatele asutustele atribuutide kontrolli võimaldamise kohustus; teiste asutuste koormuse kasvu leevendab keskse autentimisteenuse kasutamine.

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 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 karistuste normid ning mitu sätet dubleerivad nõudeid, mis on nüüdseks kehtestatud Euroopa Liidu otsekohalduvate rakendusmäärustega. Praktikas on tõlgendamisküsimusi tekitanud ka sertifikaatide kehtetuks tunnistamise aluste senine sõnastus (vt seletuskirja § 1 punktide 36–38 selgitusi).

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

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>

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-määrusega võetakse kasutusele Euroopa digiidentiteedikukru kontseptsioon, millega seotud rollide ja vastutuse jaotus Eestis ning järelevalve korraldus tuleb reguleerida seadusega;
- uuendatud eIDAS-määrus ja selle rakendusaktid kirjeldavad varasemast detailsemalt mitmeid usaldusteenuse ja selle osutamise 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 digiidentiteedikukru 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 digiidentiteedikukru 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 kukrusse 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 muudatust, mis lisaks uuenenud eIDAS-määruse rakendamisest 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 usaldusväarsuse taseme hindamist, ka Euroopa digiidentiteedikukkur. Euroopa digiidentiteedikukkur saab olla ainult usaldusväarsuse 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; vastavalt ametkondadevahelise elektroonse identiteedi juhtrühma arvamusele nähakse pädeva asutusena ette Riigi Infosüsteemi Amet.

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 digiidentiteedikukku pakkumist ja selleks vajalikke tegevusi allhankida.

Lõige 3 määrab kindlaks osapoole, kellele peab saama teada anda Euroopa digiidentiteedikukrule tugineva isiku tehtavatest väidetavalt ebaseaduslikest või kahtlastest taotlustest andmete saamiseks. Selleks asutuseks nimetatakse Andmekaitse Inspektsioon.

Lõige 4 määrab valdkonna eest vastutava ministeeriumi korraldama Euroopa digiidentiteedikukku 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 digiidentiteedikukku 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.

§ 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 kukrule tuginevate isikute kohta. Paragrahviga nähakse ette vastava andmekogu loomine, sinna esitatavate andmete koosseis, andmete esitamise korra kehtestamine, andmete säilitamise tähtaeg ning registreeringu peatamine ja tühistamine.

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

Andmekogu asutamisel on järgitud avaliku teabe seaduse § 43⁵ nõudeid: paragrahvi lõikes 1 sätestatakse andmekogu pidamise eesmärk ja vastutav töötleja (Riigi Infosüsteemi Amet), lõikes 3 registrisse kantavate andmete koosseis, lõikes 7 andmete säilitamise tähtaeg (kümme aastat registreeringu lõppemisest, mis vastab rakendusmääruse (EL) 2025/848 artiklile 10) ning lõigetes 5 ja 6 volitusnorm andmekogu põhimääruse kehtestamiseks. Punkt 3 ei hõlma isikuandmeid. Registri andmed on eelnõu § 3¹ lõike 4 kohaselt osalise juurdepääsupiiranguga, mille täpsem ulatus sätestatakse põhimääruses. Rakendusmääruse (EL) 2025/848 artikli 3 lõige 4 näeb aga ette, et registreeringut omavate kukrule tuginevate isikute kohta käiv nimetatud rakendusmääruse I lisa loetletud teave tuleb teha internetis avalikult kättesaadavaks nii inimloetavas kui ka masinloetavas vormingus. Seetõttu tuleb põhimääruses eristada avalikustatav teave (rakendusmääruse I lisa) juurdepääsupiiranguga andmetest. Isikuandmete töötlemine registris piirdub peamiselt juriidiliste isikute kontaktisikute andmetega. Registri liidestamisel teiste andmekogudega järgitakse avaliku teabe seaduse § 43⁹ lõiget 5 (andmevahetus X-tee kaudu).

§ 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 digiidentiteedikukru seotud turvarikkumistele ning teavitada vajaduse korral Euroopa Komisjoni ja teisi liikmesriike, kuid ei pane Euroopa digiidentiteedikukru pakkuja otseselt 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 pakumisel 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 viivitamata turvaintsidentidest, mis oluliselt mõjutab või võib mõjutada Euroopa digiidentiteedikukru või selle kaudu osutatava teenuse turvalisust, töökindlust või usaldusväärsust; säte hõlmab nii tegelikke kui ka olulise mõjuga võimalikke turvaintsidente.

Lõikes 2 määratakse kindlaks teate minimaalne 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 pakumise.

§ 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. Senine paragrahvi 5 lõige 4 tunnistatakse kehtetuks, kuna üksikasjalikud nõuded tegevuse lõpetamise kavale on praeguseks kehtestatud eIDAS-määruse otsekohalduva rakendusaktiga.

§ 1 punkt 11. 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 täpsustataksegi, kuidas sellises olukorras Eestis isikut tuvastatakse.

