14.04.2023

Isikut tõendavate dokumentide seaduse muutmise seaduse eelnõu väljatöötamise kavatsus

I. Probleem, sihtrühm ja eesmärk

1. Probleemi kirjeldus ja selle tekke põhjus

2014. aastal loodud e-residentsuse programmi eesmärk on soodustada Eesti majanduse, teaduse, hariduse ja kultuuri arengut, võimaldades välisriigi kodanikele turvalise ligipääsu Eesti riigi e-teenustele ning Eesti ja Euroopa majandusruumile. E-residentsust on võimalik kasutada muu hulgas ettevõtte asutamiseks ja selle juhtimiseks ning finantsteenuste kasutamiseks.

E-residentsuse programmi elukaare jooksul on oluline pidevalt arvestada ja hinnata üha kiiremini muutuvat julgeolekuolukorda ja sellega kaasnevaid riske ning kavandada asjakohased maandamismeetmed. Oluline on, et riskide realiseerumine ei tooks kaasa märkimisväärselt negatiivseid tagajärgi riigi julgeolekule, majandusele ja e-residentsuse programmile.

E-residentsuse programmi riskide maandamise üks peamine eeldus on, et riik teab, kes on Eesti e-residendid (edaspidi *e-resident*). Selleks viiakse e-residentsuse taotlejate seas läbi riskipõhine eel- ja järelkontroll tagamaks, et e-residentideks saaksid ainult õiguskuulekad välismaalased, eelkõige riikidest, kellega on Eestil kehtestatud viisavabadus või kellega on Eestil justiits-, julgeoleku- ja õiguskaitsealased koostöösuhted. Tuleb arvestada, et isiku tegelikus taustas võivad esineda olulised puudujäägid, kui ta on pärit riigist, kellega koostöö puudub.

Ühe suurima e-residentsuse programmi riskina on nii rahapesu ja terrorismi rahastamise riiklikus riskihinnangus[1] kui ka Euroopa Nõukogu rahapesu ja terrorismi rahastamise tõkestamise meetmeid hindava eksperdikomitee (edaspidi *Moneyval*) hindamisaruandes[2] välja toodud, et e-residentsuse programm võimaldab välismaalastel kasutada Eestis e-residentsust ebasoovitavaks ettevõtluseks ning varjata ettevõtluse tegelikku sisu ja eesmärki ning sellest kasu saajaid. Eriti probleemne on see kolmandate riikide puhul, kellega puuduvad Eestil justiits-, julgeoleku- ja õiguskaitsealased koostöösuhted. See tähendab, et Eestil pole võimalik tõhusalt kontrollida selliste riikide kodanike tausta, saada nende kohta usaldusväärset teavet ega veenduda, et e-residendi digitaalse isikutunnistuse (edaspidi *digi-ID*) kasutaja on selle omanik. Seetõttu võib venida või ebaõnnestuda õigusrikkumiste uurimine, tõendite kogumine, kohtumenetlus, pankrotimenetlus jne.

[1] Rahandusministeerium 2020. Rahapesu ja terrorismi rahastamise riiklik riskihinnang.
[2] Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism 2022. Anti-money laundering and counter-terrorist financing measures. Estonia. Fifth Round Mutual Evaluation Report.

Politsei- ja Piirivalveamet (edaspidi *PPA*) kontrollib digi-ID taotluse menetlemisel taotleja isikusamasust, seost Eestiga ning seda, kas taotleja on pannud toime süüteo Eestis või teises riigis ja kas teda kahtlustatakse rahapesus. Samuti teeb PPA muid menetlustoiminguid, lähtudes taotleja profiilist ja oma võimalustest. Sellele vaatamata on aga osa e-residentsuse programmi riske realiseerunud. On tuvastatud äärmusluse ja terrorismiga seotud e-residente ning e-residentsuse programmi on püütud kasutada immigratsioonipettustes. Samuti on tuvastatud juhtumeid, kus e-residentide ettevõtted on seotud investeerimis- ja laenupõhise ühisrahastuse kelmustega. Ka virtuaalvääringu valdkonnas võidakse e-residentsust kuritarvitada, näiteks anda digi-ID kasutada teisele isikule. Selline käitumine ei ole õiguspärane, kuna teisel isikul on keelatud digi-ID-d kasutada. Puudub võimalus kontrollida, kas digi-ID taotleja ja kasutaja on sama isik, misläbi on e-residendil võimalik varjata oma tegelikku eesmärki ja tausta.

Paljud e-residentsuse väärkasutamise juhtumid on saanud teatavaks tänu rahvusvahelisele koostööle, mille tulemusel laekub PPA-le igal aastal e-residentide riskikäitumisele, sealhulgas rahapesule ja virtuaalvääringu pettustele, viitavaid päringuid riikidest, kellega Eestil on toimiv koostöö. Näiteks tunnistati 2022. aastal sellistest päringutest ajendatult kehtetuks 26 digi-ID-d. Digi-ID kehtetuks tunnistamine maandab aga riske vaid osaliselt, kuna e-residendiga seotud ettevõtte õigusvõime säilib ka pärast digi-ID kehtetuks tunnistamist.

Seega on toimiva koostöö korral võimalik maandada riske läbi tugeva taustakontrolli, kuid see ei toimi riskiriikide kodanike puhul. Sageli on just riskiriigid seotud suurema terrorismi ja selle rahastamise ohuga ning pelgalt tugevam taustakontroll pole piisav kuritegevus- ja julgeolekuriskide maandamiseks määral, mis võimaldaks Eestil vältida olulist kahju.

