

Isikut tõendavate dokumentide seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri

1. Sissejuhatus

1.1. Sisukokkuvõte

Isikut tõendavate dokumentide seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu (edaspidi *eelnõu*) on töötatud välja, et **suurendada identiteedi-halduse turvalisust ja ajakohastada tööprotsesse**, viies need vastavusse tänapäevaste vajaduste ja võimalustega. Selleks on kavandatud teha järgmised olulisemad muudatused.

- 1) **Luuakse õiguslik alus tagastada läbi vaatamata e-residendi digitaalse isikutunnistuse** (edaspidi *e-residendi digi-ID*) **taotlus** juhul, kui e-residendi digi-ID taotleja on kõrgema rahapesu- või terrorismi rahastamise riskiga riigi või sellise riigi kodanik, millega puudub Eestil justitiis-, julgeoleku- või õiguskaitsealane koostöösuhe (edaspidi *riskiriik*).
- 2) **Antakse Ettevõtluse ja Innovatsiooni Sihtasutusele** (edaspidi *EIS*) **õigus töödelda** e-residendi digi-ID väljaandmise menetluses kogutud **isikuandmeid** ja e-residendi digi-ID andmeid.
- 3) **Antakse Politsei- ja Piirivalveametile** (edaspidi *PPA*) **õigus nõuda DNA-ekspertiisi** juhul, kui isik taotleb esimest korda Eesti kodaniku isikut tõendavat dokumenti ja tekib põhjendatud kahtlus, et välisriigis väljaantud Eesti kodakondsuse õigust tõendav dokument ei ole ehtne või selle alusandmed ei ole õiged. Praktikas on saagenenud olukorrad, kus Venemaa või Valgevene kodanik soovib hilisema isaduse tuvastamisega tõendada, et ta põlvneb Eesti kodanikust, kuid esitatud tõendites või andmetes on põhjust kahelda.
- 4) **Ajakohastatakse isikut tõendava dokumendi** (edaspidi *dokument*) **väljaandmist**: luuakse dokumendi taotlejale erinevaid võimalusi, tõhustatakse menetlust ja vähendatakse bürokraatiat. Näiteks võimaldatakse Eesti kodanikul valida kohustusliku dokumendina isikutunnistuse asemel ka passi ja luuakse võimalus volitada esindajat dokumenti kätte saama ka pärast dokumendi väljaandmise taotluse (edaspidi *dokumendi taotlus*) esitamist.
- 5) Luuakse võimalus **kontrollida isikusamasust mobiilirakenduse** (edaspidi *mRiik*) **kaudu**.
- 6) 1. novembrist 2025 kaotatakse:
 - turvalisuse kaalutlustel **võimalus dokumendi sertifikaadi** (edaspidi *sertifikaat*) **kehtivust peatada ja taastada**, kuna hakatakse rakendama uut ID-1 formaadis dokumentide¹ tootmise lepingut, ning
 - vähese vajaduse ja kulude optimeerimise tõttu **võimalus anda välja ID-1 formaadis teiseid digitaalseid isikutunnistusi**.
- 7) **Tuuakse põhimäärusest seaduse tasandile** automaatse biomeetrilise isikutuvastuse süsteemi andmekogu (edaspidi *ABIS*), Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu, Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu, isikut tõendavate dokumentide andmekogu (edaspidi *ITDAK*) ning sissesõidu-keeldude riikliku registri **andmete säilitamise maksimaalne tähtaeg ja andmekoosseis**.

¹ ID-1 formaadis dokumendid on isikutunnistus, elamisloakaart ja digitaalne isikutunnistus.

Et tuua ABIS-e andmete säilitamise maksimaalne tähtaeg seaduse tasandile, muudetakse lisaks ITDS-ile seitset seadust.

Eelnõu rakendamisega kaasneb **oluline positiivne mõju riigi julgeolekule, siseturvalisusele, välissuhetele ja majandusele**. Mõju riigiasutuste korraldusele, e-riigile ja infoühiskonnale ning sotsiaalne mõju on väheolulised.

1.2. Eelnõu ettevalmistajad

Eelnõu ja seletuskirja on koostanud Siseministeeriumi:

- nõunik Elen Kraavik (elen.kraavik@siseministeerium.ee);
- õigusnõunik Maret Saanküll (maret.saankyll@siseministeerium.ee);
- õigusnõunik Kaspar Lepper (kaspar.lepper@siseministeerium.ee) – politsei ja piirivalve seaduse (edaspidi *PPVS*) muudatused.

Eelnõu väljatöötamise olid kaasatud Majandus- ja Kommunikatsiooniministeerium (edaspidi *MKM*), EIS, Kaitsepolitseiamet (edaspidi *KAPO*), PPA ja Rahapesu Andmebüroo (edaspidi *RAB*).

Eelnõu ja seletuskirja juriidilist kvaliteeti on kontrollinud Siseministeeriumi õigusosakonna õigusnõunikud Gerly Herm (tel 612 5230, gerly.herm@siseministeerium.ee) ja Kertu Nurmsalu (tel 612 5084, kertu.nurmsalu@siseministeerium.ee).

Eelnõu ja seletuskirja on keeleliselt toimetanud Siseministeeriumi õigusosakonna keeletoimetaja Heike Olmre (tel 612 5241, heike.olmre@siseministeerium.ee).

1.3. Märkused

Eelnõu ei ole seotud muu menetluses oleva eelnõuga ega Euroopa Liidu õiguse rakendamise ga. Eelnõu § 9 punktidega 1 ja 2 täpsustatakse õiguselguse huvides vaid juba Eesti õigusesse üle võetud tagasisaatmisdirektiivi² rakendamise regulatsiooni VSS-is,

Eelnõu § 1 punkt 43, millega võimaldatakse kontrollida isikusamasust mRiigi kaudu, on seotud **Vabariigi Valitsuse tegevusprogrammi 2023–2027**³ eesmärgiga 3.2.4 „Loomes e-riigi mobiilirakenduse, mille kaudu riik jõuab informatsiooni ja teenustega personaalselt iga eestimaalaseeni“.

Eelnõuga muudetakse järgmisi seadusi:

- 1) ITDS – RT I, 06.07.2023, 35;
- 2) kodakondsuse seadus (edaspidi *KodS*) – RT I, 06.07.2023, 44;
- 3) konsulaarseadus (edaspidi *KonS*) – RT I, 20.06.2022, 58;
- 4) kriminaalmenetluse seadustik (edaspidi *KrMS*) – RT I, 06.07.2023, 50;
- 5) PPVS – RT I, 06.07.2023, 64;
- 6) riigilõivuseadus (edaspidi *RLS*) – RT I, 06.07.2023, 83;
- 7) vangistuseseadus (edaspidi *VangS*) – RT I, 06.07.2023, 115;
- 8) välismaalasele rahvusvahelise kaitse andmise seadus (edaspidi *VRKS*) – RT I, 06.07.2023, 119;

² Euroopa Parlamendi ja nõukogu 16. detsembri 2008. aasta direktiiv 2008/115/EÜ ühiste nõuete ja korra kohta liikmesriikides ebaseaduslikult viibivate kolmandate riikide kodanike tagasisaatmisel. – [ELT L 348, 24.12.2008, lk 98–107](#).

³ Vabariigi Valitsuse 18. mai 2023. aasta korralduse nr 131 „Vabariigi Valitsuse tegevusprogrammi 2023–2027“ kinnitamine“ [lisa](#).

- 9) väljasõidukohustuse ja sissesõidukeelu seadus (edaspidi *VSS*) – RT I, 06.07.2023, 126;
10) väärtemenetluse seadustik (edaspidi *VTMS*) – RT I, 06.07.2023, 127.

Eelnõu on seotud:

- **siseturvalisuse arengukava 2020–2030**⁴ alaeesmärgiga 4.4 „Eesti arengut toetav kodakondsus-, rände- ja identiteedihalduspoliitika“, mille kohaselt on vaja arendada ja viia ellu usaldusväärset ja turvalist identiteedihalduspoliitikat ning tagada tõsikindel isikutuvastus;
- **eID valge raamatu**⁵ eesmärkide ja põhimõtetega, sealhulgas sellega, et Eesti on innovaatiline ja uuenduslik tugeva e-riigi mainega riik, kus katsetatakse uusi lahendusi ja tehnoloogiat;
- **e-residentsuse jätkustrateegiaga 2022–2025**⁶, milles on toodud ühe riskimaandusviisi na välja, et e-residentsust ei pakuta üldjuhul nende riikide kodanikele, millest tuleneb ulatuslik julgeoleku- või e-residendi digi-ID väärkasutuse oht, ja et e-residendina on eriti eelistatud taotlejad riikidest, millega on Eestil justüits-, julgeoleku- või õiguskaitsealane koostöö.

Eelnõu vastuvõtmiseks on vaja Eesti Vabariigi põhiseaduse § 104 lõike 2 punktide 1 ja 14 kohaselt **Riigikogu koosseisu häälteenamust**, sest muudetakse KodS-i ja KrMS-i.

2. Seaduse eesmärk

2.1. Eelnõu vajalikkus ja hetkeolukord

Siseturvalisuse arengukava 2020–2030 alaeesmärgi 4.4 „Eesti arengut toetav kodakondsus-, rände- ja identiteedihalduspoliitika“ kohaselt on muu hulgas vaja arendada ja viia ellu usaldusväärset ja turvalist identiteedihalduspoliitikat ning tagada tõsikindel isikutuvastus.

Eesti on turvaliste digidokumentide väljaandmises ja kasutamises maailmas esikohal. Kuigi ka praegune süsteem toimib hästi, on valdkondlik areng ja muudatused vältimatult vajalikud, et seda positsiooni säilitada. Tuleb käia kaasas ühiskonna ootuste ning valdkondliku ja info- tehnoloogilise arenguga, ajakohastades õigusruumi ja tööprotsesse. Tugev identiteedihaldus on oluline alustala riigi julgeoleku ja avaliku korra tagamisel. Selleks on riigil riikliku identiteedi loomisel kohustus tõsikindlalt veenduda isiku isikusamasuses ja õiguses sellele identiteedile.

2.2. Eelnõu eesmärk ja kavandatud lahendused

Ühiskonna ootus saada mugavamaid teenuseid ja tehnoloogia kiire areng koosmõjus rangete rahvusvaheliste standardite ja keerulise julgeolekuolukorraga seavad riigile väljakutse, kuidas leida tasakaal rangete turvanõuete ja ühiskonna ootuste vahel. Sellest lähtudes on eelnõul **kaks peamist eesmärki**:

- 1) suurendada identiteedihalduse turvalisust;
- 2) ajakohastada identiteedihalduspoliitika valdkonna tööprotsesse, et viia need vastavusse tänapäevaste vajaduste ja võimalustega.