§ 1 punkt 12. 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 13. 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.

Lõige 12 sätestab Euroopa digiidentiteedikukru pakkuja õiguse teha päringuid asjaomastesse registritesse, kui see on vajalik isikutuvastusandmete kukrusse kandmiseks või nende ajakohasuse kontrollimiseks. Kehtiva rakendusmääruse (EL) 2024/2977 kohaselt on kohustuslik andmeväli ka kukru kasutaja sünnikoht, mille kukrusse kandmine võib eeldada päringut rahvastikuregistrisse. Samuti nõuab eIDAS-määruse artikli 5a lõike 9 punkt c, et liikmesriigid tagavad võimaluse tunnistada Euroopa digiidentiteedikukru kasutaja surma korral kehtetuks. Tegemist on isikuandmete töötlemise õigusliku alusega, mille vajalikkus tuleneb vahetult eIDAS-määrusest ja selle rakendusaktidest; päringute maht piirdub kukru väljaandmiseks ja ajakohasena hoidmiseks vajalikuga.

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).

§ 1 punkt 14. Paragrahvi 6 pealkirja täiendatakse, lisades sinna ka Euroopa digiidentiteedikukru pakkuja.

§ 1 punkt 15. Kuna muudetakse 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 16. 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 pakujate üle järelevalvet nii ex ante kui ka ex post, tagamaks pakujate 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.

§ 1 punktid 17 ja 18. Paragrahvi 7 lõike 3 punkti 1 muudetakse ja lõiget 3 täiendatakse punktiga 1⁹, 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.

§ 1 punkt 19. 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.

Punktiga 4 lisatakse taotlemisel esitatavate dokumentide hulka tõend kindlustuse olemasolu kohta. Punktiga 5 loetletakse 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.

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).

§ 1 punkt 20. Paragrahvi 7 lõige 4 tunnistatakse kehtetuks, kuna eIDAS-määruse rakendusaktid kirjeldavad ammendavalt standardeid, mille kohaselt tuleb usaldusteenuse osutamise põhimõtteid kirjeldada.

§ 1 punkt 21. 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 22. Kuna loamenetlus käsitleb kahte eri luba, lisatakse punktiga 2¹ paragrahvi 8 viide eIDAS-määrusele, mille kohase sertifitseerimise peab Euroopa digiidentiteedikukru pakkuja olema läbinud.

§ 1 punkt 23. Paragrahvi 9 lõike 1 punkti 1 ehk loa andmisest keeldumist kirjeldavasse sättesse lisatakse ka Euroopa digiidentiteedikukru pakkuja luba puudutav.

§ 1 punkt 24. Paragrahvi 9 lõikesse 1 lisatud punkt 4 annab võimaluse loa andmisest keelduda, kui vastavushindamisaruandes või sertifitseerimise hindamise aruandes leitakse olulise vastuolu kujul ilmne viga. Olulise vastuolu kujul ilmse vea all peetakse silmas aruandes esinevat viga, mis on ühtaegu ilmne (aruande enda põhjal äratuntav) ja oluline (seab kahtluse alla aruande järelduste usaldusväärsuse); üksnes vormiline või tähendust mittemuutev ebatäpsus loa andmisest keeldumise alust ei anna. Selline piiritlus tagab kooskõla põhiseaduse §-st 10 ja § 13 lõikest 2 tuleneva õigusselguse põhimõttega: loa taotleja jaoks on ette nähtav, millise puuduse korral võib loa andmisest keelduda.

§ 1 punkt 25. 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 26. 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 27. Paragrahvi 9 lõike 3 sõnastust muudetakse nii, et hõlmatud ei oleks ainult kvalifitseeritud usaldusteenused, vaid ka Euroopa digiidentiteedikukru pakkumise teenus.

§ 1 punkt 28. Paragrahvi 9 lõike 4 sõnastust muudetakse, et kajastada olukorda, kus usaldusnimekirja kirjeid ei kustutata, vaid neid muudetakse, et need peegeldaksid tegelikku kehtivuse seisut.

§ 1 punkt 29. Paragrahvi 12 pealkirjas asendatakse 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 30. 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

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

eIDAS-määrus, et liikmesriigid loovad riigipõhise Euroopa digiidentiteedikukru sertifitseerimise kava.

§ 1 punkt 31. 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.

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 32. Paragrahvi 13 pealkirja täiendatakse, kuna muudatustest teavitamine peab hõlmama ka Euroopa digiidentiteedikukrut.

§ 1 punkt 33. Paragrahvi 13 lõike 1 muudatusega viiakse usaldusteenuse muudatustest teavitamise tähtsajad kooskõlla uuendatud eIDAS-määruses sätestatuga. Ühtlasi laiendatakse muudatustest teavitamise kohustust ka Euroopa digiidentiteedikukru pakkujale.