Eeltoodud asjaoludega arvestamata jätmine toob kuritegevus- ja julgeolekuohtude kõrval mainekahju nii Eesti riigile, majandusruumile kui ka e-residentsuse programmile ning ei ole kooskõlas programmi eesmärgiga.

Arvestades eeltoodut ja fakti, et riskiriikide kodanike tausta ei ole võimalik tõhusalt kontrollida ega saada nende kohta usaldusväärset teavet, ei ole põhjendatud jätkata senist juhtumipõhist digi-ID taotluste hindamist, vaid tuleb **piirata kõrgema terrorismi rahastamise riskiga riikide kodanike ligipääsu e-residentsusele.**

2. Sihtrühm

Kavandatava muudatuse peamine sihtrühm on Rahapesu Andmebüroo (edaspidi *RAB*) nimekirjas olevate kõrgema terrorismi rahastamise riskiga riikide (edaspidi *riskiriik*) kodanikud, kes soovivad pärast muudatuse jõustumist taotleda digi-ID-d. Muudatuse teisene sihtrühm on PPA ametnikud, kes menetlevad digi-ID taotlusi.

Riskiriikide kodanikud

RAB-i nimekirjas[3] on praegu 28 riskiriiki: Afganistan, Alžeeria, Araabia Ühendemiraadid, Burkina Faso, Egiptus, Iraak, Iraan, Jeemen, Jordaania, Kongo DV, Liibanon, Liibüa, Lõuna-Sudaan, Mali, Maroko, Mosambiik, Nigeeria, Niger, Pakistan, Palestiina Omavalitsus, Põhja-Korea, Saudi Araabia, Somaalia, Sudaan, Süüria, Tuneesia, Türgi ja Usbekistan[4].

[3] Rahapesu Andmebüroo 2022. Juhend kahtlaste tehingute tunnuste kohta. Lisa: kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid.

[4] Lisaks on nimekirjas Venemaa Föderatsiooni Põhja-Kaukaasia föderaalringkond. Venemaa ja Valgevene kohta kehtib Vabariigi Valitsuse 8. märtsi 2022. aasta otsus e-residentsuse programmi mittevõimaldamise kohta ning kavandatav muudatus hõlmab ka neid.

Kavandatava muudatuse kohaselt ei piirata digi-ID väljaandmist Türgi ja Araabia Ühendemiraatide kodanikele ning seda nii julgeoleku-, majandus- kui ka välispoliitilistel põhjustel. Türgi on NATO liikmesriigina Eestile oluline julgeolekupartner ning aktiivseid riskiriigi kodakondsusega e-residente (edaspidi *riskiriigi e-resident*) on kõige rohkem Türgist, s.o 44% riskiriigi e-residentidest. Samuti on selliste riskiriigi e-residentide ettevõtete hulgas, kes on alustanud reaalset majandustegevust, kõige rohkem Türgi kodanike ettevõtteid. Kõikide riskiriigi e-residentide ettevõtete tasutud maksudest moodustavad Türgi kodakondsusega e-residentide ettevõtete riiklikud maksud *ca* 96% ja tööjõumaksud 90%. Araabia Ühendemiraadid on Eestile oluline piirkond riiklike ja ärisuhete loomisel ning edendamisel, samuti Eesti ekspordi arendamisel. Araabia Ühendemiraadid olid 2020. aastal Eesti jaoks suuruselt 36. eksporditurg, kus Eesti, sealhulgas e-residentide ettevõtetel on suurepärased ärivõimalused, näiteks IT-sektoris.

Sihtrühma suurus

28. veebruari 2023. aasta seisuga on kehtiv digi-ID **6406** riskiriigi kodanikul, mis on *ca* **10%** kõikidest kehtivatest digi-ID-dest.

Tabel 1. Riskiriigi e-residendid

Kodakondsus	**Arv**	**Osakaal %**
Türgi	2817	43,97
Pakistan	672	10,49
Iraan	638	9,96
Egiptus	493	7,70
Tuneesia	352	5,49
Maroko	270	4,21
Alžeeria	166	2,59
Nigeeria	158	2,47
Liibanon	150	2,34
Süüria	133	2,08
Jordaania	125	1,95
Usbekistan	87	1,36
Iraak	57	0,89
Jeemen	49	0,76
Liibüa	48	0,75
Saudi Araabia	38	0,59
Sudaan	36	0,56
Palestiina Omavalitsus	35	0,55
Afganistan	29	0,45
Kongo DV	19	0,30
Mali	12	0,19
Burkina Faso	11	0,17
Araabia Ühendemiraadid	8	0,12
Mosambiik	2	0,03
Somaalia	1	0,02
Kokku	**6406**	**100,00**

Allikas: PPA

PPA ametnikud
Kavandatava muudatuse teisene sihtrühm on PPA ametnikud, kes menetlevad digi-ID taotlusi. Neid on kaheksa.

3. Eesmärk ja saavutatava olukorra kirjeldus

Eeltoodud riskide maandamiseks on kavas muuta isikut tõendavate dokumentide seadust (edaspidi *ITDS*) selliselt, et PPA ei võta edaspidi vastu digi-ID taotlusi RAB-i nimekirja kantud riskiriikide kodanikelt, kui ei rakendu erisus.