Ühelt poolt **tuuakse** identiteedihalduspoliitika valdkonda **innovaatilisust ja paindlikkust**. Näiteks ootab ühiskond vajaduspõhiseid muudatusi, mis võimaldaksid kontrollida isikusamasust mobiiltelefoniga. Teiselt poolt **edendatakse märgatavalt identiteedihalduspoliitika valdkonna riskihaldust**, võimaldades riigil rakendada julgeolekukaalutlustel tugevamaid

⁴ Siseministerium. [Siseturvalisuse arengukava 2020–2030](#).

⁵ Riigi Infosüsteemi Amet 2018. [Valge Raamat. Identiteedihaldus ja isikut tõendavad dokumendid 1.0](#).

⁶ Majandus- ja Kommunikatsiooniministerium. [E-residentsuse jätkustrateegia 2022–2025](#).

meetmeid, tagamaks, et riiklik staatus antakse vaid õiguskuulekale isikule, kellel on sellele õigus.

Lisaks täpsustatakse eelnõuga õigusselguse huvides tagasisaatmisdirektiivist tulenevat lahku-misettekirjutuse regulatsiooni ning korrastatakse ABIS-e ja teiste andmekogude regulatsiooni, et tagada ühetaoline lähenemine ja **vastavus isikuandmete kaitse üldmäärusele**⁷. Eelnõuga ei muudeta andmete töötlemise põhimõtteid.

2.3. Eelnõu väljatöötamise kavatsus

2.3.1. Siseministeeriumi väljatöötamiskavatsus

ITDS-i muutmise seaduse eelnõu väljatöötamise kavatsus⁸ riskiriigi kodaniku e-residendi digi-ID taotluse vastuvõtmisest keeldumise kohta oli eelnõude infosüsteemis kooskõlastamisel 24.05.2023–07.06.2023. Selle kooskõlastasid Justiitsministeerium (edaspidi *JUM*), Rahandusministeerium (edaspidi *RAM*) ja Välisministeerium (edaspidi *VÄM*) märkustega. Teised ministeeriumid kooskõlastuskirja ei esitanud. Arvamust avaldasid Andmekaitse Inspektsioon, KAPO, Maksu- ja Tolliamet, PPA, RAB ning Siseministeeriumi infotehnoloogia- ja arenduskeskus (edaspidi *SMIT*).

Seletuskirja koostamisel on arvestatud *JUM*-i ja *RAM*-i märkustega ning esitatud arvamustega. Lisatud on selgitusi riskiriigi kodanikele kehtestatavate piirangute kohta ja ajakohastatud statistikat.

→ **VÄM-i ettepanek jätta riskiriikide loetelust välja Saudi Araabia**

VÄM tegi ITDS-i muutmise seaduse eelnõu väljatöötamise kavatsuse kooskõlastamisel ettepaneku jätta riskiriikide seast välja Saudi Araabia põhjusel, et Saudi Araabia on Eesti äri-diplomaatia prioriteetne sihtriik, Saudi Araabia turul on suur potentsiaal ja riik on muutunud viimastel aastatel oluliselt avatumaks. Samuti ei ole VÄM-i sõnul otstarbekas tõmmata piire Pärsia lahe Araabia riikide koostöönõukogu liikmete⁹ vahel.

Ettepanekut kaaludes on Siseministeerium (edaspidi *SIM*) koos allasutuste ja RAB-iga jõudnud seisukohale, et julgeolekukaalutlustel **ei ole praegu võimalik teha Saudi Araabiale erandit**. See muudaks Eesti majanduskeskkonna terrorismi rahastamise suhtes haavatavaks. Saudi Araabia on jätkuvalt üks islamifundamentalismi keskmeid. See maailmavaade on omakorda alus julgeolekuohtlikule islamistlikule äärmusideoloogiale. Saudi Araabias valitsevad arusaamad inimõigustest ja isikuvabadustest ei ole kooskõlas demokraatlike lääneriikide arusaamadega. Saudi Araabia toimib endiselt usuäärmusluse koolituskeskusena, mille mõju Eestis võib erand soodustada. Saudi Araabia on riik, kes toetab mittedemokraatlikku ideoloogiat ja vaigistab kriitikat monarhia vastu muu hulgas terrorismivastase seadustiku alusel.¹⁰

⁷ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – [ELT L 119, 4.5.2016, lk 1–88](#).

⁸ Eelnõude infosüsteemi toimiku nr [23-0622](#).

⁹ Araabia Ühendemiraadid, Bahrein, Katar, Kuveit, Omaan ja Saudi Araabia.

¹⁰ Freedom House 2023. [Freedom in the World 2023 – Saudi Arabia](#); US Department of State 2022. [2022 Country Reports on Human Rights Practices: Saudi Arabia](#). Vt ka näiteks [Abdulrahman al-Sadhani juhtum](#), kus ta sai Twitteris tehtud satiirilise postituse tõttu 2021. aastal 20-aastase vanglakaristuse.

Seega ei saa inimõiguste kaitse puudulikkuse tõttu usaldada ka Saudi Araabia nende sõnul „üha edukamat“ tööd terrorismivastase võitluse nimel. Selle julmimaks näiteks võib pidada ajakirjaniku Jamal Khashoggi tapmist 2017. aastal¹¹. Samuti kuulub Saudi Araabia kõrgema terrorismi rahastamise riskiga riikide hulka. Saudi Araabia kodanike kohta kehtivad samad erisused nagu teiste riskiriikide kodanike kohta. Neile võimaldatakse taotleda e-residendi digi-ID-d juhul, kui nad tegelevad Eestis tõestatavalt majandustegevusega, elavad püsivalt Euroopa Liidus või Ühendkuningriigis või on Eesti välisesinduse töötajad või aukonsulid, või juhul, kui nad esitavad korduvtaotluse.

Türgi ja Araabia Ühendemiraatide kodanikele erandi võimaldamise oluline argument oli Eesti välisesinduse olemasolu nendes riikides. See on hea näitaja riikidevahelise toimiva koostöö kohta.

2.3.2. MKM-i väljatöötamiskavatsus

MKM-i ITDS-i muutmise seaduse eelnõu väljatöötamise kavatsus¹², milles kavandati anda EIS-ile õigus töödelda e-residendiga seotud andmeid, oli eelnõude infosüsteemis kooskõlastamisel 12.12.2022–10.01.2023. Selle kooskõlastasid märkustega JUM ning märkusteta RAM, SIM ja VÄM. Teised ministriumid kooskõlastuskirja ei esitanud. Arvamust avaldas Statistikaamet. Seletuskirja koostamisel on arvestatud JUM-i märkustega.

Nii SIM-i kui ka MKM-i väljatöötamiskavatsus esitati arvamuse avaldamiseks ka Riigikogule.

2.3.3. Andmekogude regulatsiooni korrastamine

Andmekogude regulatsiooni korrastamise kohta ei koostatud eelnõu väljatöötamise kavatsust. Vabariigi Valitsuse 22. detsembri 2011. aasta määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 1 lõike 2 punkti 5 kohaselt ei pea eelnõu väljatöötamise kavatsust koostama, kui eelnõu seadusena rakendamise eesmärgiga ei kaasne olulist õiguslikku muudatust ega muud olulist mõju.

Eelnõuga korrastatakse ABIS-e, Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu, Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu, ITDAK-i ning sissesõidukeeldude riikliku registri regulatsiooni, et see vastaks isikuandmete kaitse üldmäärusele, ning tagatakse regulatsiooni ühetaolisus. Eelnõuga ei muudeta andmete töötlemise põhimõtteid. Andmekogude andmekoosseis ja andmete säilitamise tähtsused on praegu sätestatud andmekogude põhimäärustes. Eelnõuga tuuakse regulatsioon määruse tasandilt seaduse tasandile. Sisulisi muudatusi andmekogude regulatsioonis eelnõuga ei tehta, mistõttu ei kaasne selle rakendamise eesmärgiga olulist õiguslikku muudatust ega muud olulist mõju.

2.3.4. Lahkumisettekirjutuse regulatsiooni korrastamine

Lahkumisettekirjutuse regulatsiooni korrastamise kohta ei koostatud eelnõu väljatöötamise kavatsust. Vabariigi Valitsuse 22. detsembri 2011. aasta määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 1 lõike 2 punkti 5 kohaselt ei pea eelnõu väljatöötamise kavatsust koostama, kui eelnõu seadusena rakendamise eesmärgiga ei kaasne olulist õiguslikku muudatust ega muud olulist mõju.

Eelnõuga korrastatakse lahkumisettekirjutuse regulatsiooni, et oleks üheselt arusaadav, et viibimisalusega Eestis viibivale välismaalasele tehakse lahkumisettekirjutus lahkumiseks VSS-i

¹¹ [Saudi Araabia tunnistas, et Khashoggi mõrvati](#) 2018. – ERR/BNS, 22. oktoober.

¹² Eelnõude infosüsteemi toimiku nr [22-1522](#).

§-s 17 nimetatud vastuvõtvasse riiki, ning kui see on kolmas riik, peab välismaalane lahkuma lisaks Eestile ka teistest Schengeni konventsiooni ja Euroopa Liidu liikmesriikidest.

Eelnõuga ei muudeta lahkumisettekirjutuse regulatsiooni põhimõtteid. Lahkumisettekirjutuses märgitakse ka praegu ära, millisesse riiki viibimisalusetas Eestis viibiv välismaalane peab lahkuma. Samuti on lahkumisettekirjutuses märgitud, et kui vastuvõttev riik on kolmas riik, peab välismaalane lahkuma lisaks Eestile ka teistest Schengeni konventsiooni ja Euroopa Liidu liikmesriikidest. Muudatusega viiakse regulatsioon kooskõlla praktika ja tagasisaatmis-direktiivi täpse sõnastusega.

3. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb üheteistkümnest paragrahvist. Eelnõu §-ga 1 muudetakse ITDS-i, §-ga 2 KodS-i, §-ga 3 KonS-i, §-ga 4 KrMS-i, §-ga 5 PPVS-i, §-ga 6 RLS-i, §-ga 7 VangS-i, §-ga 8 VRKS-i, §-ga 9 VSS-i ja §-ga 10 VTMS-i. Eelnõu §-s 11 sätestatakse seaduse jõustumise aeg.

Võrdlev analüüs on jagatud teema järgi **kuueks alapeatükiks**.