§ 1 punkt 34. Paragrahvi 13 lõiget 3 täiendatakse, seades pädevale asutusele tähtsaja, mille jooksul tuleb teada anda taotluse uuesti esitamise vajadusest. Ühtlasi laiendatakse sätet ka Euroopa digiidentiteedikukru pakkujale.

§ 1 punkt 35. 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 36. 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 lõikes 2 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.

§ 1 punkt 37. Paragrahvi 19 lõikega 4 lisatava sätte eesmärk on näha ette selge õiguslik alus sertifikaatide kehtetuks tunnistamiseks, kui on ilmnenu, et sertifikaatide väljastamine ei vasta

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

usaldusteenuse loa tingimustele või eIDAS-määruses või kõnesolevas seaduses sätestatud nõuetele. Muus osas senise sätte sõnastus on laiahaardeline ning ei tekitanud praktikas küsitavusi ja vastuolulisi tõlgendamisvõimalusi.

§ 1 punkt 38. Paragrahvi 19 lõiget 5 muudetakse, jättes välja viite isikut tõendavate dokumentide seaduses loetletud sertifikaadi kehtetuks tunnistamise alustele ja korrale, kuna samatähenduslik sätte 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.

§ 1 punkt 39. Paragrahvi 22 teksti täiendatakse viitega kõnesoleva paragrahvi lõikes 2 sätestatud erisusele, mis tuleneb eIDAS-määruses toodud järelevalveülesannete kirjeldusest ja hõlmab riikliku andmekaitse järelevalveasutuse pädevust.

§ 1 punkt 40. Paragrahvi 22 senine tekst loetakse lõikeks 1 ja paragrahvi täiendatakse lõikega 2, mis määrab kindlaks Andmekaitse Inspeksiooni rolli järelevalve tegemisel. Euroopa digiidentiteedikukkur peab võimaldama lihtsat teadete edastamist Andmekaitse Inspeksioonile kukrule tuginevate isikute ebaseaduslike või kahtlaste isikuandmetega seotud päringute kohta. Järelevalvemeetmena nähakse ette võimalus piirata Euroopa digiidentiteedikukrule tugineva isiku võimalusi sellele tugineda.

§ 1 punkt 41. Lisanduva paragrahviga 23¹ kehtestatakse sunniraha ülemmääraks kuni 5 000 000 eurot või ettevõtja puhul kuni 1 protsent tema eelneva majandusaasta ülemaailmsest kogukäibest, olenevalt sellest, kumb summa on suurem. Sunniraha ülemmäär on siis sama suur kui väärtekaristuse ülemmäär ning võimaldab pädeval asutusel rikkumiste korral tõhusalt sekkuda. Pädev asutus peab sunniraha määramisel hindama, millises määras on sunniraha rakendamine Eesti kontekstis proportsionaalne.

§ 1 punkt 42. Lisanduva peatükiga 3¹ 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.

§ 1 punkt 43. Eelnõuga lisatava peatüki 3² „Teabevahetus ja aruandlus“ ning § 23⁴ 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 määruses (EL) nr 910/2014 nimetatud teenuse osutajale statistika kogumiseks ja esitamiseks vajalik teabevahetuskohustus. Andmeid kogutakse teenuse osutajalt vajaduspõhiselt ja proportsionaalsuse põhimõttel.

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 „kukrule 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 „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 olevate terminitega.

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 artiklid 5a–5e, 7f, 9, 12, 46a ja 46b), kukrule 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 lisa 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 riigisisised rollid, järelevalve ja karistused.¹² Eelnõu põhilahendused on järgmised: Riigi Infosüsteemi Amet määratakse pädevaks asutuseks ja järelevalveasutuseks (eelnõu § 1 punktid 3 ning 39–42), riigile luuakse võimalus Euroopa digiidentiteedikukru pakkumine ja selleks vajalikud tegevused allhankida (eelnõu § 1 punkt 3), asutatakse kukrute tuginevate isikute register (eelnõu § 1 punkt 6) ning kehtestatakse Euroopa Liidu nõuetele vastavad sunniraha- ja trahvimäärad (eelnõu § 1 punktid 41 ja 42). Selguse huvides kirjeldatakse käesolevas peatükis nii eelnõu enda kui ka eIDAS 2 määruse kohaldamisega kaasnevaid mõjusid, sest sihtrühmade jaoks avalduvad need koos ja lahutamatu. Kavandatud 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).

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.¹³ Euroopa Liidu tasandil on olemas ka põhjalik mõjuhindang. Komisjoni mõjuhindangu¹⁴ 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 teenusepakujate vastuvõtvõime oli ebaühtlane. Komisjoni mõjuhindangut toetavas uuringus¹⁵ hinnati eri poliitikavalikute kulusid ja tulusid avaliku sektori asutustele, internetiteenuste osutajatele, vastavushindamisasutustele, usaldusteenuse osutajatele ja e-identimise vahendite pakujatele. Kuna väljatöötamiskavatsust ei koostatud, esitatakse käesolevas peatükis mõjude analüüs väljatöötamiskavatsuse tasemele vastava põhjalikkusega, tuginedes muu hulgas nimetatud Euroopa Liidu tasandi mõjuhindangule.

