
4.3. E-residentsuse programmi seonduvate riskide analüüs

4.3.1. E-residentsus

E-residentsus pakub välisriigi kodanikele turvalist ligipääsu Eesti riigi e-teenustele. E-residendi digi-ID-kaardi omanik saab dokumente digitaalselt allkirjastada ja logida sisse kõikidesse portaalidesse ja infosüsteemidesse, mis tunnistavad Eesti ID-kaarti. E-residendi digi-ID ei ole füüsiline isikut tõendav või reisidokument ja sellel ei ole fotot. E-residentsus ei anna kodakondsust, maksuresidentsust, elamisluba ja Eestisse või Euroopa Liitu sisenemise luba. E-residendi digitaalse isikutunnistuse väljaandmisest keeldumise alused on olnud samad, mis viisa või tähtajalise elamisloa andmisest keeldumise alused ja sissesõidukeelu kohaldamise alused. Lisaks tuleb arvestada, et ühelgi isikul ei ole subjektiivset õigust e-residentsust saada, sest see on hüve, mida Eesti riik saab usaldusväärsetele isikutele pakkuda. Siiski on täheldatud kolmandate riikide kodanike poolt e-residentsuse ärakasutamist ühe osana immigratsiooniskeemides, püüdes migrante selle läbi elamisloa- või viisamenetluses usaldusväärsemana näidata.

Eesti on esimene ja seni ainus riik maailmas, mis pakub e-residentsust. Sarnased programmid on väljatöötamisel ka Leedus, Ukrainas ja Portugalis. Alates 2014. aasta detsembrist annab e-residendi digi-ID välismaalasele võimaluse ajada asju digitaalselt ja asukohast sõltumata. Nii on näiteks väljast poolt Euroopa Liitu pärit inimesel võimalik luua omale baaskeskus Euroopa Liidus asjaajamiseks – tal on võimalik asutada äriühing Eestis ning osaleda aktiivselt selle juhtimises, elades ise näiteks Indias või Ameerika Ühendriikides. E-residentsus sobib suurepäraselt ka Eestisse juba investeerinud ja ettevõtte loonud ettevõtjatele nt. soomlastele, kes haldavad oma siinseid ettevõtteid interneti teel.

Eesti e-residendid võivad lisaks ettevõtte asutamisele kaugjuhtida ettevõtet ning digitaalselt allkirjastada dokumente ja lepinguid, esitada elektrooniliselt tuludeklaratsiooni, saada ligipääsu rahvusvahelistele makseteenuste pakkujatele ning teha e-panganduse tehinguid, kui neil on Eestis avatud pangakonto. E-residentsusega ei kaasne pangakontot ega õigust sellele, vaid pangakonto saamiseks tuleb läbida eraldi menetlus, mille käigus hinnatakse isiku ja tema rahaliste vahendite päritolu usaldusväärsust. Samas on juhtumeid, mil e-resident omandab riuliettevõtte koos olemasoleva pangakontoga, saades selliselt juhatuse liikmena lihtsamini juurdepääsu finantsteenustele.

Kokkuvõte:

E-residentsus võimaldab välismaalastel kasutada Eestit ebasoovitavaks ettevõtluseks, mis võimaldab varjata ettevõtte tegevuse tegelikku sisu ja eesmärki ning sellest kasuajajaid. Eriti probleemne on see kolmandate riikide osas, millistega Eestil pole justits-, julgeoleku- ega õiguskaitsealaseid koostöösuhteid, mis tähendab, et Eestil pole võimalik nimetatud riikidest pärit taotlejate kohta usaldusväärset teavet saada ega hiljem vajadusel nende toime pandud süütegusid efektiivselt menetleda.

4.3.2. E-residentsuse programmiga seonduvad riskid ning nende ennetamine ja tõkestamine

Suur hulk avalik-õiguslikke ja eraõiguslikke teenuseid olid potentsiaalsetele e-residentidele kättesaadavad ka enne programmi käivitamist eraõiguslike isikutuvastusvahendite, nt pangalinkide kaudu. Kuivõrd mis tahes eraõiguslikud isikutuvastusmeetmed on isikutuvastamise tõsikindluse aspektist vähem turvalised kui riigi välja antud isikut tõendavad dokumendid, tagas e-residentsuse kasutuselevõtt, et seos toiminguga ja selle sooritanud isiku vahel tuvastatakse oluliselt tõsikindlamalt.