Riskiriigi kodanikule varem väljastatud digi-ID jääb kehtima, ja kui see aegub, saab ta esitada kordustaotluse. Korduva digi-ID väljaandmist hindab PPA juhtumi kaupa.

II. Hetkeolukord, uuringud ja analüüsid

4. Kehtiv regulatsioon, seotud strateegiad ja arengukavad

Digi-ID väljaandmist on reguleeritud ITDS-i 5[2]. peatükis. Digi-ID väljaandmisest keeldumise alused on sätestatud ITDS-i §-s 20[6], mille kohaselt digi-ID:

- väljaandmisest keeldutakse, kui:
  1) isik ohustab avalikku korda või riigi julgeolekut;
  2) digi-ID-d taotletakse majandustegevuseks ja esineb majandustegevuse keelamise alus;
  3) isik ei ole tõsikindlalt tuvastatud või tema isikusamasuses on põhjust kahelda;
- väljaandmisest võib keelduda, kui:
  1) esineb viisa või tähtajalise elamisloa andmisest keeldumise või sissesõidukeelu kohaldamise aluseks olev asjaolu;
  2) digi-ID väljaandmine ei ole kooskõlas ITDS-i § 20[5] lõikes 2 nimetatud eesmärgiga soodustada Eesti majanduse, teaduse, hariduse või kultuuri arengut.

Digi-ID väljaandmisest keeldumise alused ei võimalda laiapinnaliselt keelduda digi-ID taotluste vastuvõtmisest riskiriikide kodanikelt. Igas juhtumis tuleb eraldi kaalutleda, kas taotleja ohustab avalikku korda või riigi julgeolekut või kas talle dokumendi väljaandmine on kooskõlas e-residentsuse eesmärgiga.

E-residentsuse valdkonna arengusuunad on seotud siseturvalisuse arengukava 2020-2030[5] tegevussuunaga 4.3 „Usaldusväärne ja turvaline identiteedihalduspoliitika“, mille kohaselt peab tõsikindel, stabiilne ja jätkusuutlik riiklik identiteedihalduspoliitika, milles on Eesti maailmas valdkonna eestvedaja, arvestama vajadusega tagada avalik kord ja riigi julgeolek.

E-residentsuse järgnevate aastate põhisuunad on määratud e-residentsuse jätkustrateegias 2022–2025[6]. E-residentsuse riskide maandamise meetmetena on selles toodud välja, et e-residentsust ei pakuta üldjuhul nende riikide kodanikele, millest tuleneb ulatuslik julgeoleku- või digi-ID väärkasutuse oht, ning e-residendina on eriti eelistatud taotlejad riikidest, kellega Eesti teeb justiits-, julgeoleku- ja õiguskaitsealast koostööd.

[5] Siseministeerium. Siseturvalisuse arengukava 2020–2030.
[6] Majandus- ja Kommunikatsiooniministeerium. E-residentsuse jätkustrateegia 2022–2025.

E-residentsuse riske on läbivalt analüüsitud erinevates riskihinnangutes. Riskiriikide kodanikele e-residentsuse võimaldamine on ühe suurima e-residentsuse programmi riskina nimetatud nii rahapesu ja terrorismi rahastamise riiklikus riskihinnangus kui ka Moneyvali hindamisaruandes.

5. Tehtud uuringud

Seaduseelnõu väljatöötamise kavatsusele (edaspidi *VTK*) ei eelnenud eraldi uuringuid ega analüüse.

6. Kaasatud pooled

Enne VTK koostamist peeti arutelusid seotud pooltega: Ettevõtluse ja Innovatsiooni Sihtasutuse, RAB-i, PPA ja Kaitsepolitseiametiga.

Kavandatav muudatus kiideti heaks e-residentsuse nõukogus, kuhu kuuluvad e-residentsuse programmiga seotud ministeeriumide ja nende valitsemisala asutuste esindajad[7].

III. Probleemi võimalikud mitteregulatiivsed lahendused

7. Kaalutud võimalikud mitteregulatiivsed lahendused

• **Avalikkuse teavitamine**	EI
• **Rahastuse suurendamine**	JAH
• **Mitte midagi tegemine ehk olemasoleva olukorra säilitamine**	JAH
• **Senise regulatsiooni parem rakendamine**	JAH
• **Muu**	EI

7.1. Kaalutud võimalike mitteregulatiivsete lahenduste võrdlev analüüs

Rahastuse suurendamine. Rahapesu ja terrorismi rahastamise riiklikus riskihinnangus on toodud ühe järelevalve tõhustamise meetmena välja rahastuse suurendamine. Sellega ei ole aga võimalik muudatuse sihtrühmas soovitud mõju saavutada, kuna Eestil ei ole riskiriikidega justiits-, julgeoleku- ja õiguskaitsealaseid koostöösuhteid ning taustakontrollis on võimalik lähtuda vaid taotleja ütlustest, mida ei ole võimalik kontrollida riiklikest allikatest. Seega ei aita rahastuse suurendamine saavutada soovitud eesmärki.