Mõjude hindamisel on ajaline raamistik järgmine. eIDAS 2 määrus jõustus 20. mail 2024. Määruse artikli 5a lõike 1 kohaselt peab iga liikmesriik tegema vähemalt ühe Euroopa digiidentiteedikukru (edaspidi ka *digikukkur*) kättesaadavaks 24 kuu jooksul artikli 5a lõikes 23 ja artikli 5c lõikes 6 osutatud rakendusaktide jõustumisest.¹⁶ Samast ajast muutub sisuliselt kohaldatavaks avaliku sektori asutuste kohustus aktsepteerida digikukkrut e-identimist ja e-autentimist nõudvatele internetipõhiste teenuste juurdepääsul (artikli 5f lõike 1).¹⁷

¹² 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.pdf

¹³ Eesti seisukohad Euroopa digiidentiteedi raamistiku määruse eelnõu (COM(2021) 281 final) kohta. EISI toimik 21-0812. <https://eelvoud.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.

¹⁴ 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>

¹⁵ 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>

¹⁶ 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>

¹⁷ 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

Erasektori 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).¹⁸

Peamised sihtrühmad on: 1) füüsilised isikud ehk digikukru potentsiaalsed kasutajad – ligikaudu 1,36 miljonit Eesti elanikku¹⁹ ja teiste liikmesriikide kükrite 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 tuginevad isikud, kellelt nõutakse kasutaja tugevat autentimist, muu hulgas panganduse, finantsteenuste, 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; 6) Riigi Infosüsteemi Amet (edaspidi ka RIA) kui pädev asutus, järelevalveasutus ja digikukru pakkumise korraldaja; 7) Andmekaitse Inspeksioon andmekaitsealase järelevalve tegijana ning 8) 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 määрусega kehtestatud artikli 5a lõige 13) ning kukkur peab pakkuma kõigile füüsilistele isikutele vaikumisi 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.²⁰ Kasutajal on täielik kontroll oma andmete üle: ta saab andmeid valikuliselt avaldada, kasutada varjunimesid ning jälgida kõiki tehinguid ühise töölauda 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.²¹

Eelnõuga tehtav oluline riigisisene kaalutusotsus on isikukoodi kandmine kukrusse. Kuigi eelnõuga korraldatakse otsekohalduva Euroopa Liidu määрус rakendamist Eestis, on siiski valikukohti, mida Euroopa Liidu määрус ette ei kirjuta. Eelnõus nähakse ette, et lisaks

sektori tuginevate isikute poolt). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analüüs.pdf>

¹⁸ Vt viide 16. <https://www.ria.ee/riigi-infosüsteem/elektroonilise-identiteedi-teenused/digikukkur-eudi-wallet>

¹⁹ Statistikaameti andmebaas [e-andmebaas]. RV021. <https://stat.ee/et/avasta-statistikat/valdkonnad/rahvastik/rahvaarv>

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

²¹ Benefits. EU Digital Identity Wallet. Euroopa Komisjoni veebileht, 23.10.2025. <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487811/Benefits>

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 kukrusse kandmine on vajalik, sest Eesti e-teenuste isikutuvastus põhineb valdavalt isikukoodil ning ilma selleta ei oleks kukkur Eesti teenustes seniste riiklike e-identimise vahenditega samaväärselt kasutatav. Meede on proportsionaalne: isikukood on avalik-õiguslikult reguleeritud ja laialdaselt kasutatav identifikaator, mille töötlemine kukrus piirdub isikutuvastusandmete koosseisuga ega too kaasa uue andmekogu loomist. Kaalutud alternatiiv – kukru väljaandmine ilma isikukoodita – jätkaks kukru kasutusalas peamiselt piiriüleseks ega täidaks eesmärki. Andmekaitseriske, sealhulgas isikukoodi ülemäärase avaldamise riski, maandavad eIDAS-määruse nõuded andmete valikulise avaldamise kohta: kasutaja otsustab, milliseid andmeid ta tuginevale isikule avaldab, ning 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 nutitelefoni 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) 2019/882²² 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).²³

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.²⁴ Negatiivse mõju riskina tuleb arvestada uute võimalike pettuseskeemide (nt õngitsus- ja QR-koodiründed) levikuga kukru kasutuselevõtu algusfaasis. Seda riski aitavad maandada määruse ja rakendusaktide turvanõuded, kukru sertifitseerimine ning kasutajate teavitamise tegevused.²⁵

Mõju olulisus: mõju ulatus on keskmine (teenuste kasutamise viis muutub, kuid sihtrühma käitumisega ei kaasne kohanemiskulusi, sest kasutamine on vabatahtlik ja senised vahendid

²² 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).