Võrdleva analüüsi sisukord

3. Eelnõu sisu ja võrdlev analüüs	6
3.1. E-residendi digi-ID väljaandmine	7
3.1.1. Haldusorgani õigus edastada isikuandmeid järelevalvemenetluses (§ 1 p-d 9 ja 12).....	7
3.1.2. PPA õigus edastada andmeid EIS-ile ja EIS-i õigus neid töödelda (§ 1 p 11)	7
3.1.3. E-residendi kohustus hoida oma kontaktandmed ajakohasena (§ 1 p 33)	10
3.1.4. RAB-i õigus töödelda e-residendi andmeid (§ 1 p-d 51 ja 52).....	10
3.1.5. Riskiriigi kodanikule e-residendi digi-ID väljaandmise piiramine (§ 1 p 48).....	11
3.1.6. E-residendi digi-ID taotlemine ainult PPA iseteeninduses ja isikliku ilmumise kohustus (§ 1 p-d 50 ja 54–57)	14
3.1.7. E-residendi digi-ID riigilõiv (§ 6 p-d 2 ja 3)	15
3.1.8. Viitemuudatus e-residendi digi-ID väljaandmise aluses (§ 1 p 47).....	16
3.2. Dokumendiliigid, dokumendikohustus ja isikusamasuse kontrollimine	16
3.2.1. Pass kohustusliku dokumendina (§ 1 p 3) ja koduteeninduse piirangu kaotamine (§ 1 p-d 15 ja 16)	16
3.2.2. Sertifikaadi kehtivuse peatamise ja taastamise lõpetamine (§ 1 p-d 2, 4, 10, 13, 27, 49 ja 53).....	18
3.2.3. Digitaalse isikutunnistuse väljaandmise lõpetamine (§ 1 p-d 13, 45 ja 46, § 3 p-d 3–5 ning § 6 p-d 1 ja 4).....	18
3.2.4. Uue dokumendi taotlemine andmete muutumise korral (§ 1 p 30)	19
3.2.5. Terminikasutuse ühtlustamine (§ 1 p 1) ning samaliigilise dokumendi esitamise ja surma korral dokumendi tagastamise nõude kaotamine (§ 1 p-d 28 ja 32).....	20
3.2.6. Dokumendi kontrollimine (§ 1 p-d 41 ja 42).....	21
3.2.7. mRiik (§ 1 p 43).....	21
3.2.8. Digitaalsete andmete kehtivusaeg (§ 1 p-d 44 ja 61).....	22
3.3. Dokumendi väljaandmise menetlus ja andmetöötlus	22
3.3.1. Isikunime dokumenti kandmine (§ 1 p-d 5 ja 6).....	22
3.3.2. Dokumendi taotleja DNA-ekspertiis (§ 1 p-d 7 ja 21)	22
3.3.3. Isikuandmete töötlemine teavituse saatmiseks (§ 1 p 8)	24
3.3.4. Dokumendi taotlemine vanglas (§ 1 p-d 14 ja 17–20)	24
3.3.5. Volitatud esindaja määramine dokumendi taotluse menetlemise ajal (§ 1 p 22)	25
3.3.6. Dokumendi väljastamine (§ 1 p-d 23–26 ja 58) ja väljaandja termin (§ 1 p-d 29 ja 31).....	25
3.3.7. Välismaalase passi väljaandmise alus (§ 1 p-d 59 ja 60).....	26

3.3.8. Isiku daktüloskopeerimine tagasipöördumisdokumendi taotlemise korral (§ 1 p-d 62–64)	27
3.4. Andmete töötlemine riiklikes andmekogudes	27
3.4.1. ITDAK-i andmekoosseis ja ITDAK-i andmete säilitamise tähtajad (§ 1 p-d 34–38)	27
3.4.2. ABIS-e andmete säilitamise tähtajad (§ 1 p-d 39 ja 40, § 2 p-d 7 ja 8, § 3 p-d 1 ja 2, §-d 4, 7 ja 8, § 9 p-d 13 ja 14 ning § 10)	28
3.4.3. Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu andmekoosseis ja andmete säilitamise tähtajad (§ 2 p-d 3–6)	30
3.4.4. Sissesõidukeeldude riikliku registri ning Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu andmekoosseis ja andmete säilitamise tähtajad (§ 9 p-d 5–7 ja 10–12)	30
3.4.5. Piirikontrolli andmekogu biomeetriliste andmete võrdlemine (§ 5 p 1)	31
3.4.6. Andmekogude regulatsiooni tehnilised muudatused (§ 2 p-d 1 ja 2, § 5 p-d 2–4 ning § 9 p-d 3, 4, 8 ja 9)	33
3.5. Lahkumisettekirjutus (§ 9 p-d 1 ja 2)	34
3.6. Seaduse jõustumine (§ 11)	34

3.1. E-residendi digi-ID väljaandmine

3.1.1. Haldusorgani õigus edastada isikuandmeid järelevalvemenetluses (§ 1 p-d 9 ja 12)

Eelnõu § 1 punktidega 9 ja 12 muudetakse ITDS-i § 9² lõikeid 8 ja 9, et lubada PPA-l e-residendi digi-ID kasutamise üle järelevalve menetluses:

- edastada isikuandmeid kolmandatele isikutele (lg 8) ja
- koguda andmeid menetluses tähtsust omada võivate asjaolude kohta andmekogudest, teistelt avalik-õiguslikke ülesandeid täitvatelt asutustelt ja isikutelt ning eraõiguslikelt isikutelt (lg 9).

PPA-l on kohustus e-residendi digi-ID taotlejat selle kasutamise üle järelevalve menetluses põhjalikult eel- ja järelkontrollida ning teha vajadusel päringuid e-residendi digi-ID taotleja kodakondsusriigi pädevatesse asutustesse, et veenduda tema õiguskuulekuses ja esitatud andmete õigsuses. Näiteks on PPA-l Soomega karistusregistri andmete vahetamise kokkulepe, mille alusel tagatakse PPA-le juurdepääs statistikale, mis näitab mitmel isikul oli mingil perioodil Soomes kehtiv kriminaalkaristus e-residendi digi-ID taotluse menetlemise või järelkontrolli ajal.

Lisaks muudetakse ITDS-i § 9² lõigete 8 ja 9 sõnastus kompaktsemaks. Kehtivas sõnastuses on eristatud e-residendi digi-ID-d ja muid dokumente, kuid õigus andmeid edastada on mõlemal juhul sama, välja arvatud järelevalvemenetluses. Kuna e-residendi digi-ID on ITDS-i tähenduses digitaalne isikutunnistus ehk dokument ning õigus edastada isikuandmeid kolmandatele isikutele dokumendi väljaandmise ja kehtetuks tunnistamise ning sertifikaadi kehtivuse peatamise ja kehtetuks tunnistamise menetluses laieneb ka e-residendi digi-ID-le, on vaja eristada e-residendi digi-ID-d vaid selle kasutamise üle järelevalve menetluses. Muude dokumentide kasutamise üle ITDS-i alusel järelevalvet ei teostata.

3.1.2. PPA õigus edastada andmeid EIS-ile ja EIS-i õigus neid töödelda (§ 1 p 11)

Eelnõu § 1 punktiga 11 täiendatakse ITDS-i § 9² lõigetega 8¹ ja 8².

Lõikega 8¹ antakse PPA-le õigus edastada EIS-ile – täpsemalt e-residentsuse programmi meeskonnale – tema päringu peale e-residendi digi-ID väljaandmise menetluses kogutud andmeid ja e-residendi digi-ID andmeid:

- e-residendi digi-ID taotleja ees- ja perekonnanimi, isikukood, kui see on olemas, sugu, sünniaeg, kodakondsus ja kontaktandmed;
- e-residendi digi-ID väljaandmise koht ja aeg, kehtivusaeg ja kehtetuks tunnistamise aeg;
- e-residendi digi-ID taotlemise eesmärk ja plaanitava tegevuse kirjeldus ning taotlemise põhjendus.

Et võimaldada põhjalikumat taustakontrolli ja e-residendi digi-ID taotluse eesmärgipärasuse paremat hindamist, täiendati 1. aprillil 2021 siseministri määrust¹³ loeteluga lisaandmetest, mille peab e-residendi digi-ID taotleja esitama. E-residendi digi-ID taotlejale avaneb PPA iseteeninduses mahukas taotlusankeet valikvastustega, kus ta peab oskama teha selge valiku oma taotlemise eesmärgi kohta, lähtudes e-residentsuse programmi eesmärgist soodustada Eesti majanduse, teaduse, hariduse ja kultuuri arengut. Lisaks peab e-residendi digi-ID taotleja selgitama oma taotlemise eesmärgi valikut, põhjendama taotlemist ja kirjeldama planeeritavat tegevust, milleks ta e-residendi digi-ID-d vajab. Nii on PPA-l rohkem võimalusi teha põhjalikku taustakontrolli ja hinnata e-residendi digi-ID taotluse eesmärgipärasust. See omakorda aitab vähendada ja ennetada e-residendi digi-ID võimalikku väärkasutust.

Lõikega 8² antakse EIS-ile õigus lõikes 8¹ nimetatud andmeid töödelda vaid selleks, et:

- 1) analüüsida ITDS-i § 20⁵ lõikes 2 nimetatud eesmärgi¹⁴ täitmise tulemuslikkust ja mõju ning osutada selle eesmärgi täitmiseks vajalikke personaliseeritud teenuseid;
- 2) tuvastada ja maandada konkreetse e-residendiga seotud riske.

E-residentsuse programmi eesmärkide saavutamiseks ja tegevusteks on EIS-il teatud määral vaja töödelda e-residendi isikuandmeid ja e-residendi digi-ID andmeid. Isikuandmete töötlemine peab vastama isikuandmete kaitse üldmääruse nõuetele. Isikuandmete töötlemise põhimõtted on sätestatud isikuandmete kaitse üldmääruse artiklis 5, mille lõike 1 punkti b kohaselt peab isikuandmeid koguma täpselt ja selgelt kindlaksmääratud õiguspärastel eesmärkidel ning neid ei tohi töödelda hiljem viisil, mis on nende eesmärkidega vastuolus. Samuti võib punkti c kohaselt töödelda üksnes isikuandmeid, mis on asjakohased, olulised ja vajalikud töötlemise eesmärgi saavutamiseks.