Mitte midagi tegemine ehk olemasoleva olukorra säilitamine. Kehtivat õigust muutmata antaks riskiriikide kodanikele ka edaspidi digi-ID, st võimaldaksime riigina endiselt kahjustada Eesti majandust, julgeolekut ja mainet. Moneyvali hindamisaruanne tõstis e-residentsuse riskide maandamise vajalikkuse aktiivselt päevakorda, sest juhul, kui hindamisaruandes käsitletud probleemidega ei tegeleta, riskib Eesti tõsiste majanduslike ja maineliste tagajärgedega. Et seda vältida, ei saa säilitada olemasolevat olukorda.

Senise regulatsiooni parem rakendamine. Kehtiv õigus ei võimalda laiapinnaliselt keelduda digi-ID taotluste vastuvõtmisest riskiriikide kodanikelt, kuid on rakendatud erinevaid riskide maandamise meetmeid. E-residentsuse jätkustrateegias 2022–2025 on nimetatud järgmised

[7] Esindatud on Justiitsministeerium, Majandus- ja Kommunikatsiooniministeerium, Rahandusministeerium, Siseministeerium, Välisministeerium, Ettevõtluse ja Innovatsiooni Sihtasutus ning PPA.

riskide maandamise meetmed: 1) taustakontrolli tõhustamine, 2) teenuseosutajate tehtav kontroll digi-ID kasutamise üle, 3) Riigi Infosüsteemi Ameti seiretugi, 4) digi-ID sertifikaadi kehtivuse peatamine, 5) digi-ID sertifikaadi kehtetuks tunnistamine ning 6) keskendumine turvalistele sihtriikidele. Kõiki nimetatud meetmeid, välja arvatud viimast, on juba rakendatud, kuid nagu 2022. aasta Moneyvali hindamisaruandest selgus, ei ole need meetmed olnud piisavalt tõhusad ega maanda olulisi riske riskiriikide puhul, kellega puudub Eestil koostöö.

7.2. Järeldus mitteregulatiivse lahenduse sobimatuse kohta

Eeltoodu põhjal saab järeldada, et mitteregulatiivsed lahendused ei täida soovitud eesmärki ja kõige paremini maandab riske digi-ID taotlemise piirang riskiriikide kodanikele. Sageli on just riskiriigid seotud suurema terrorismi ja selle rahastamise ohuga ning mitteregulatiivsed lahendused pole piisavad kuritegevus- ja julgeolekuriskide maandamiseks määral, mis võimaldaks Eestil vältida olulist kahju.

IV. Probleemi võimalikud regulatiivsed lahendused

8. Välisriigid, mille regulatiivseid valikuid probleemi lahendamiseks on analüüsitud või on kavas seaduseelnõu koostamisel analüüsida

Eesti oli esimene riik maailmas, kes lõi e-residentsuse programmi – oleme selles valdkonnas teerajaja. E-residentsust pakuvad või hakkavad pakkuma mitmed riigid, sealhulgas Aserbaidžaan, Brasiilia, Gruusia, Leedu, Lõuna-Aafrika Vabariik, Portugal ja Ukraina. Teiste riikide lahendusi ei ole põhjalikult analüüsitud. Tutvutud on Leedu e-residentsuse programmiga. Leedu hakkas e-residentsust pakkuma 2021. aastal ja teadaolevalt Leedus e-residentsuse andmist ei piirata.

Edasisi analüüse ei ole plaanis teha. Muudatuse väljatöötamisel lähtutakse riigi julgeoleku tagamise vajadustest.

9. Regulatiivsete võimaluste kirjeldus

Digi-ID väljaandmise, kehtivuse peatamise ja kehtetuks tunnistamise menetlus on reguleeritud ITDS-i §-s 20[7]. Paragrahvi tuleb täiendada, et võimaldada keelduda digi-ID taotluste vastuvõtmisest riskiriikide kodanikelt, arvestades alltoodud erisusi.

Kavandatava muudatuse kohaselt ei saa edaspidi digi-ID taotlust esitada RAB-i nimekirjas olevate riskiriikide kodanikud, kuid piirangut ei kohaldata:

- Türgi või Araabia Ühendemiraatide kodanikule (vt selgitust punktis 2);
- riskiriigi kodanikule, kes on elanud vähemalt kolm aastat Euroopa Liidu riigis või Ühendkuningriigis ja kellel on selle riigi kehtiv elamisluba. Isik peab digi-ID taotlemisel esitama PPA-le elukohajärgse riigi elamisloa andmed või elamisloakaardi koopia ja võtma digi-ID kättesaamisel kaasa nii kehtiva kodakondsusjärgse passi kui ka elamisloakaardi. Euroopa Liidu riikide vahel on toimivad koostöösuhted ja andmevahetusmudel, misläbi on Eestil võimalik nendest riikidest saada isiku kohta usaldusväärset lisainfot. Euroopa Liidus on kehtestatud ühtsed standardid elamisloakaartidele, mis võimaldab menetlejal selgelt tuvastada, kas isiku esitatud andmed ja dokument on õiguspärased. Samas kolmandates riikides on kasutusel erinevad elamisõigust tõendavad alusdokumendid, mille õigsuse tuvastamine ei pruugi olla võimalik;