Samas on võimalik, et e-residentsuse programmi loomisel ei teadvustatud piisavalt pädevate asutuste koostatud riskihinnanguid. Eriti probleemne on isikutuvastamise tõsikindluse tagamine isikute puhul, kes on pärit riikidest, millega Eestil puuduvad justits-, julgeoleku- ja õiguskaitsealased koostöösuhted. Samuti pole võimalik selliste riikide kodanike tausta efektiivselt kontrollida ega vajadusel hiljem nende toime pandud süütegusid menetleda.

E-residentsusega loodud võimalus tegutseda ettevõtjana võib oluliselt raskendada süütegude uurimist, kuna nt maksupettuse või kelmuse toime pannud isiku tabamisel ja menetlustoimingute läbiviimisel võib olla oluliseks probleemiks tema alaline elamine välisriigis. Seetõttu võivad venida või ebaõnnestuda õigusrikkumiste uurimine, tõendite kogumine, kohtumenetlus, pankrotimenetlus jne.

E-residentsuse programmiga seonduvate riskide maandamise üheks peamiseks eelduseks on asjaolu, et riik teab, kes on Eesti e-residendid ja kellele ta on usaldanud Eesti digitaalse identiteedi. Andes välismaalasele Eesti Vabariigi digitaalse isikutunnistuse, tuvastab Politsei- ja Piirivalveamet välismaalase isiku tema kodakondsusjärgse riigi isikut tõendava dokumendi järgi, mille välismaalane esitab. Isiku tuvastamise ja taustakontrolli juures on oluline arvestada asjaoluga, et isiku tegeliku tausta osas võivad esineda olulised puudujäägid, kui isik on pärit riigist, millega Eestil ei ole justiits-, julgeoleku- ja õiguskaitsealast koostööd. Olemuslikult ei ole riik tuvastanud isikut suuremal määral, kui viisa või elamisloa menetluses. Identiteedi väärkasutamise riski suurendab e-residentsuse taotlejate tuvastamine Eesti saatkondade asemel väliste teenusepakkujate poolt, kellele riik delegeerib isiku tuvastamise ja biomeetria hõivamise ülesande.

E-residendi digi-ID on riigi väljaantav isiku digitaalset identiteeti tõendav dokument, millega ei kaasne suuremad riigi garantiid väljastatud dokumendi kasutamisele kui riigi mis tahes muu väljaantava isikut tõendava dokumendiga. Eesti kui dokumendi väljaandja võtab isiku identiteedi kindlaksmääramisel aluseks tema kodakondsusjärgse riigi väljaantud ja Eesti Vabariigi tunnustatud isikut tõendava dokumendi ning annab selle alusel isikule Eesti isiku digitaalset identiteeti tõendava dokumendi. Riiklik garantii seisneb seega selles, et digi-ID väljastatakse selleks õigust omavale ja tuvastatud isikule, kontrollides võimaluste piires, et dokument pole võltsitud ja dokumendi esitaja on sama isik, kellele dokument on väljastatud. Lisaks on riigil võimalus e-residendi digi-ID sertifikaadi kasutamisevõimalus kohe peatada kui kahtlustatakse väärkasutust – selline võimalus on oluline väärkasutuse ennetamiseks ja tõkestamiseks, kuid see eeldab piisavat ressursi. E-residentsuse programmi laienedes suureneb vastavalt ka ressursivajadus. Kuna isiku digitaalse allkirjaga või autentimise lahendused on kasutusel ka väljaspool Eestit, sõltub sertifikaadi peatamine väärkasutamise juhtumi andmete edastamisest Politsei- ja Piirivalveametile. Välisriikides toime pandud süütegude tuvastamine sõltub välisriigi poolsest võimekusest rikkumisi tuvastada ja tahtest neist teavitada.

Dokumendi väärkasutus võib seisneda:

- 1) digi-ID-ga õigusrikkumiste toimepanemises, sealhulgas kelmused, maksupettused, finantskuriteod, rahapesu ja organiseeritud kuritegevus või terrorismi rahastamine, või
- 2) digi-ID teisele isikule kasutada andmises.

Käesolevaks ajaks on osa riske ka realiseerunud.

E-residentsus ise väärkasutuse riski ei põhjusta, aga võib õigusrikkumise toimepanemise muuta lihtsamaks ja odavamaks – seega atraktiivsemaks.