EIS-i õiguslik alus isikuandmeid töödelda on isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt e: avalikes huvides oleva ülesande täitmine. EIS-i üks ülesanne on EIS-i põhikirja¹⁵ punkti 2.1.1 kohaselt „aidata kaasa Eesti kui parima ning kestliku elu- ja ettevõtluskeskkonnaga riigi kujunemisele“. See on avalikes huvides olev ülesanne. Isikuandmete kaitse üldmääruse artikli 6 lõike 3 punkti b kohaselt peab avalikes huvides oleva ülesande täitmise korral olema isikuandmete töötlemise alus kehtestatud liikmesriigi õiguses. Seejuures võib see alus sisaldada erisätteid, näiteks:

- töötlemise seaduslikkust;
- töödeldavate andmete liik;
- andmesubjekte;
- üksuseid, kellele võib isikuandmeid avaldada, ja avaldamise põhjuseid ning
- töötlemise eesmärgi piirangut.

¹³ Siseministri 18. detsembri 2015. aasta määruse nr 77 „[Isikutunnistuse, elamisloakaardi, digitaalse isikutunnistuse, Eesti kodaniku passi, meremehe teenistusraamatu, välismaalase passi, ajutise reisidokumendi, pagulase reisidokumendi või meresõidutunnistuse väljaandmise taotlemisel esitatavate tõendite ja andmete loetelu, väljastamise kord ning väljaandmise tähtajad](#)“ § 24¹.

¹⁴ ITDS-i § 20⁵ lõike 2 kohaselt on e-residendile digi-ID väljaandmise eesmärk soodustada Eesti majanduse, teaduse, hariduse või kultuuri arengut, luues võimaluse kasutada e-teenuseid Eesti digitaalse dokumendiga.

¹⁵ [EIS-i põhikiri](#). Vaadatud 05.10.2023.

Praegu töötleb EIS e-residendi andmeid e-residendi nõusolekul. Samas täidab EIS seejuures avalikes huvides olevat ülesannet, mis ei saa sõltuda e-residendi nõusolekust. Nõusolekupõhine andmetöötlus ei anna riigile vajalikku kogupilti. Samuti võib see mõjutada EIS-i analüüside ja uuringute täpsust, mistõttu ei pruugi nende põhjal tehtud otsused viia õige tulemuseni. PPA andmetel ei anna umbes 20% e-residentidest nõusolekut oma andmete töötlemiseks. Lisaks võib e-resident võtta alati oma nõusoleku tagasi, mis võib samuti statistikat moonutada. E-residente oli 1. juuli 2023. aasta seisuga 105 000. Ehkki EIS-i põhikirja kohaselt on EIS-il andmete töötlemise õigus¹⁶, vajab ta õigusselguse põhimõtte¹⁷ ja isikuandmete kaitse üldmääruse artikli 6 lõike 3 punkti b kohaselt e-residendi andmete töötlemiseks selget õiguslikku alust.

Andmetöötlus võimaldab EIS-il paremini e-residente toetada

E-residendi isikuandmete töötlemine annab EIS-ile võimaluse e-residenti paremini toetada, lähtudes tema profiilist ning e-residendi digi-ID taotlemise eesmärgist ja plaanitavast tegevusest, näiteks toetada teda Eestis ettevõtlusega alustamisel sõltuvalt tema tegevusvaldkonnast. EIS-i e-residentsuse programmi meeskonnal on e-residendiga Eestis kõige vahetum kontakt terve e-residentsuse jooksul. Seetõttu on EIS loogiline kontaktpunkt riigi ja e-residendi vahel, et selgitada välja, mis näiteks takistab e-residendil liikuda selle eesmärgi poole, mille saavutamiseks ta e-residendiks hakkas. Näiteks, kui e-resident on e-residendi digi-ID taotluses märkinud, et ta on Saksamaal iduettevõtja ja tema eesmärk on luua Eestisse finantstehnoloogia ettevõtte, saab EIS teda toetada vajaliku infoga, millist tegevusluba on selleks vaja, ja viia ta kokku erialaekspertidega, kes oskavad teda abistada. Samuti loob EIS rakendust „My e-Residency Portal“, mis toob asutuste info ühte personaalsesse keskkonda kokku. Kõik see kannab eesmärki, et e-residendi huvi luua Eestis ettevõtte ja panustada Eesti majandusse ei raageks.

E-residendi digi-ID taotlemise eesmärgi ja plaanitava tegevuse andmete töötlemine aitab EIS-il ka täiustada e-residentidele teenuse osutajate võrgustikku „e-Residency Marketplace“, võimaldades aru saada, kas ja milliseid teenuseid on vaja võrgustikku juurde. Näiteks, kui andmeanalüüsist selgub, et suur hulk Hispaania e-residente on loovsektori taustaga ja huvitatud looma Eestis ettevõtte oma intellektuaalomandi haldamiseks, on väga tähtis, et EIS tagaks ennetavalt piisava hulga õigusbüroosid, kes spetsialiseeruvad intellektuaalomandiõigusele ja suudavad neid e-residente teenindada.

EIS saab pakkuda PPA-le isikuandmete edastamiseks ka tehnilist tuge. Näiteks on EIS valmis aitama PPA-d e-residendi digi-ID tehnilise toega ja digi-ID kehtivuse lõppemisest teavitamisel, et e-resident esitaks õigel ajal uue e-residendi digi-ID taotluse. Praegu saab PPA e-residendile teavitusi ainult e-kirja teel, kuid kui see ülesanne liiguks EIS-ile, saaks kasutada ka muid teavituskanaleid, näiteks SMS-e, mille võimekust PPA-l ei ole.

Andmetöötlus võimaldab maandada riske kooskõlas andmekaitsepõhimõtetega

Järelevalves on äärmiselt oluline kasutada EIS-i e-residentsuse programmi meeskonna vahetut kontakti e-residentidega, et programmi riske tõhusamalt maandada. EIS-i e-residentsuse programmi meeskonnas on eraldi riskijuht, kes vastutab keskse riskijuhtimise eest. E-residentide andmete töötlemine annab võimaluse tuvastada võimalikke e-residendi digi-ID väärkasutuse mustreid ja e-residendi profiilist tulenevaid riske ning luua riskiaruandeid, mis võimaldavad anda järelevalveasutustele regulaarset infot ja tõhustada koostööd laiemalt. Riskihalduse ja

¹⁶ Sealsamas, p 2.2.11: „oma vastutusvaldkondades andmete ja informatsiooni kogumine, süstematiseerimine, analüüsimine ja edastamine“.

¹⁷ Õigusselguse põhimõtte tuleneb Eesti Vabariigi põhiseaduse § 13 lõikest 2.

järelevalve tõhustamiseks EIS-ile e-residendi andmete töötlemise õiguse andmine on praeguses julgeolekuolukorras väga vajalik meede. Tõenäoliselt on just ebaausate kavatsustega e-residendid selle umbes 20% hulgas, kes ei anna EIS-ile oma andmete töötlemiseks vabatahtlikku nõusolekut ning soovivad tegutseda võimalikult varjatult ja tagaplaanil. Riskide maandamise lisavõimekus on toodud vajadusena välja nii rahapesu ja terrorismi rahastamise riiklikus riskihinnangus¹⁸ kui ka Euroopa Nõukogu rahapesu ja terrorismi rahastamise tõkestamise meetmeid hindava eksperdikomitee (edaspidi *Moneyval*) hindamisaruandes¹⁹.

Kõik EIS-i tegevused ja e-residendi andmete töötlemise eesmärgid on kooskõlas andmete kogumise algse eesmärgiga ega ole seega vastuolus isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktiga b. E-residendi andmete edastamiseks EIS-ile luuakse automatiseeritud andmevahetus üle infosüsteemide andmevahetuskähi (edaspidi *X-tee*). Andmed liiguvad ITDAK-ist e-residentsuse andmebaasi kord ööpäevas. E-residentsuse andmebaas on majutatud riigipilve, mida haldab EIS-i IT-haldus. E-residentsuse andmebaasi andmetele on ligipääs kolmel e-residentsuse programmi meeskonna liikmel, kelle tööülesanded on seotud e-residentide andmete töötlemisega. E-residentsuse andmebaasi kasutajad autentivad ennast sisselogimisel ja juurdepääs on piiratud EIS-i seesmiseks kasutamiseks mõeldud IP-aadressidega. Andmetöötlus logitakse kasutaja kaupa kronoloogilise jadana, mida on võimalik võtta kahtluse korral välja.

3.1.3. E-residendi kohustus hoida oma kontaktandmed ajakohasena (§ 1 p 33)

Eelnõu § 1 punktiga 33 täiendatakse ITDS-i § 14 lõikega 6. Muudatusega kohustatakse e-residendi digi-ID kasutajat hoidma oma kontaktandmed, eelkõige e-posti aadressi, ajakohasena, et PPA saaks vajadusel saata talle tema dokumendi kohta teavitusi. Kohustus pannakse e-residentidele, kuna praktikas on just nendega kõige keerulisem saada vajadusel kontakti.

3.1.4. RAB-i õigus töödelda e-residendi andmeid (§ 1 p-d 51 ja 52)

Eelnõu § 1 punktidega 51 ja 52 muudetakse ITDS-i § 20⁸ lõiget 1 ja täiendatakse paragrahvi lõikega 2¹.

Lõikes 1 loetletud e-residendi digi-ID kasutamise üle riikliku järelevalve teostajate hulka lisatakse RAB. Samuti täpsustatakse, et lõikes 1 nimetatud asutused teostavad riiklikku järelevalvet oma pädevuse piires.

RAB-i järelevalvepädevus tuleneb rahapesu ja terrorismi rahastamise tõkestamise seaduse (edaspidi *RahaPTS*) § 60 lõikest 5¹, mille kohaselt on RAB-il õigus edastada sama paragrahvi lõikes 4 nimetatud teavet PPA-le, et PPA saaks otsustada e-residendi digi-ID väljaandmise, kehtivuse peatamise ja kehtetuks tunnistamise ning suurinvestorile ettevõtluseks tähtjalise elamisloa andmise või pikendamise, andmisest või pikendamisest keeldumise ja kehtetuks tunnistamise üle.

Eelnõuga lisatakse RAB ka ITDS-i § 20⁸ lõikes 1 sätestatud järelevalveasutuste loetellu, et oleks üheselt selge, et tal on pädevus teostada järelevalvet e-residendi digi-ID kasutamise üle.

Lõikega 2¹ antakse RAB-ile õigus riiklikus järelevalves töödelda e-residendi digi-ID väljaandmise menetluses kogutud andmeid ning e-residendi digi-ID kasutamise andmeid, et RAB

¹⁸ Rahandusministeerium 2020. [Rahapesu ja terrorismi rahastamise riiklik riskihinnang](#).