- riskiriigi kodanikule, kes tegeleb Eestis majandustegevusega. Digi-ID-d võimaldatakse taotleda riskiriikide kodanikel, kes tõestatavalt tegelevad Eestis juba majandustegevusega, st need, kes on enne e-residendiks saamist Eestis ettevõtte asutanud või kellel on ettevõtlusseos Eesti ettevõttega, näiteks juhatuse liikmena. Erisust kohaldatakse juhul, kui ettevõte tegutseb aktiivselt ning selle kohustused Eesti riigi ees on täidetud ja puuduvad võlad. Ettevõttele, kellel on nullkäive ja kes ei maksa makse, erisust ei kohaldata. Eestil on majandustegevusega tegelevate riskiriikide kodanike ja nende tegevuse kohta lisainfot, mida on võimalik kontrollida;
- riskiriigi kodanikule kordustaotluse esitamisel. Kordustaotluse menetlemisel on võimalik hinnata e-residendi senist tegevust ja seda, kas ta täidab e-residentsuse programmi eesmärki, panustades Eesti majanduse, teaduse, hariduse või kultuuri arengusse. Erisust kohaldatakse juhul, kui e-resident tegeleb tõestatavalt Eestis majandustegevusega ning sellega kaasneb Eestile maksutulu, st nullkäibega ettevõttele erisust ei kohaldata;
- Eesti välisesinduse töötajale, aukonsulile ja Eesti riigiasutuse lepingupartneri, näiteks välise teenusepakkuja töötajale. Eestil on ka riskiriikides, näiteks Egiptuses, välisesindusi ja ei ole välistatud, et digi-ID-d vajavad saatkonna töötajad on selle riigi kodanikud. Ka aukonsul ja Eesti riigiasutuse lepingupartneri töötaja võivad olla riskiriikide kodanikud, kes vajavad oma tööülesannete täitmiseks digi-ID-d. Kõik sellised isikud läbivad põhjaliku taustakontrolli ja riskide ilmnemise korral saab digi-ID väljaandmisest keelduda.

10. Regulatiivsete võimaluste põhiseadusega ning Euroopa Liidu ja rahvusvahelise õigusega määratud raamid

Muudatuse tulemusel kaotavad riskiriikide kodanikud edaspidi võimaluse taotleda digi-ID-d ja seeläbi ka võimaluse kasutada Eesti e-teenuseid. Enamasti kasutatakse digi-ID-d äritegevuseks. Juhul, kui isik soovib ennast Eestiga siduda, saab ta selleks kasutada teisi võimalusi. Näiteks on võimalik luua ettevõte notari vahendusel. Seega on riskiriigi kodanikul endiselt võimalus alustada Eestis äritegevust sarnaselt ülejäänud kolmandate riikide kodanikega.

Eesti Vabariigi põhiseaduses ei ole e-residentsust reguleeritud. E-residentsus on reguleeritud ITDS-i 5^2. peatükis. Seega on e-residentsus hüve, mitte isiku põhiõigus. Mitte kellelgi ei ole subjektiivset õigust taotleda e-residentsuse saamiseks digi-ID-d ning riigil on pädevus otsustada, kellele ja mis tingimustel seda võimaldatakse. Digi-ID väljaandmisega annab Eesti riik välismaalasele õiguse siseneda riigi infoühiskonda ja kasutada Eesti e-teenuseid. Digi-ID on ajutine hüve, mille puhul võib eeldada, et olenevalt riigi ja rahvusvahelisest julgeolekuolukorrast ning välispoliitilistest eesmärkidest võivad selle andmise tingimused muutuda. Tuues paralleeli riigi territooriumil viibimisega, on riigil suveräänne õigus kontrollida, kui palju ja millistele tingimustele vastavaid välismaalasi ta oma territooriumile lubab. Sarnast põhimõtet on võimalik üle kanda tänapäevasele infoühiskonnale ja kohaldada e-riigi digikeskkonnale. Rahvusvahelises õiguses üldtunnustatud põhimõtte kohaselt ja arvestades riigina endale võetud rahvusvahelisi kohustusi on igal riigil suveräänne õigus omada kontrolli hüvede üle, mida riik välismaalastele annab. Isikul, kes ei ole selle riigi kodanik, puudub õigus kasutada mittekodakondsusjärgse riigi e-teenuseid.

V. Regulatiivsete võimaluste mõjude eelanalüüs ja mõju olulisus

11. Kavandatavad muudatused ja nende mõjud

ITDS-i § 20^7 lisatakse alus, mis võimaldab keelduda digi-ID taotluse vastuvõtmisest riskiriigi kodanikult, arvestades VTK punktis 9 nimetatud erisusi.

Muudatust on võimalik paindlikult ja etapikaupa kohaldada ning see arvestab laiemalt Eesti riigi julgeolekut ning majanduslikke ja välispoliitilisi huve.

Muudatus ei mõjuta kehtiva digi-ID-ga riskiriikide kodanikke. Olemasolev digi-ID kehtib kuni kehtivusaja lõppemiseni või selle järelkontrollis kehtetuks tunnistamiseni. Digi-ID kehtivusaeg on viis aastat. Kui isiku digi-ID kaotab kehtivuse, võimaldatakse tal erisuse kohaselt edaspidi esitada kordustaotlus ja ta peab uuesti põhjendama digi-ID vajadust ning andma selgitusi enda ja oma kavatsuste kohta.

Piirangu alt jäävad välja Türgi ja Araabia Ühendemiraatide kodanikud. Türgi on NATO liikmesriigina Eestile oluline julgeolekupartner ning Araabia Ühendemiraadid on Eestile oluline piirkond riiklike ja ärisuhete loomisel ja edendamisel, et arendada Eesti eksporti. Araabia Ühendemiraadid olid 2020. aastal Eesti jaoks suuruselt 36. eksporditurg, kus Eesti, sealhulgas e-residentide ettevõtetel on suurepärased ärivõimalused, näiteks IT-sektoris.