²³ 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>

²⁴ Vt viide 23, lisa 8 (Nõuded alaealistele kukruteenuse pakkumiseks). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuu.pdf>

²⁵ Vt viide 17, ptk 7 (QR-kood ründesaidi ründekaitse). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuu.pdf>

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

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; kukru 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 Euroopa digiidentiteedikukkur sisaldab 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 rüündepind: 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.²⁶ 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.²⁷ Määruse artikkel 5e näeb turvarikkumise korral ette kukru 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

²⁶ 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>

²⁷ Vt viide 17, ptk 5 (Massallkirjastamise piirangud ja tingimused). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuus.pdf>

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 kukruid, mistõttu peavad Eesti teenusepakkujad olema valmis aktsepteerima ka teiste liikmesriikide kukruid. Peame arvestama, et osa liikmesriike võib oma kukrud kasutusele võtta juba 2026. aasta lõpuks.²⁸

Teiseks peavad kõik digikukrule tugineda soovivad ettevõtjad end registreerima kukrule tuginevate isikute riiklikus registris (määruse artikkel 5b, komisjoni rakendusmäärus (EL) 2025/848²⁹). Registreerimisprotsess peab olema kulutõhus ja riski suhtes proportsionaalne: rakendusmäärus nõuab veebipõhist ja võimaluse korral automaatset registreerimist ning taotluste menetlemist põhjendamatult 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.³⁰ Eelnõuga ei kehtestata 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 analüüsides³¹ ning digikukru kasutuse majandusmudeli selgitamise vajadus tõstatati juba 2021. aasta kaasamisel.³²

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 Liidus.³³ 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.³⁴ Samal ajal karmistuvad vastavusnõuded: kvalifitseeritud usaldusteenuse osutajaid auditeeritakse vähemalt iga 24 kuu järel (artikli 20 lõige 1) ning liikmesriigid peavad

²⁸ Vt viide 16. <https://www.ria.ee/riigi-infosustee/elektroonilise-identiteedi-teenused/digikukkur-eudi-wallet>

²⁹ Vt viide 6. http://data.europa.eu/eli/reg_impl/2025/848/oj

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

³¹ 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>

³² Vt viide 29. http://data.europa.eu/eli/reg_impl/2025/848/oj

³³ Vt viide 23, ptk 2 (Digiidentiteedikukru ökosüsteem). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuus.pdf>

³⁴ 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>

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). Eelnõuga e-identimise ja e-tehingute usaldusteenuste seaduses kehtestatavad karistusnormid (eelnõu § 1 punktid 41 ja 42) 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.³⁵ 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.³⁶ Need on liidu koondhinnangud; Eesti-spetsiifiline kvantitatiivne hinnang koostatakse eelnõu menetluse käigus (vt punkt 6.6).

Eesti kaalutlusotsustest 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 juhuks, kui kukru 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 hinnanguliselt 350–400 miljoni euro võrra aastas.³⁷ 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

³⁵ 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>

³⁶ Vt viide 21. <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487811/Benefits>

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

elektrooniliste tõendite kasutuselevõtt vähendada paber- ja plastdokumentide kasutust, kuid see mõju ei ole mõõdetav ega antud 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 digikukku pakkumise korraldamine riigi nimel (sh võimalus pakkumine ja selleks vajalikud tegevused allhankida), kukrule tuginevate isikute riikliku registri asutamine ja pidamine koos pääsuserifikaatide väljastamise korraldamisega, Euroopa digiidentiteedikukku pakkuja loamenetlus, e-identimise süsteemide usaldusväärsuse taseme samaväärsuse hindamine e-identimise ja e-tehingute usaldusteenuste seaduse³⁸ § 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 digiidentiteedikukku raamistiku järelevalveasutuse roll (määruse artikkel 46a).³⁹ 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 digikukku 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.⁴⁰ Andmekaitse Inspeksiooni töökoormus suureneb digikukku ja sellega seotud töötlemistoimingute andmekaitsealase järelevalve võrra, sealhulgas kasutajate teadete menetlemisega, mida saab esitada otse kukku ühise töölaua kaudu (artikli 5a lõike 4 punkt d).

Digikukku ökosüsteemi käivitamine eeldab lisaks mitme muu asutuse panust. Riiklik sertifitseerimiskava tuleb igal liikmesriigil kehtestada oma kukkulahenduse 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 ministriumide ülesanne (eelnõu § 1 punkt 31). Kukku vastavushindamisasutuse akrediteerimine on riikliku akrediteerimisasutuse (Eesti Standardimis- ja Akrediteerimiskeskus) uus akrediteerimisteenus, millest tuleb teavitada Euroopa Komisjoni.⁴¹ Digikukku kavandatakse eraldiseisva mobiilirakendusena. Kui digikukku kavandatakse kombineerituna mõne muu mobiilirakendusega (nt riigiäpiga), muutub kukku sertifitseerimine keerukamaks ja EUDI-