¹⁹ 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](#).

saaks täita oma RahaPTS-i § 54 lõike 1 punktides 1 ja 2 sätestatud ülesandeid. RahaPTS-i § 58 lõike 1 kohaselt on RAB-il õigus oma seadusjärgsete ülesannete täitmiseks saada enda määratud tähtjaks teavet teistelt riigiasutustelt. E-residendi digi-ID kasutamise logiandmetest on RAB-il võimalik kontrollida oma seadusjärgsete ülesannete täitmisel näiteks seda, kas e-residendi digi-ID-d on kasutatud riskiriigis.

3.1.5. Riskiriigi kodanikule e-residendi digi-ID väljaandmise piiramine (§ 1 p 48)

Eelnõu § 1 punktiga 48 täiendatakse ITDS-i § 20⁶ lõigetega 1¹ ja 1², millega luuakse õiguslik alus tagastada riskiriigi kodaniku e-residendi digi-ID taotlus läbi vaatamata ning volitatakse siseministrit kehtestama määrusega riskiriikide nimekirja ja riskiriigi kodanikule e-residendi digi-ID väljaandmise erisused. Muudatus ei mõjuta kehtiva e-residendi digi-ID-ga riskiriigi kodanikke. Kehtiv e-residendi digi-ID kehtib kuni kehtivusaja lõpuni või järelevalvemenetluse tulemusena kehtetuks tunnistamiseni. E-residendi digi-ID kehtib üldjuhul viis aastat.

2014. aastal loodud e-residentsuse programmi eesmärk on soodustada Eesti majanduse, teaduse, hariduse ja kultuuri arengut, et võimaldada välismaalastele turvalist ligipääsu Eesti e-teenustele ning Eesti ja Euroopa Liidu majandusruumile. E-residendil on võimalik oma digi-ID-d kasutada e-keskkonnas isiku tõendamiseks ja digiallkirjastamiseks. Nii saab luua ettevõtte ja kasutada finantsteenuseid.

E-residendi digi-ID väljaandmise riske on hallatud e-residentsuse programmi loomisest alates. See on pidev protsess, mis peab lähtuma muutuvast julgeolekuolukorrast. E-residentsuse programmi riskide maandamise üks peamine eeldus on, et riik teab, kes on Eesti e-residendid, ja et nendeks saaksid ainult õiguskäivad välismaalased. E-residendi digi-ID taotluse esitamisel peab isik põhjendama oma taotlust, täitma mahuka taotlusankeedi ja esitama lisaandmeid oma tausta kohta. Samuti tehakse talle taustakontroll. PPA kontrollib e-residendi digi-ID taotleja isikusamasust, tema seost Eestiga ning seda, kas ta on pannud toime süüteo Eestis või teises riigis ja kas teda kahtlustatakse rahapesus. Samuti teeb PPA muid menetlus-toiminguid, lähtudes e-residendi digi-ID taotleja profiilist.

Riskide maandamiseks on juba kohaldatud meetmeid, näiteks:

- täiendatud e-residendi digi-ID taotlemise iseteenindust, et saada lisainfot ja tõhustada taustakontrolli;
- suurendatud e-residentsuse ohuhinnangute ja menetlustaktika analüüsivõimet PPA-s;
- rakendatud spetsiifilisemat riskipõhist lähenemist, sealhulgas pööratud tõendamiskohustust ehk nõuet esitada karistuse või ärikeelu puudumist tõendavaid dokumente.

Meetmete kohaldamise tulemusena on suurenenud esmase e-residendi digi-ID taotluse kohta negatiivse otsuse tegemise ja digi-ID kehtetuks tunnistamise arv. Kui 2018. aastal oli negatiivsete otsuste osakaal 2%, siis 2022. aastal 8%. Järelekontrolli tulemusena on 2022. aastal tunnistatud kehtetuks 224 e-residendi digi-ID-d, 2020. ja 2021. aastal vastavalt 29 ja 89. Alates 2022. aasta juunist kasutab PPA ka järelekontrolli automaatlahendust, mis võimaldab kontrollida e-residendiga seotud riskiinfot regulaarselt ja automaatselt.

Sellele vaatamata on osa e-residentsuse programmi riske realiseerunud. Tuvastatud on 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 laenuõhise ühisrahastuse kelmustega. Ka virtuaalvääringu valdkonnas võidakse e-residentsust kuritarvitada, näiteks anda e-residendi digi-ID kasutada teisele isikule. Selline käitumine ei ole õiguspärane, kuna teisel isikul on keelatud e-residendi digi-ID-d kasutada. Nii rahapesu ja terrorismi rahastamise riiklik us riskihinnangus kui ka Moneyvali

hindamisaruandes on toodud välja, et e-residentsuse programm võimaldab välismaalasel kasutada Eesti e-residentsust ebasoovitavaks ettevõtluseks ning varjata ettevõtluse tegelikku sisu ja eesmärki ning sellest kasu saajaid.

Eriti probleemne on see selliste kolmandate riikide puhul, kellega puudub Eestil justiits-, julgeoleku- või õiguskaitsealane koostöösuhe, st koostöö ei ole reguleeritud näiteks rahvusvahelise konventsiooni, kahepoolse lepingu ega vastastikuse mõistmise memorandumiga. Koostöösuhte puudumine tähendab, et Eestil ei ole võimalik kontrollida e-residendi digi-ID taotleja tausta tema kodakondsusriigi pädevast asutusest, et kontrollida tema esitatud andmete usaldusväärsust. Sageli on just riskiriigid seotud suurema rahapesu ning terrorismi ja selle rahastamise ohuga ning pelgalt tugevam taustakontroll pole piisav, et maandada kuritegevus- ja julgeolekuriske määral, mis võimaldaks Eestil vältida olulist kahju.

Sellise jääkriski võtmine riigina toob kuritegevus- ja julgeolekuohtude kõrval mainekahju nii Eesti riigile, majandusruumile kui ka e-residentsuse programmile ning ei ole kooskõlas programmi eesmärgiga. Seetõttu on võetud suund võimaldada e-residentsust eelkõige nende riikide kodanikele, kellega on Eestil viisavabadus või justiits-, julgeoleku- või õiguskaitsealane koostöösuhe. Eelnõuga kehtestatakse õiguslik alus, mis võimaldab PPA-l tagastada riskiriigi kodaniku e-residendi digi-ID taotluse läbi vaatamata. Ka Moneyvali hindamine kinnitas, et selline muudatus on äärmiselt oluline muu hulgas selleks, et Eesti ei satuks ise riskiriikide nimekirja, kuna e-residentsuse programmis nägid ekspandid rahapesuohhte.

Riskiriikide määramisel lähtutakse RAB-i nimekirjast „Kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid“²⁰ (edaspidi *RAB-i riskiriikide nimekiri*), kohaldades erisusi, mis võtavad lisaks julgeolekukaalutlustele arvesse Eesti majanduslikke ja välispoliitilisi huve ning e-residentsuse programmi üldeesmärke. RAB-i riskiriikide nimekiri on küll suure terrorismi rahastamise riskiga riikide kohta, kuid kuna rahapesu- ja terrorismi rahastamise risk on üldjuhul suur samades riikides, on muudatusega kaetud ka suure rahapesuriskiga riigid. Muudatusest mõjutatud riskiriikide loetelu on tabelis 1. Riskiriikide kodanikel on 1. juuli 2023. aasta seisuga 8097 kehtivat e-residendi digi-ID-d, mis on umbes 13% kõikidest kehtivatest e-residendi digi-ID-dest.

Tabel 1. Riskiriigid, kelle kodanike e-residendi digi-ID taotlus tagastatakse pärast muudatuse jõustumist läbi vaatamata, ja nende kodanikele väljaantud kehtivate e-residendi digi-ID-de arv 2023. aasta 1. juuli seisuga

	Riskiriik	Kehtivate e-residendi digi-ID-de arv
1	Afganistani Islamivabariik	30
2	Alžeeria Demokraatlik Rahvavabariik	164
3	Burkina Faso	11
4	Egiptuse Araabia Vabariik	504
5	Iraagi Vabariik	52
6	Iraani Islamivabariik	637
7	Jeemeni Vabariik	44
8	Jordaania Hašimiidi Kuningriik	113
9	Kongo Demokraatlik Vabariik	18
10	Liibanoni Vabariik	146
11	Liibüa Riik	47
12	Lõuna-Sudaani Vabariik	0

²⁰ RAB 2022. Juhend kahtlaste tehingute tunnuste kohta. Lisa: [kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid](#).

13	Mali Vabariik	13
14	Maroko Kuningriik	269
15	Mosambiigi Vabariik	1
16	Nigeeria Liitvabariik	158
17	Nigeri Vabariik	0
18	Pakistani Islamivabariik	684
19	Palestiina Omavalitsus	35
20	Korea Rahvademokraatlik Vabariik	0
21	Saudi Araabia Kuningriik	34
22	Somaalia Liitvabariik	1
23	Sudaan	29
24	Süüria Araabia Vabariik	127
25	Tuneesia Vabariik	359
26	Usbekistan	85
27	Valgene Vabariik	793
28	Venemaa Föderatsioon	3743
	KOKKU	8097

Allikas: PPA

Võrreldes RAB-i riskiriikide nimekirjaga jäetakse eelnõuga välja Türgi ja Araabia Ühendemiraadid ning lisatakse Venemaa ja Valgevene. Türgi ja Araabia Ühendemiraatide kodanike e-residendi digi-ID taotlust ei jäeta läbi vaatamata nii julgeoleku-, majandus- kui ka välispoliitilistel põhjustel.

- **Türgi** on NATO liikmesriigina Eestile oluline julgeolekupartner ning RAB-i riskiriikide nimekirja riskiriikidest on Türgil kõige suurem aktiivsete e-residentide kogukond. 1. juuli 2023. aasta seisuga on 2855 Türgi kodanikku, kellel on kehtiv e-residendi digi-ID. See on umbes 4,5% kõikidest kehtivatest e-residendi digi-ID-dest. Võrreldes teiste RAB-i riskiriikide nimekirja riskiriikidega on Türgi e-residentide ettevõtted enim alustanud reaalsel majandustegevust Eestis. Kõikide RAB-i riskiriikide nimekirja riskiriikide e-residentide ettevõtete tasutud maksudest on Türgi e-residentide ettevõtete riiklikud maksud umbes 96% ja tööjõumaksud 90%.
- **Araabia Ühendemiraadid** on Eestile oluline piirkond riiklike ja ärisuhete loomisel ja edendamisel ning 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. Araabia Ühendemiraatide e-residente on vähe: 1. juuli 2023. aasta seisuga on neil üheksa kehtivat e-residendi digi-ID-d.

Riigi riskiriigiks määramine ei tähenda selle kodanikele, et nad ei saa üldse e-residendi digi-ID-d taotleda. Eelnõuga antakse siseministrile volitus kehtestada **määrus, millega luuakse erisused riskiriigi kodanikele, kes vastavad vähemalt ühele järgmistest tingimustest**²¹.