Erandina on võimalik anda riskiriigi kodanikule digi-ID, kui ta on elanud vähemalt kolm aastat Euroopa Liidu liikmesriigis või Ühendkuningriigis ja tal on selle riigi kehtiv elamisluba. Statistika kohaselt on digi-ID taotlemisel märkinud oma elukohaks riskiriigist erineva riigi 23% riskiriigi e-residentidest, kelle hulgast *ca* 70% elavad Euroopa Liidus või Ühendkuningriigis ning ülejäänud 30% kolmandates riikides. Näiteks on 65% Iraani kodakondsusega e-residentidest märkinud oma elukohariigiks Iraani, 13% Türgi ja 7% Eesti.

Samuti on võimalik anda digi-ID riskiriigi kodanikule, kes tegeleb Eestis majandustegevusega. 8. veebruari 2023. aasta seisuga on kehtiva digi-ID-ga riskiriikide kodanikud loonud 2444 ettevõtet, mis moodustab 9% kõikidest e-residentide ettevõtetest, millest omakorda on maksumaksjaid, st käibega ettevõtjaid, *ca* 32%. Türgi kodakondsusega e-residentidel oli 1190 ettevõtet, mis moodustab 48% kõigist riskiriigi e-residentide ettevõtetest.

Sotsiaalne, sealhulgas demograafiline mõju

Sihtrühm: riskiriikide kodanikud, kellel on soov tulevikus taotleda digi-ID-d. 10. märtsi 2023. aasta seisuga on riskiriigi e-residente 6406. E-residente on kokku 100 219, kellest 63 332-l on kehtiv digi-ID. Tõenäoliselt ei suurene riskiriikide kodanike huvi e-residentsuse vastu ka tulevikus. Seega jääb riskiriigi e-residentide arv eeldatavasti samaks ja sihtrühma suurus on võrreldes e-residentide koguarvuga keskmine.

Mõju ulatus on väike, kuna digi-ID-ga ei kaasne sihtrühmale olulisi eeliseid: see ei anna kodakondsust, ei ole reisidokument ega viisa ega anna õigust Eestis viibida. Digi-ID-d saab kasutada vaid Eesti e-teenustes ja välisriigi kodanikul, kellel puudub seos Eestiga, ei ole digi-ID-d vaja. Seega puudub sihtrühmal kohanemisvajadus ja kohanemisraskusi ei teki.

Mõju esinemise sagedus on väike, sest sihtrühma kokkupuude muudatusega on ebaregulaarne ja juhuslik. Riskiriikide kodanikel, kellel puudub kokkupuude Eestiga, ei ole digi-ID-d igapäevaelus vaja.

Ebasoovitava mõju kaasnemise risk on väike. Muudatuse tulemusel kaotavad riskiriikide kodanikud edaspidi võimaluse taotleda digi-ID-d ja seeläbi ka võimaluse kasutada Eesti e-teenuseid. Enamasti kasutatakse digi-ID-d äritegevuseks ja juhul, kui isik soovib ennast Eestiga siduda, saab ta selleks kasutada teisi võimalusi, näiteks on võimalik luua ettevõte notari vahendusel.

Seega on muudatusel sihtrühmale väheoluline mõju.

Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele

Sihtrühm: PPA ametnikud, kes menetlevad e-residentsuse taotlusi. Neid on kaheksa. PPA-s töötab *ca* 5000 inimest. Seega on muudatuse sihtrühm väike.

Mõju ulatus ja esinemise sagedus on väikesed ja ei too kaasa sihtrühma töö ümberkorraldust ega ümberõppevajadust.

Ebasoovitava mõju kaasnemise risk on samuti väike. PPA ametnike töömaht ei suurene.

Seega on muudatusel sihtrühmale väheoluline mõju.

Mõju riigi julgeolekule ja välissuhetele

Sihtrühm: Eesti elanikud. 2023. aasta alguse seisuga elas Eestis 1 357 739 inimest.[8]

Muudatus avaldab olulist positiivset mõju Eesti riigi sisejulgeolekule ja -turvalisusele arvestades sh riigi majanduslikke ja välispoliitilisi huve.

Positiivse mõju saavutamiseks peab riik võtma tõhusaid meetmeid oma elanike turvatunde tagamiseks ning riskide maandamiseks. Riikide puhul, kellega Eestil puudub justiits-, julgeoleku- ja õiguskaitsealane koostöö, ei ole e-residentsusega kaanevate riskide maandamist võimalik tagada muul moel kui piirata digi-ID väljaandmist. Riskiriikide kodanikele e-residentsuse võimaldamine on vastuolus e-residentsuse eesmärgiga ning kahjustab Eesti julgeolekut ja välismainet.

Riskiriikide kodanikud võivad kasutada digi-ID-d erinevate küber- ja majanduskuritegude toime panemisel või kasutada e-residentsust hüppelaua ja abivahendina viisa või elamisloa saamisel.