³⁸ Vt viide 3. <https://www.riigiteataja.ee/akt/130122025016>

³⁹ Vt viide 23, ptk 2. <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukku-II-etapi-analuu.pdf>

⁴⁰ Vt viide 14, 5. lisa. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0124>

⁴¹ 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/Digikukku-II-etapi-analuu.pdf>

nõuded võivad laieneda rakenduse muudele funktsioonidele; seetõttu tuleb arhitektuurivalikul eraldi hinnata turvaperimeetrit, sertifitseerimise ulatust ja lisamoodulite mõju hindamisobjektile.⁴² Digikukru kui kõrge usaldusväärsuse tasemega e-identimise vahendi väljaandmine eeldab isikutuvastusandmete väljastamisel koostööd Rahvastikuregistri ja Isikut tõendavate dokumentide andmekogu pidajaga.⁴³ 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.⁴⁴

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 tuginevate isikute nimel tegutsevad vahendajad ei tohi salvestada andmeid tehingu sisu kohta (artikli 5b lõige 10).⁴⁵ 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.⁴⁶ Asutused, kes kesket autentimisteenust ei kasuta, peavad oma autentimislahendused ise kohandama. Kohaliku omavalitsuse üksustele ei panda eelnõuga uusi iseseisvaid ülesandeid ega rahastamiskohustusi; nende koormus piirdub keskse autentimisteenuse kaudu lisanduvate võimaluste kasutuselevõttuga.

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 (tähtaegse valmimise risk). Mõju on **oluline**.

Järeldamine

Järeldamise alus on suures osas määruses endas ette nähtud. 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

⁴² Vt viide 17, ptk 2 (Superäpp). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuus.pdf>

⁴³ 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>

⁴⁴ 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>

⁴⁵ Vt viide 17, ptk 11 (TARA kui digikukru liides). <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-III-etapi-analuus.pdf>

⁴⁶ Vt viide 29. http://data.europa.eu/eli/reg_impl/2025/848/oj

Euroopa Komisjonile igal aastal 31. märtsiks avatud ja masinloetavas vormingus.⁴⁷ Euroopa Komisjon hindab omakorda määruse artikli 5f lõike 5 kohaselt 24 kuu jooksul digikukrute kasutuselevõttust nende nõudlust, kättesaadavust ja kasutatavust. Riigisisese seiravad Justiits- ja Digiministeerium ja RIA digikukru kasutuselevõttu jooksvalt vähemalt eelnimetatud artikli 48a näitajate alusel, millele lisanduvad registreeritud kukrule tuginevate isikute arv ning digikukruga tehtud autentimiste ja allkirjastamiste maht. Seaduse rakendumise järelhindamise käigus hinnatakse muu hulgas karistusnormide ja riigilõivude asjakohasust ning halduskoormuse tegelikku muutust.

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

Seaduse rakendamisega kaasnevad lisakulud riigieelarvele jagunevad rakendamise kuludeks (Euroopa digiidentiteedi kukru taristu loomine ja haldamine ning teenuste liidestamine) ja järelevalve tugevdamise kuludeks. Kulusid kannavad Riigi Infosüsteemi Amet, Justiits- ja Digiministeerium, Andmekaitse Inspeksioon ning digikukruga liidestuvad ministeeriumid. Kohaliku omavalitsuse üksustele lisakulusid ega uusi ülesandeid ei kaasne. Kulud kajastavad riigieelarve lisavajadust perioodil 2027–2030 ja on arvestatud asutuste eelarvestuste alusel⁴⁸: infotehnoloogiliste arenduste maksumus keskmise turuhinna ja eeldatava töömahu alusel, tööjõukulud tööperede palgatasemete alusel. Samas tuleb arvestada, et projekt jätkub ja sellega kaasnevad kulud ka pärast 2030. aastat.

7.1. Riigi Infosüsteemi Ameti kulud

RIA kannab rakendamise kulusid kokku **15 933 500 eurot** ja järelevalve tugevdamise püsikulu **300 000 eurot** (75 000 eurot aastas), seega kokku **16 233 500 eurot**. Rakendamise kuludest moodustavad ühekordsed investeeringud 2 990 000 eurot ning majandamis- ja tööjõukulud vastavalt 10 182 500 ja 2 761 000 eurot. Rakendustegevused on: – digikukru teenusepakkuja hankimine, sealhulgas hanke ja lepingu kulud, valdkonna kommunikatsioon ning analüüsid ja uuringud (sh üleliidulise koostalitlusvõime tagamiseks vajalikel kohtumistel osalemine); – tuginevate isikute registri loomine ja haldamine; – tõendite vahendamise lüüsi loomine ja haldamine; – olemasolevate e-identimise baasestuste TARA API, DigiDoc ja SiGa kohandamine digikukru vajadustele. Järelevalve hõlmab EUDI raamistiku järelevalvet, sealhulgas tegevuslubade väljastamist, teenuseosutajate üle arvestuse pidamist ning aruandlust Euroopa Komisjonile ja Euroopa Liidu Küberturvalisuse Ametile (ENISA). Rakendustegevuste kulud aastate lõikes on esitatud tabelis 1.