- 1) Isik on elanud vahetult enne e-residendi digi-ID taotluse esitamist vähemalt kolm järjestikust aastat **Euroopa Liidu liikmesriigis või Ühendkuningriigis** ja tal on selle riigi kehtiv elamisluba. Euroopa Liidu liikmesriikide vahel ning Euroopa Liidu ja Ühendkuningriigi kui endise Euroopa Liidu liikmesriigi vahel on toimivad koostöösuhted ja andmevahetusmudel, mis läbi on Eestil võimalik saada nendest riikidest isiku kohta usaldusväärset lisainfot. Neis riikides on kehtestatud ühtsed elamisloakaartide standardid, mis võimaldavad menetlejal veenduda isiku esitatud andmete ja dokumendi õigsuses. Kolmandates riikides on aga kasutusel erinevad elamisõigust tõendavad alusdokumendid, mille õigsuse tuvastamine ei pruugi olla võimalik.

²¹ Ukraina-vastase täiemahulise sõja tõttu ei kohaldata neid erisusi Venemaa ja Valgevene kodanikele, välja arvatud korduvtaotluse erisus.

- 2) Isikul on **Eestis püsiv majandustegevus**. E-residendi digi-ID-d võimaldatakse taotleda riskiriigi kodanikul, kes tegeleb tõestatavalt Eestis majandustegevusega, st ta on loonud enne e-residendiks saamist Eestis ettevõtte või tal on ettevõtlusseos Eesti ettevõtjaga, näiteks juhatuse liikmena. Erisust kohaldatakse juhul, kui ettevõtte tegutseb aktiivselt ning selle kohustused Eesti 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.
- 3) Isik esitab **e-residendi digi-ID korduvtaotluse**. Korduvtaotluse 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 ja sellega kaasneb Eestile maksutulud, st nullkäibega ettevõttele erisust ei kohaldata.
- 4) Isik on **Eesti välisesinduse töötaja või aukonsul**. Eestil on ka riskiriikides, näiteks Egiptuses, välisesindusi ja ei ole välistatud, et välisesinduse töötaja, kes vajab oma tööülesannete täitmiseks e-residendi digi-ID-d, on riskiriigi kodanik. Kõik sellised isikud läbivad põhjaliku taustakontrolli ja riskide ilmnemise korral saab PPA e-residendi digi-ID taotluse tagastada seda läbi vaatamata.

76% riskiriigi kodanikest e-residentidest ei ela Euroopa Liidus ega Ühendkuningriigis, sealhulgas ei ole neist 53%-l Eestis ärisuhteid. Seega puudub eelnõu tõenäoliselt umbes 53% riskiriigi kodanikest e-residente. Kõikidest kehtiva e-residendi digi-ID-ga e-residentidest on see ca 3%.

Tõhustatud eel- ja järelkontrolli ning muid juba juurutatud riskide maandamise meetmeid rakendatakse eriti rangelt nende suhtes, kellele kohaldatakse eelnimetatud erisusi, ja nende suhtes, kes ei ole küll riskiriigi kodanikud, kuid märgivad oma elukohariigiks riskiriigi, Türgi või Araabia Ühendemiraadid.

Riskiriikide loetelu, erisused riskiriigi kodanikele ja jääriskid on otsustatud e-residentsuse nõukokku kuuluvate ministeeriumide ja asutuste²² ühisel kokkuleppel, et muudatus arvestaks laiapinnaliselt Eesti huve ja seisukohti. On äärmiselt tundlik ja keeruline väljakutse leida Eesti riigi huvide tagamiseks tasakaal, mis lähtub riigi julgeoleku ja siseturvalisuse tagamise vajadusest, arvestades samas riigi maine ning välispoliitiliste, majanduslike ja e-residentsuse programmi eesmärkidega. Kavandatud erisustega see tasakaal saavutatakse.

3.1.6. E-residendi digi-ID taotlemine ainult PPA iseteeninduses ja isikliku ilmunise kohustus (§ 1 p-d 50 ja 54–57)

Eelnõu § 1 punktidega 50 ja 54–57 muudetakse ITDS-i § 20⁷ lõiget 1¹ ning § 20¹² pealkirja ning lõikeid 1 ja 2, täiendatakse § 20¹² lõikega 1¹ ja tunnistatakse kehtetuks § 20¹² lõige 3. Muudatustega viiakse kehtiv õigus kooskõlla väljakujunenud praktikaga, et e-residendi digi-ID taotluse saab esitada vaid PPA iseteeninduses.

- 1) ITDS-i § 20⁷ lõiget 1¹ muudetakse nii, et edaspidi esitatakse e-residendi digi-ID taotlus isiklikult PPA iseteeninduses. Kehtiva lõike kohaselt võib isik esitada e-residendi digi-ID taotluse Eesti konsulaarametnikule, kes edastab selle pärast taotleja isikusamasuse kontrollimist ja biomeetriliste andmete võtmist PPA-le läbivaatamiseks. Praktikaks kasutatakse aga e-residendi digi-ID taotluse esitamiseks PPA iseteenindust. E-residendi digi-ID taotlejad elavad üldjuhul välisriigis ja seetõttu on taotluse esitamine PPA iseteeninduses neile oluliselt mugavam. Seega viiakse ITDS kooskõlla IT-lahenduste ja praktikaga.

²² E-residentsuse nõukokku kuuluvad JUM, MKM, RAM, SIM, VÄM, EIS ja PPA.

- 2) ITDS-i § 20¹² pealkirja täiendatakse sõnadega „isikusamasuse kontrollimise“. Isik tuvastatakse, kui ta taotleb dokumenti esimest korda ja riigil puuduvad tema kohta andmed. Kui isik taotleb hiljem uut dokumenti, kontrollitakse isikusamasust. Seetõttu on korrektne tuua pealkirjas esile isikutuvastuse kõrval ka isikusamasuse kontroll.
- 3) ITDS-i § 20¹² lõigetest 1 ja 2 jäetakse välja osa, mille kohaselt ei pea ilmuma e-residendi digi-ID taotluse esitamiseks isiklikult dokumendi väljaandja asukohta või Eesti välisesindusse. Eelnõu § 1 punktiga 50 sätestatakse, et e-residendi digi-ID taotlus esitatakse isiklikult PPA iseteeninduses. Seega ei ole enam asjakohane viidata ITDS-i § 20¹² lõikes 1 nõudele ilmuda e-residendi digi-ID taotluse esitamiseks isiklikult dokumendi väljaandja asukohta või Eesti välisesindusse. Nii praktikas kui ka ITDS-i § 20¹² lõigete 1 ja 2 muudatuse kohaselt peab e-residendi digi-ID taotleja isiku tuvastamiseks või isikusamasuse kontrollimiseks ilmuma isiklikult väljaandja asukohta või Eesti välisesindusse üksnes e-residendi digi-ID väljaandmise menetluses või e-residendi digi-ID väljastamisel. Selline lahendus on paindlik ja võimaldab e-residendi digi-ID taotlejal otsustada, millal tal on mugavam minna enda isikut tuvastama või isikusamasust kontrollima.
- 4) ITDS-i § 20¹² lõikega 1¹ kehtestatakse nõue, et alla 15-aastane e-residendi digi-ID taotleja peab isiku tuvastamiseks või isikusamasuse kontrollimiseks ilmuma e-residendi digi-ID väljaandja asukohta või Eesti välisesindusse **isiklikult koos seadusliku esindajaga**. ITDS-i § 12¹ lõigete 3 ja 4 kohaselt ei pea alla 15-aastane dokumendi kättesaamiseks isiklikult dokumendi väljastaja asukohta ilmuma ning dokumendi võib väljastada tema seaduslikule esindajale. ITDS-i § 20¹² lõikega 1¹ kehtestatakse erisus alla 15-aastasele e-residendi digi-ID taotlejale. Muudatus on vajalik alaealise õiguste ja huvide kaitseks. Sellega antakse dokumendi väljaandjale võimalus veenduda, et e-residendi digi-ID taotluses esitatud isikuandmete taga on tegelik isik ja ei ole esitatud valeandmeid ehk laps ei ole fiktiivne.
- 5) ITDS-i § 20¹² lõige 3 tunnistatakse kehtetuks, kuna e-residendi digi-ID taotluse saab esitada vaid PPA iseteeninduses, mitte e-posti teel, nagu on kehtivas lõikes.

3.1.7. E-residendi digi-ID riigilõiv (§ 6 p-d 2 ja 3)

Eelnõu § 6 punktidega 2 ja 3 muudetakse RLS-i § 272 lõikeid 6 ja 20.

Lõikest 6 jäetakse välja Eesti välisesinduses e-residendi digi-ID taotlemise riigilõiv, kuna e-residendi digi-ID-d on võimalik taotleda vaid PPA iseteeninduses. Lisaks täiendatakse lõiget teise lausega, sätestades, et kui e-residendi digi-ID taotlus jäetakse läbi vaatamata, ei tagastata riigilõivu. Riigilõivu tagastamine on põhjendatud juhul, kui e-residendi digi-ID taotleja on näiteks kogemata esitanud korraga kaks e-residendi digi-ID taotlust ja tasunud riigilõivu topelt või loobub taotlemisest enne, kui tema e-residendi digi-ID taotlus on võetud menetlusse. Kui e-residendi digi-ID taotlust on hakatud juba sisuliselt menetlema ja e-residendi digi-ID taotleja ei kõrvalda menetleja tuvastatud puuduseid või ei täida tõendamiskohustust, näiteks ei esita pärast korduvaid meeldetuletusi passi nõuetekohast koopiat, ei suuda põhjendada e-residendiks saamise motiive või ei esita oma kodakondsusriigi karistusregistri väljavõtet, on põhjust kahelda tema motiivides ja huvis saada e-residendiks.