E-residentsust on kasutatud immigratsiooniskeemides, misläbi on varjatud eesmärkidega isikutel lihtsam siseneda rändemenetlusse, mille tulemusena suurenevad julgeoleku ja migratsiooniga seotud riskid. Näiteks taotlevad Iraani e-residendid paljudel juhtudel ka Eestis viibimise aluseid. Iraani avalike allikate põhjal[9] annab Eesti e-residentsus võimaluse Euroopa Liitu sisenemiseks ja rahvusvahelise äri tegemiseks, kuna lihtsustab viibimisaluste saamist

[8] Statistikaamet. Rahvaarv.
[9] Iraani avalikud allikad e-residentsuse kohta

Eestis ja Euroopa Liidus. PPA statistika kohaselt omavad või on omanud näiteks 15% Iraani e-residentidest lisaks e-residentsusele muid staatusi (näiteks elamisluba), mis teeb neist enim teisi staatusi omavad riskiriikide e-residendid.

Tabel 2. Iraani e-residentide taotlused 2014-2022. a

Kodakondsus	2014	2015	2016	2017	2018	2019	2020	2021	2022	Kokku
Iraan	1	25	59	82	213	189	129	161	116	975

Allikas: PPA

Muudatusega maandame riskiriikide kodanike kogukondade suurenemisest tulenevaid julgeolekut ja turvalisust ohustavaid tegureid. Nendeks on vaenulik mõjutustegevus, terrorism, radikaliseerumine, mõju raskele ja organiseeritud kuritegevusele, sh eriti majanduskuritegudele, korruptsioonile, rahapesule ja terrorismi rahastamisele, küberkuritegevusele ning sellega kaasnevatele ühiskondlikele tagajärgedele. Muudatuse rakendamine aitab ennetada võimalike süütegude toimepanemist mõjudes ühtlasi positiivselt elanike turvatundele ja elukeskkonna turvalisusele.

Piirangu alt jäetakse välja Türgi ja Araabia Ühendemiraatide kodanikud, sest Türgi on NATO liikmesriigina Eestile oluline julgeolekupartner ning Araabia Ühendemiraadid oluline piirkond riiklike ja ärisuhete loomisel ja edendamisel, et arendada Eesti eksporti. Araabia Ühendemiraadid olid 2020. aastal Eesti jaoks suuruselt 36. eksporditurg, kus Eesti, sealhulgas e-residentide ettevõtetel on suurepärased ärivõimalused, näiteks IT-sektoris.

Muudatus avaldab olulist positiivset mõju Eesti riigi sisejulgeolekule ja -turvalisusele, kuigi mõju ulatus, esinemise sagedus ja ebasoovitava mõju kaasnemise risk on sihtrümale väikesed. Muudatus ei mõjuta Eesti elanike igapäevast elukorraldust, elanike senist toimimist ega eelda sihtrühma sihiteadlikku ümberkohanemist. Samuti on sihtrühma kokkupuude muudatusega ebaregulaarne ja juhuslik. Ebasoovitav mõju, selle ulatus ja esinemise sagedus Eesti elanike elukorraldusele ja turvalisusele suureneks muudatuse kohaldamata jätmisega.

Seega on muudatusel sihtrühmale oluline mõju.

Mõju majandusele

Sihtrühm: Eesti elanikud. 2023. aasta alguse seisuga elas Eestis 1 357 739 inimest.[10]

Muudatus avaldab olulist positiivset mõju Eesti majandusele. Ühe suurima e-residentsuse programmi riskina toodi Moneyval´i hindamisaruandes välja, et e-residentsuse programm võimaldab välismaalastel kasutada e-residentsust ebasoovitavaks ettevõtluseks ning varjata ettevõtluse tegelikku sisu ja eesmärki ning sellest kasu saajaid ning eriti probleemne on see riskiriikide puhul. Moneyval´i hindamise tulemusena võib hinnatav riik sattuda ebausaldusväärsete riikide nimekirja (hall ja must nimekiri) ning see toob kaasa ulatusliku mõju Eesti kodanikele ja ettevõtetele, sest selles nimekirjas olevate ettevõtete ja eraisikute suhtes tuleb kõikidel välispankadel ja ka teistel asutustel rakendada täiendavaid ettevaatusabinõusid. Eestis tegutsevad rahvusvahelised ettevõtted viiksid suure tõenäosusega oma ettevõtted mujale ja Eesti ettevõtetel ning eraisikutel oleks pangakonto avamine keerulisem ning tõuseks laenuraha ehk intressi suurus. Ka üleüldine asjaajamine ning arveldamine oleks meie

[10] Sealsamas.

ettevõtetega raskem, kuna maksed peaksid läbima tihedama sõela võrreldes valges nimekirjas olevate riikide ettevõtetega. Ettevõtted peaksid täpsemalt tõestama raha päritolu ja kinnitama, et tegemist pole teeseldud tehingutega.

Riskiriigi e-residentide ettevõtete statistika:
8. veebruari 2023. aasta seisuga on kehtiva digi-ID-ega riskiriigi e-residendid loonud kokku 2444 ettevõtet, mis moodustab 9% kõigist e-residentide ettevõtetest. Nendest 1190 ettevõtet on loonud Türgi kodanikud, s.o 48% kõigist riskiriikide kodanike ettevõtetest. Kavandatava muudatuse kohaselt kehtib Türgi kohta erisus, st Türgi kodanikele piirangut ei kohaldata. Türgis on riskiriikidest kõige rohkem aktiivseid e-residente: 44% riskiriigi e-residentidest. Samuti on Türgi kodakondsusega e-residentidel riskiriikidest enim ettevõtteid, mis on alustanud reaalset majandustegevust. Kõikide riskiriigi e-residentide ettevõtete tasutud maksudest moodustavad Türgi kodanike ettevõtete riiklikud maksud *ca* 96% ja tööjõumaksud 90%.