Tabel 1. RIA rakendustegevused ja kulud aastatel 2027–2030 (eurodes)

Rakendustegevus	2027	2028	2029	2030	Kokku
1. Digikukru teenusepakkuja hankimine	2 896 833	3 729 800	2 641 400	2 305 800	11 573 833
2. Tuginevate isikute register	562 000	386 100	394 800	405 600	1 748 500
3. Tõendite vahendamise lüüs	524 667	386 100	394 800	405 600	1 711 167
4. TARA API kohandamine	150 000	100 000	0	0	250 000

⁴⁷ Vt viide 23, lisa 9. <https://www.ria.ee/sites/default/files/documents/2026-05/Digikukru-II-etapi-analuus.pdf>

⁴⁸ Kulude arvestuse aluseks on asutuste koostatud eelarvestused.

Rakendustegevus	2027	2028	2029	2030	Kokku
5. DigiDoc'i kohandamine	150 000	150 000	0	0	300 000
6. SiGa kohandamine	200 000	150 000	0	0	350 000
Kokku	4 483 500	4 902 000	3 431 000	3 117 000	15 933 500

Allikas: Riigi Infosüsteemi Ameti eelarvestus.

7.2. Justiits- ja Digiministeeriumi, Andmekaitse Inspektsiooni ja liidestuvate ministeeriumide kulud

Justiits- ja Digiministeeriumi lisavajadus on kokku **2 410 000 eurot** (2027. ja 2028. aastal 685 000 aastas, 2029. aastal 570 000 ja 2030. aastal 470 000 eurot). Kulud on seotud riikliku sertifitseerimisskeemi väljatöötamise ja kinnitamisega.

Andmekaitse Inspektsiooni lisavajadus on kokku **302 088 eurot** (75 522 eurot aastas⁴⁹), sellest tööjõukulu 68 206 ja majandamiskulu 7316 eurot aastas, mis on vajalik eIDAS-määrusest tulenevate järelevalvekohustuste täitmiseks, sealhulgas menetlemaks andmesubjektide teateid kahtlaste või ebaseaduslike andmepäringute kohta.

Digikukruga liidestuvate ministeeriumide (haldusalade) kulud on kokku **2 000 000 eurot** (2029. ja 2030. aastal 1 000 000 eurot aastas). RIA ning Justiits- ja Digiministeerium loovad eIDAS-määrusele vastavad üldkomponendid ja -funktsioonid, kuid teenuste liidestamine digikukruga ja tõendite koostalitlusvõime tagamine on iga haldusala ülesanne.

7.3. Kulude koondülevaade

Kulud asutuste ja aastate lõikes on esitatud tabelis 2. Rakendamise ja järelevalve lisavajadus on perioodil 2027–2030 kokku 20 945 588 eurot.

Tabel 2. Kulud asutuste ja aastate lõikes aastatel 2027–2030 (eurodes)

Asutus	2027	2028	2029	2030	Kokku
Riigi Infosüsteemi Amet (rakendamine ja järelevalve)	4 558 500	4 977 000	3 506 000	3 192 000	16 233 500
Justiits- ja Digiministeerium	685 000	685 000	570 000	470 000	2 410 000
Andmekaitse Inspektsioon	75 522	75 522	75 522	75 522	302 088
Liidestuvad ministeeriumid	0	0	1 000 000	1 000 000	2 000 000
Kokku	5 319 022	5 737 522	5 151 522	4 737 522	20 945 588

Allikas: asutuste koostatud eelarvestused.

7.4. Mõju kohaliku omavalitsuse üksuste eelarvetele

Kohaliku omavalitsuse üksustele ei panda eelnõuga uusi iseseisvaid ülesandeid ega rahastamiskohustusi ning eelnõu rakendamisega ei kaasne neile lisakulusid; nende koormus piirdub keskse autentimisteenuse kaudu lisanduvate võimaluste kasutuselevõtuga. Digikukru

⁴⁹ Andmekaitse Inspektsiooni eelarvestuse tekstiline selgitus esitab aastase lisavajaduse 75 519 eurot (palgakulu 68 203 ja majandamiskulu 7316 eurot); erinevus eelarveridade summast (75 522 eurot) tuleneb ümardamisest.

tugi lisatakse riigi kesksesse autentimisteenusesse (TARA) riigieelarve vahenditest, misjärel jõuab see kohaliku omavalitsuse üksusteni ilma nende eraldi arenduste, töökoormuse või kuluta.

7.5. 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 rakendamise eest ei kaasne.

Kulud kaetakse riigieelarvest ning vastavad eelarvetaotlused esitatakse riigieelarve protsessis. Praegu nendeks ülesanneteks eelarves katet ei ole. Lisaressursi tagamine on rakendamise eeldus: ilma selleta ei ole võimalik täita määrusest (EL) 2024/1183 (eIDAS2) tulenevaid ülesandeid, millega kaasneb Euroopa Liidu õiguse rikkumise menetluse ja rahaliste sanktsioonide risk.