E-residentsus on ajutine hüve, mille andmisel lähtutakse ühelt poolt riigi julgeolekuolukorrast ja e-residentsuse programmi eesmärkidest ning teiselt poolt e-residendi digi-ID taotleja motiividest ja tema panusest e-residentsuse programmi eesmärkidesse. Eestil on kohustus tagada, et riiklik dokument antakse välja vaid selleks õigustatud isikule. Riigil on pädevus otsustada, kellele ja mis tingimustel e-residendi digi-ID välja antakse, ning mitte kellelgi ei ole

subjektiivset õigust seda saada. E-residendi digi-ID väljaandmise menetlus on oluliselt ressursimahukam kui Eesti kodaniku dokumendi väljaandmise menetlus. E-residendi digi-ID väljaandmise menetluses tehakse e-residendi digi-ID taotlejale taustakontroll, mis sisaldab päringuid ja lisaandmete küsimist, et veenduda isiku isikusamasuses ja tema motiivides ning selles, et ta ei kujuta ohtu riigi julgeolekule. Kui e-residendi digi-ID taotleja ei ole korduvate meeldetuletuste peale esitanud e-residendi staatuse saamiseks ja digi-ID väljaandmiseks korrektseid andmeid ega selgeid põhjendusi, on riigilõivu tagastamata jätmise põhjendatud, sest e-residendi digi-ID taotluse menetlemisel on juba tehtud tööd ja toiminguid, mis on toonud riigile kaasa kulu.

Lõikest 20 jäetakse välja viide ITDS-i § 272 lõikele 6, sest eelnõu kohaselt arvestatakse e-residendi digi-ID väljastamise riigilõivu selle taotlemise riigilõivu sisse. Üldjuhul elavad e-residendid välisriigis, mistõttu saavad nad oma e-residendi digi-ID kätte Eesti välisesindusest.

3.1.8. Viitemuudatus e-residendi digi-ID väljaandmise aluses (§ 1 p 47)

Eelnõu § 1 punktiga 47 muudetakse ITDS-i § 20⁵ lõiget 1, milles on määratletud e-residendi digi-ID. Kehtiva lõike järgi antakse e-residendi digi-ID välja ITDS-i § 20¹ lõikes 2 nimetama ta isikule. Kuna see lõige tunnistatakse eelnõu § 1 punktiga 45 kehtetuks, tuleb muuta ka viidet dokumendile, mille omamise või taotlemise korral ei anta isikule e-residendi digi-ID-d. Muudatuse kohaselt ei anta edaspidi e-residendi digi-ID-d isikule, kellel on kehtiv Eesti isikutunnistus või elamisloakaart või kes taotleb seda e-residendi digi-ID-ga samal ajal. Muudatus on tehniline.

3.2. Dokumendiliigid, dokumendikohustus ja isikusamasuse kontrollimine

3.2.1. Pass kohustusliku dokumendina (§ 1 p 3) ja koduteeninduse piirangu kaotamine (§ 1 p-d 15 ja 16)

Eelnõu § 1 punktidega 3, 15 ja 16 muudetakse ITDS-i § 5 lõikeid 1 ja 2 ning § 11⁵ lõiget 3 ning tunnistatakse kehtetuks § 11⁵ lõige 2.

ITDS-i § 5 lõike 1 kohaselt peab Eestis elaval Eesti kodanikul olema isikutunnistus. Pass on vabatahtlik. Muudatusega võimaldatakse inimesel valida, kas ta taotleb kohustusliku dokumendina isikutunnistust või passi. Isikutunnistuse kohustuslikkus oli oluline Eesti e-riigi ja e-teenuste laialdase kasutuselevõtu toetamiseks, olles alguses ainus eID vahend²³. Praegu on aga infoühiskond ja e-teenused pigem mobiilipõhised ning inimesed eelistavad e-keskkonnas kasutada mobiil-ID vormis digitaalset isikutunnistust (edaspidi *mobiil-ID*) või muid mobiilipõhiseid autentimis- ja allkirjastamisvahendeid. Alates 2017. aasta 1. jaanuarist on passi kehtivusaeg üldjuhul kümme aastat²⁴. Seevastu isikutunnistus kehtib viis aastat. Isikutunnistuse viieaastane kehtivusaeg tuleneb vajadusest tagada eID-tehnoloogia – kiibi, sertifikaatide, võtmete ja algoritmide – turvalisus ja kasutatavus kogu füüsilise dokumendi kehtivusajal.

Muudatus annab inimesele võimaluse taotleda kohustusliku dokumendina pikema kehtivusajaga pass, säästes selliselt nii riigilõivukulu kui ka aega, mis kulub dokumendi taotlemisele ja kättesaamisele. Kui inimene kasutab e-keskkonnas mobiilipõhist autentimis- ja allkirjastamisvahendit ehk mobiil-ID-d ja füüsilise dokumendina passi, on tal tarvis taotleda PPA-st dokumenti iga kümne aasta tagant. Pass kohustusliku dokumendina sobib ka sellele sihtrühmale, kes mingil põhjusel e-teenuseid ei tarbi, näiteks osa vanemaealisi. Mobiil-ID-d on

²³ Isikutunnistusi hakati välja andma 01.01.2002.

²⁴ Viieaastase kehtivusajaga pass on vaid alla 15-aastaselt lapsel, erandkorras ka vanemal inimesel.

võimalik taotleda kehtiva dokumendi olemasolu korral ja selleks sobib nii isikutunnistus kui ka pass.

- **Isikutunnistuse alusel** saab **mobiil-ID-d** taotleda nii mobiilioperaatori esinduses kui ka iseteeninduses. Mobiil-ID kehtib viis aastat. Samuti saab isikutunnistuse alusel registreerida **Smart-ID** konto. Smart-ID konto kehtib kolm aastat.
- **Passi alusel mobiil-ID** taotlemiseks ja lepingu sõlmimiseks tuleb minna sobiva mobiilioperaatori²⁵ esindusse, mis asuvad suuremates ostukeskustes. Mobiilioperaator kontrollib kohapeal mobiil-ID taotleja isikusamasust ja pärast lepingu sõlmimist on mobiil-ID kohe kasutusvalmis.
- **Passi alusel Smart-ID** konto registreerimine sõltub sellest, kas Smart-ID-d taotletakse esimest korda või korduvalt. Esimest korda on võimalik Smart-ID-d taotleda pangakontoris. Eestis pakuvad seda teenust Luminor, SEB ja Swedbank. Pärast esimest korda on võimalik täisealisel isikustada Smart-ID konto passiga biomeetrilise isikutuvastuse²⁶ abil.

Tabel 2. Kehtivate dokumentide ja Smart-ID kordumatute kasutajate statistika seisuga 17.08.2023

Eesti kodaniku pass	Isikutunnistus	Mobiil-ID	Smart-ID
840 667	1 095 955	244 000	694 000

Allikas: PPA ja SK ID Solutions AS

Võrreldes passiga on isikutunnistuse eelis selle kompaktsus kaasas kandmisel, arvestades, et isikutunnistusega on võimalik reisida ka Euroopa Liidus ja Schengeni alal. Kehtiva dokumendi kaasas kandmine on piirületusel kohustuslik, isegi kui seda piiril ei kontrollita, näiteks laeva, auto või bussiga naaberriiki sõites. Eestis ei pea üldjuhul dokumenti kaasas kandma. Dokumenti kaasas kandmise kohustus kehtib vaid juhtudel, kui on tarvis tõendada teatud erioigusi, näiteks mootorsõiduki juhtimisel juhul, kui juhiluba ei ole kaasas, relva kandmisel või näiteks alkoholi ostes vanuse tõendamisel.

Isikutunnistusel on veel teisi funktsioone, näiteks kasutatakse seda sageli kliendikaardina, et ei peaks rahakotis kandma mitmeid plastkaarte. Ka see funktsioon on muutumas isikutunnistuspõhisest mobiilpõhiseks, sest infoühiskond ja inimeste käitumisharjumused on muutunud ning kõiki toiminguid eelistatakse teha mobiiltelefoniga. Püsikliendi staatus on enamasti seotud isikukoodiga ja oma õigust saada soodustusi saab sellega tõendada. Isikukoodi esitamiseks ja püsikliendi staatusega sidumiseks ei ole tänapäeval tingimata vaja kanda isikutunnistust füüsiliselt kaasas. Lisaks töötatakse välja mRiiki, mis võimaldab kontrollida isikusamasust ja esitada andmeid, sealhulgas isikukoodi, Eesti riikliku teabevärava mobiilirakenduses, ning Euroopa Liidu tasandil kavandatakse eIDAS-e määruse 2.0²⁷ raames digikukru lahendust, mille üks osa on ka digidokument. Kokkuvõtvalt ei teki muudatusega inimestele lisakohustust, vaid antakse valikuvõimalus, arvestades tegelikke vajadusi.

ITDS-i § 5 lõikes 2 sätestatakse, et kehtivat isikutunnistust ega Eesti kodaniku passi ei pea olema Eestis elaval alla 15-aastasel Eesti kodanikul. Kehtivas lõikes on viidatud konkreetselt isikutunnistusele, aga lõike 1 muudatuse tõttu tuleb lõikes 2 hõlmata ka Eesti kodaniku pass.

ITDS-i § 11⁵ lõige 2 tunnistatakse kehtetuks ja lõiget 3 muudetakse, et kaotada piirang PPA koduteenindusele reisidokumendi taotlemisel. Praegu võib PPA minna reisidokumendi taotluse

²⁵ Välja arvatud Telia, kes pakub mobiil-ID lepingu sõlmimist vaid iseteeninduses, kuhu sisselogimiseks on vaja isikutunnistust.

²⁶ smart-ID.ee. [Biomeetriline isikutuvastus: kas ma saan seda kasutada?](#) Vaadatud 06.10.2023.

²⁷ Euroopa Komisjoni 3. juuni 2021. aasta ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega. – [COM/2021/281 final](#).

vastuvõtmiseks ja biomeetriliste andmete võtmiseks reisidokumendi taotleja Eesti elamis- või viibimiskohta vaid kahel juhul:

- 1) kui taotleja esitab reisidokumendi taotluse koos isikutunnistuse või elamisloakaardi taotlusega, mis on praegu kohustuslikud dokumendid, või
- 2) kui reisidokumendi on vaja ravi saamise eesmärgil välisriiki reisimiseks.

Edaspidi ei ole neid põhjendusi vaja, sest ka reisidokument on võimalik valida kohustuslikuks dokumendiks. Kohustusliku dokumendi taotlemisel võib PPA pakkuda taotlejale koduteenindust, kui taotleja tervises seisund ei võimalda tal minna isiklikult PPA-sse kohale. Sellisel juhul peab taotleja koduteeninduse taotlusele lisama enda tervises seisundit tõendava dokumendi.

3.2.2. Sertifikaadi kehtivuse peatamise ja taastamise lõpetamine (§ 1 p-d 2, 4, 10, 13, 27, 49 ja 53)

Eelnõu § 1 punktidega 13 ja 49 tunnistatakse kehtetuks ITDS-i § 9⁵ ja § 20⁶ lõige 5. **Eelnõu § 1 punktidega 2, 4, 10, 27 ja 53** muudetakse ITDS-i § 3¹ lõiget 3, 3. peatüki pealkirja, § 9² lõikeid 8 ja 9, § 13 lõiget 1², § 20⁶ pealkirja, § 20⁷ pealkirja, lõike 3 sissejuhatavat lauseosa ning lõikeid 4 ja 5 ning § 20⁸ lõiget 3. Muudatustega jäetakse ITDS-ist välja viited sertifikaadi kehtivuse peatamisele ja taastamisele.