Tabel 3. Riskiriigi e-residentide ettevõtete arv

Türgi	1316
Iraan	311
Egiptus	195
Pakistan	184
Tuneesia	125
Maroko	112
Liibanon	70
Nigeeria	63
Alžeeria	54
Süüria	46
Jordaania	43
Usbekistan	34
Sudaan	17
Liibüa	16
Iraak	15
Jeemen	12
Saudi Araabia	11
Palestiina Omavalitsus	10
Kongo DV	7
Afganistan	7
Mali	4
Burkina Faso	4
Somaalia	1
Mosambiik	1
Põhja-Korea	1
Araabia Ühendemiraadid	1

Allikas: Ettevõtluse ja Innovatsiooni Sihtasutus

2022. aasta I poolaastal deklareeris käibe või maksud 374 riskiriigi e-residendi ettevõtet. Neist 337 deklareeris käibe ja 78 maksud. Ettevõtete deklareeritud käive oli 63,3 miljonit eurot. Sellest 14% ehk 8,6 miljonit eurot moodustas selliste ettevõtete käive, millega seotud e-resident ei elanud riskiriigis. 2022. aasta I poolaastal tasusid riskiriigi e-residendid maksudena kokku

281 000 eurot, millest 30% ehk 85 000 eurot tasusid riskiriigi e-residendid, kes elavad väljaspool riskiriiki. See teeb 1,2% kõigist e-residentide ettevõtete makstud tööjõumaksudest.

Eeltoodu põhjal on muudatuse mõju ulatus ja esinemise sagedus suur.
Ebasoovitava mõjuna võib kaasneda tulu vähenemine Eesti majandusele, mis e-residentide ettevõtetest Eesti riigile laekub. Samas, kui riskiriigi kodanik soovib end Eestiga siduda ja siin ettevõtte luua, jääb talle nagu kõikidele mitteresidentidele alles võimalus luua ettevõte notari vahendusel. Seega on ebasoovitava mõju kaasnemise risk väike.

Kokkuvõtvalt on muudatusel sihtrühmale oluline positiivne mõju.

12. Muudatuste koondmõju ettevõtete ja/või kodanike halduskoormusele

Muudatusega ei kaasne mõju ettevõtjate ja kodanike halduskoormusele.

13. Muudatuste rakendamisega seotud riigi ja kohaliku omavalitsuse eeldatavad kulud ja tulud

Muudatus toob kaasa digi-ID taotlemise keskkonna arendamise kulud, mis kaetakse Siseministeeriumi infotehnoloogia- ja arenduskeskuse eelarvest.

14. Edasine mõjude analüüs

E-residentsus on hüve, mitte isiku põhiõigus, ja mitte kellelgi ei ole subjektiivset õigust e-residentsuse saamiseks ning riigil on pädevus otsustada, kellele ja mis tingimustel hüve pakutakse, ei ole edasine mõjuanalüüs HÕNTE § 46 kohaselt vajalik.

VI. Kavandatav õiguslik regulatsioon ja selle väljatöötamise tegevuskava

15. Valitav lahendus			
ITDS-i §-s 20[7] sätestatakse alus, mis võimaldab keelduda riskiriigi kodanikult digi-ID taotluse vastuvõtmisest. Erisused ja piirangu alla kuuluvate riikide nimekiri kehtestatakse siseministri määrusega.			
15.1. Töötatakse välja uus tervikseadus		**15.2. Muudatused tehakse senise seaduse struktuuris**	X
15.3. Selgitus	Muudatus ei ole nii mahukas, et eeldaks ITDS-i uue tervikteksti väljatöötamist. Seetõttu muudetakse olemasolevat seadust.		
16. Puudutatud ja muudetavad õigusaktid			
ITDS			
17. Edasine kaasamise plaan – keda, millal ja kuidas kaasatakse			
VTK ja seejärel seaduseelnõu esitatakse eelnõude infosüsteemi kaudu kooskõlastamiseks Justiitsministeeriumile, Kaitseministeeriumile, Majandus- ja Kommunikatsiooniministeeriumile, Rahandusministeeriumile ja Välisministeeriumile ning arvamuse avaldamiseks Ettevõtluse ja Innovatsiooni Sihtasutusele, PPA-le, Kaitsepolitseiametile, Siseministeeriumi infotehnoloogia- ja arenduskeskusele, Maksu- ja Tolliametile, RAB-ile ja Andmekaitse Inspektsioonile.			
18. Põhjaliku mõjuanalüüsi toimumise aeg			
Põhjalikku mõjuanalüüsi ei ole plaanis koostada.			

19. Eeldatav kontseptsiooni (HÕNTE § 1 lg 3) valmimise ja kooskõlastamisele saatmise aeg (kui järgmise sammuna koostatakse eelnõu kontseptsioon)	Kontseptsiooni koostamist ei kavandata.
20. Eeldatav eelnõu avaliku konsultatsiooni ja kooskõlastamise aeg	2023
21. Õigusakti eeldatav jõustumise aeg	2024
22. Vastutavate ametnike nimed ja kontaktandmed	Elen Kraavik, Siseministeeriumi piirivalve- ja rändepoliitika osakonna nõunik, elen.kraavik@siseministeerium.ee