8. Rakendusaktid

Eelnõuga antakse üks uus volitusnorm: e-identimise ja e-tehingute usaldusteenuste seaduse § 3¹ lõigete 5 ja 6 alusel kehtestab valdkonna eest vastutav minister määrusega tuginevate isikute registri põhimääruse, milles sätestatakse andmekogu pidamise korraldus, täpne andmekoosseis, andmete esitamise ja registreeringu menetlemise kord ning vajaduse korral muud andmekogu pidamisega seotud korralduslikud küsimused. 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 lisa 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 30 tunnistatakse kehtetuks e-identimise ja e-tehingute usaldusteenuste seaduse § 12 lõige 2, mille tagajärjel muutub kehtetuks selle alusel antud Vabariigi Valitsuse määrus „Usaldusteenuse osutaja ja usaldusteenuse vastavushindamise kord“.⁵⁰

Euroopa digiidentiteedikukru sertifitseerimise kava, mille koostamise kohustus pannakse eelnõuga valdkonna eest vastutavale ministeeriumile (eelnõu § 1 punkt 31), ei ole õigustloov akt ega rakendusakt hea õigusloome ja normitehnika eeskirja tähenduses, vaid haldusesisene dokument, mis avaldatakse ministeeriumi veebilehel. Samuti ei eelda eelnõu muud rakendusakti: registreerimistaotluste esitamise tehniline kord tehakse kättesaadavaks 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 riigisisest rakendusmeetmet (pädeva asutuse määramine, loamenetlus, register, karistusnormid) ei nõua sihtrühmadelt sellist kohanemisaega, mis eeldaks pikemat jõustumistähtaega. Vastupidi, riigisiseste rollide ja menetluste võimalikult varane jõustumine

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

on vajalik, et 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 esitatakse eelnõude infosüsteemi (EIS) kaudu kooskõlastamiseks kõikidele ministeeriumitele ning arvamuse avaldamiseks Riigi Infosüsteemi Ametile, Andmekaitse Inspeksioonile, Tarbijakaitse ja Tehnilise Järelevalve Ametile, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule, Eesti Linnade ja Valdade Liidule, Statistikaametile, Maa- ja Ruumiametile, Rahvusarhiivile, Politsei- ja Piirivalveametile, Siseministeeriumi infotehnoloogia- ja arenduskeskusele, Registre ja Infosüsteemide Keskusele, Keskkonnaministeeriumi Infotehnoloogiakeskusele, Regionaal- ja Põllumajandusministeeriumi Infotehnoloogia Keskusele, Rahandusministeeriumi Infotehnoloogiakeskusele ja Tervise ja Heaolu Infosüsteemide Keskusele.

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

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 mõjuhinnangut toetavas uuringus.⁵² Lisaks avalikule konsultatsioonile sai komisjon kirjalikku tagasisidet esialgse mõjuhinnangu kohta (23. juulist 3. septembrini 2020), korraldas sihitatud sidusrühmauringu (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 aksepteeritavust (47% vastanutest), kasutusmugavust (43%) ja riigi tagatud usaldusväärsust (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 ministeeriumid, 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 Siseministeerium toetas eelnõu eesmäärke, huvirühmad tõstatasid küsimusi digikukru seosest olemasoleva eID-ökosüsteemi ja X-tee andmevahetusloogikaga, riigisisestest kuludest, majandusmudelitest, erasektori vastutusest ja rakendamise tähtajast ning Eesti tegi ettepaneku näha kukru kasutuselevõtuks ette 24 kuud 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

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.

⁵⁵ Vt viide 29.

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, 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 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, tuginevate isikute register, järelevalve ja karistused, sertifitseerimise ulatus – on käsitletud seletuskirja 6. peatükis ja eelnõu sisu peatükis (seletuskirja 3. peatükk).

Kooskõlastamise ja arvamuste esitamise tulemused ning saadud märkuste arvestamise ülevaade esitatakse seletuskirja lisa märkuste tabelina, milles kajastatakse iga märkuse sisu, esitaja ning arvestamine või arvestamata jätmine koos põhjendusega (hea õigusloome ja normitehnika eeskirja § 50 lõiked 2 ja 3). [Täidetakse menetluse käigus.]

Seletuskirja lisad

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

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

Lisa 3. Märkuste tabel. [Täidetakse menetluse käigus.]

⁵⁶ Pilootprojekt POTENTIAL (digitaalne juhiluba). Riigi Infosüsteemi Ameti koduleht, 19.05.2026. <https://www.ria.ee/riigi-infosusteem/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.

Lauri Hussar
Riigikogu esimees

Tallinn,2026

Algatab Vabariigi Valitsus2026

(allkirjastatud digitaalselt)