Riskide maandamiseks e-residentide usaldusväarsuse tagamiseks ja dokumendi õiguspärase kasutamise üle järelevalve teostamiseks on ette nähtud järgmised tegevused:

- e-residendile digi-ID väljastamisel teostatakse võimaluste piires (põhjaliku taustakontrolli tegemiseks pole riigil ressursi ega kohapealset informatsiooni, taotleja elukohajärgsel riigil ei tarvitse olla motivatsiooni või õiguslikku alust taotlejale taustakontrolli teha) isikute usaldusväarsuse taustakontrolli, kaasates asjassepuutuvaid asutusi ja tehes päringuid asjakohastesse Eesti ja Euroopa Liidu andmekogudesse haldusmenetluses võimaldatud ulatuses – kui on kahtlus isiku usaldusväarsuses, siis taotlejale digi-ID-d välja ei anta. Kuna tegu on haldusmenetlusega, ei ole võimalik kasutada rahvusvahelise koostöö meetmeid, mis on kasutusel kuriteo uurimisel. Justiits-, julgeoleku- ja õiguskaitsealaste koostöösuheteta kolmandate riikide osas poleks võimalik rahvusvahelise koostöö võimalusi kasutada ka juhul, kui see tööriist haldusmenetluses lubatud oleks;

- võimaldada e-residentsust vaid riikides, millega Eestil on olemas justiits- julgeoleku- ja õiguskaitsealased koostöösuhted ning laiendada e-residentsust vastavasse riiki alles peale koostöösuhte loomist;
- teenuseosutajad peavad vajadusel seirama digi-ID kasutamist, et leida väärkasutusmustreid ja kõrvalekaldeid – selleks on e-residendid infosüsteemides sertifikaatides sisalduvate tunnuste alusel eristatavad ning lisaks tehakse teenusepakkujate seas põhjalikku teavitustööd, mille sihtgrupiks on eeskätt kriitiliste teenuste ja e-residentide jaoks huvipakkuvaimate teenuste pakkujad;
- Riigi Infosüsteemi Ameti poolt pakutakse digiteenuste osutajatele info- ja eksperttuge teenuste seire arendamisel ja läbiviimisel;
- digi-ID väärkasutuse või selle omaniku valdusest väljumise kahtlustuse või vastava teate põhjal PPA dokumendi väljaandjana uurib juhtumit ja tal on õigus peatada koheselt e-residentsus, seega sertifikaatide kehtivus ja sellega kõigi digiteenuste kasutusõigus;
- väärkasutuse ilmnemisel on riigil võimalik digi-ID kasutamine kui hüve lõpetada, tunnistades dokumendi kehtetuks.

E-residentsuse programmi kasvades ja muutudes on vaja arvestada üha kiiremini muutuvat keskkonda, hinnata järjepidevalt riske, kavandada asjakohaseid maandamismeetmeid ja suurendada selleks vastavat ressursi. Ilma piisava ressursita ei ole võimalik ennetada ja tõkestada e-residentsuse väärkasutust ega maandada sellest tulenevaid riske. Erinevate osapoolte koostöös on eraldiseisvalt valminud e-residentsuse riskianalüüs (tunnistatud asutusesiseseks kasutamiseks mõeldud teabeks), kus on kajastatud e-residentsusega seonduvad riskid, maandamismeetmed ning vastutajad. Vastavate maandamismeetmete kaardistus ja meetmete rakendamine toimub Siseministeeriumi eestvedamisel ning e-residentsuse nõukogu hindab ja kinnitab maandamistegevusi perioodiliselt.

4.3.3. Statistika

E-residentide koguarv on 31.12.2020 seisuga 76 070, neist 13% olid naised ja 87% olid mehed. TOP 5 kodakondsused on Soome, Venemaa, Ukraina, Saksamaa, Hiina.

Tabel 19. E-residendi digi-ID välja andmise otsused 2014-2020

	Staatus antud kokku	Top 5 riigid
2014	114	1. Soome 2. Venemaa 3. USA 4. Läti 5. Leedu
2015	7127	1. Soome 2. Venemaa 3. USA 4. Itaalia 5. Ukraina
2016	7495	1. Soome 2. Suurbritannia 3. Venemaa 4. USA 5. Ukraina
2017	13 436	1. Ukraina 2. Soome 3. Saksamaa 4. Suurbritannia

		5. Venemaa
2018	22 367	1. Jaapan 2. Venemaa 3. Hiina 4. Ukraina 5. Saksamaa
2019	16 630	1. Venemaa 2. Saksamaa 3. Ukraina 3. India 4. Hiina
2020	12 955	1. Venemaa 2. Saksamaa 3. Hiina 4. Ukraina 5. Hispaania

Allikas: Politsei- ja Piirivalveamet

Alates 2016. aastast on kehtetuks tunnistatud 90 e-residendi digi-ID-d.

29.02.2021 seisuga oli EAS andmetel registreeritud 15 907 e-residentide asutatud ettevõtet. Arvestuses ei ole eristatud e-residente kodakondsuse järgi.