ITDS-i § 9⁵ kohaselt on dokumendi väljaandjal õigus peatada dokumendi sertifikaadi kehtivus ning taastada peatatud kehtivusega sertifikaadi kehtivus e-identimise ja e-tehingute usaldusteenuste seaduse §-des 17 ja 18 sätestatud tingimustel. Peatatud kehtivusega sertifikaadiga on aga teoreetiliselt võimalik luua krüptograafiline allkiri ja sertifikaadi kehtivuse taastamisel ei ole võimalik tuvastada, et allkiri on antud ajal, kui sertifikaadi kehtivus oli peatatud. See on aga vastuolus eIDAS-e määruse²⁸ artikli 32 nõudega kvalifitseeritud e-allkirja valideerimise kohta, sest puudub võimalus kontrollida, kas sertifikaat oli allkirja andmise ajal kehtiv. Seega lõpetatakse uue ID-1 formaadis dokumentide tootmise lepingu rakendamisega 1. novembrist 2025 võimalus sertifikaadi kehtivust peatada ja taastada nii uue lepingu alusel välja antava dokumendi kui ka varasema lepingu alusel välja antud kehtiva dokumendi puhul.

3.2.3. Digitaalse isikutunnistuse väljaandmise lõpetamine (§ 1 p-d 13, 45 ja 46, § 3 p-d 3–5 ning § 6 p-d 1 ja 4)

- 1) **Eelnõu § 1 punktidega 13, 45 ja 46** tunnistatakse kehtetuks ITDS-i § 11² lõiked 5 ja 6, § 20¹ lõige 2 ning § 20⁴ lõiked 6 ja 8.
- 2) **Eelnõu § 3 punktidega 3–5** muudetakse KonS-i § 48 pealkirja ja lõiget 2 ning tunnistatakse kehtetuks lõige 1.
- 3) **Eelnõu § 6 punktiga 1** tunnistatakse kehtetuks RLS-i § 272 lõige 5 ja **punktiga 4** muudetakse lõiget 20.

ITDS-i § 11² lõigetes 5 ja 6 ning § 20¹ lõikes 2, KonS-i §-s 48 ja RLS-i § 272 lõigetes 5 ja 20 on reguleeritud digitaalse isikutunnistuse taotlemist, väljaandmist ja väljastamist ning väljaandmise riigilõivu määra.

²⁸ 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, 28.8.2014, lk 73–114.](#)

Muudatused puudutavad ainult seda digitaalset isikutunnistust, mis antakse välja ITDS-i § 20¹ lõike 2 alusel²⁹. Lisaks sellele on digitaalsed isikutunnistused ITDS-i § 20⁴ lõike 1 kohaselt mobiil-ID ja § 20⁵ lõike 1 kohaselt e-residendi digi-ID, kuid neid muudatused ei puuduta. Seetõttu:

- 1) jääb kehtima osa sätteid, milles on reguleeritud digitaalseid isikutunnistusi, ja
- 2) muudetakse osa sätteid selliselt, et neid kohaldatakse edaspidi vaid e-residendi digi-ID-le, näiteks jääb KonS-i § 48 edaspidi reguleerima vaid e-residendi digi-ID väljastamist, sest erinevalt muust digitaalsest isikutunnistusest saab e-residendi digi-ID taotluse esitada vaid iseteeninduses, kuid e-residendi digi-ID-d on võimalik kätte saada ka Eesti välisesinduses.

Digitaalne isikutunnistus, mis antakse välja ITDS-i § 20¹ lõike 2 alusel, on teisene dokument, mida on võimalik kasutada vaid e-keskkonnas oma isiku tuvastamiseks ja digiallkirja andmiseks. Digitaalsel isikutunnistusel ei ole fotot ja seda ei saa kasutada oma isiku füüsiliseks tõendamiseks. Inimeste vajadus digitaalse isikutunnistuse järele on olnud viimastel aastatel langustrendis ning infoühiskonda ja kaasaegseid e-teenuseid eelistatakse pigem kasutada mobiil-ID-ga. Seda näitab selgelt ka tabel 3.

Tabel 3. Digitaalse isikutunnistuse ja mobiil-ID taotluste arv aastatel 2019–2023

	2019	2020	2021	2022	01.01.–31.08.2023
Digitaalne isikutunnistus	5103	4762	5019	4136	2746
Mobiil-ID	59 466	62 649	80 751	76 886	42 953

Allikas: PPA

PPA prognoosi kohaselt väheneb lähiaastatel vajadus digitaalse isikutunnistuse järele veelgi. Tavapärastel taotleval digitaalsel isikutunnistust korduvalt umbes 50% taotlejatest.

Seega lõpetatakse uue ID-1 formaadis dokumentide tootmise lepingu rakendamise alates 1. novembrist 2025 digitaalse isikutunnistuse väljaandmine ja tunnistatakse kehtetuks RLS-i § 272 lõige 5, milles on reguleeritud digitaalse isikutunnistuse taotluse läbivaatamise riigilõivu, ja muudetakse lõiget 20, et jätta välja viide lõikele 5.

Lisaks tunnistatakse kehtetuks ITDS-i § 20⁴ lõiked 6 ja 8. Lõike 6 kohaselt ei pea valdkonna eest vastutav minister kehtestama mobiil-ID taotluse vormi. Mobiil-ID taotluse vormi ei ole vaja kehtestada, kuna mobiil-ID taotlus esitatakse mobiilioperaatorile, kelle sisemisse töökorraldusse ei ole vaja määruse tasandil sekkuda. ITDS-i § 20⁴ lõikes 8 sätestatud volitusnormi, mis võimaldab valdkonna eest vastutaval ministril kehtestada määrusega mobiil-ID väljaandmise üksikasjad ja mis kehtib 2014. aasta 1. maist, ei ole läinud praktikas seni vaja. Seetõttu on otstarbekas tunnistada need sisutühjad lõiked kehtetuks. Muudatused on tehnilised.

3.2.4. Uue dokumendi taotlemine andmete muutumise korral (§ 1 p 30)

Eelnõu § 1 punktiga 30 muudetakse õigusselguse huvides ITDS-i § 14 lõiget 1, sätestades, et kui dokumendi andmed on muutunud, peab dokumendi kasutaja taotlema uue dokumendi ühe kuu jooksul andmete muutumisest arvates.

ITDS-i § 13 lõike 1 punktis 3 on sätestatud, et dokument tunnistatakse kehtetuks, kui see või selle kanne või andmed on võltsitud või ebaõiged. Samas ei kohaldata ebaõigete andmetega dokumendi jätkuva kasutamise korral karistusmeetmeid. Praktikas on ette tulnud olukordi, kus

²⁹ ITDS-i § 20¹ lõikes 2 on sätestatud, et digitaalne isikutunnistus antakse välja Eesti kodanikule ning välismaalasele, kellele on varem välja antud isikutunnistus või elamisloakaart või kes taotleb isikutunnistust või elamisloakaarti samaaegselt digitaalse isikutunnistusega.

inimene ei taotle uut dokumenti enne eelmise dokumendi kehtivusaja lõppemist ja kasutab aktiivselt ebaõigete andmetega dokumenti. Näiteks on inimene muutnud nime abiellumisel või muul põhjuse³⁰, kuid ei taotle uue nimega dokumenti. Selliselt võib näiteks isikutunnistusega digiallkirjastamise korral tekkida olukord, kus rahvastikuregistri andmetel on isikul üks perekonnanimi, kuid digiallkirjal teine. Muudatusega pannakse inimesele selge kohustus taotleda andmete muutumise korral ühe kuu jooksul uus dokument. Andmete muutumise korral teavitatakse inimest sellest kohustusest ja antakse ühtlasi teada, et kui ta ei taotle uut dokumenti ühe kuu jooksul, tunnistatakse tema dokument kehtetuks. Kui dokumendi taotlus on esitatud selle tähtaja jooksul, ei tunnistata dokumenti kehtetuks enne, kui uus dokument on väljastatud.

3.2.5. Terminikasutuse ühtlustamine (§ 1 p 1) ning samaliigilise dokumendi esitamise ja surma korral dokumendi tagastamise nõude kaotamine (§ 1 p-d 28 ja 32)

Eelnõu § 1 punktiga 1 muudetakse ITDS-i § 3¹ pealkirja ning lõikeid 1–3 ja 5, § 4¹, § 9⁵ lõikeid 1 ja 2, § 11⁴ lõiget 6, § 11⁶ lõiget 10, § 12¹ lõiget 9, § 15² lõikeid 2 ja 6 ning § 20¹⁵ lõiget 2, et ühtlustada ITDS-is lühendi „dokument“ kasutamist. See on vajalik, sest ITDS-i § 2 lõikes 1 on sätestatud, et ITDS-is kasutatakse termini „isikut tõendav dokument“ asemel edaspidi terminit „dokument“. Muudatus on tehniline.

Eelnõu § 1 punktidega 28 ja 32 muudetakse ITDS-i § 13 lõiget 5 ning tunnistatakse kehtetuks § 14 lõiked 3 ja 5, mis on kaotanud oma ajakohasuse ja ei täida tänapäevases infoühiskonnas enam oma eesmärki.

ITDS-i § 13 lõike 5 kohaselt teeb dokumendi väljastaja kehtetuks tunnistatud dokumenti kehtetuks tunnistamise kohta märke või muudab selle muul viisil kasutamiskõlbmatuks, välja arvatud juhul, kui dokument on kadunud või hävinud. Praktikast tagatakse dokumendi kasutamiskõlbmatust selle nurga äralõikamisega ja märgest dokumenti ei tehta. Lõiget 5 muudetakse seega selliselt, et edaspidi teeb dokumendi väljastaja kehtetuks tunnistatud dokumendi kasutamiskõlbmatuks siis, kui dokumendi taotleja selle uue dokumendi väljastamisel esitab. Muudatus on tehniline ja seotud ITDS-i § 14 lõike 3 kehtetuks tunnistamisega.

ITDS-i § 14 lõike 3 kohaselt tuleb praegu dokumendi väljastamisel esitada samaliigiline dokument, et PPA menetleja saaks teha selle nurga äralõikamisega kasutamiskõlbmatuks. Nõue on aegunud, sest varasem samaliigiline dokument tunnistatakse ITDAK-is kehtetuks ja teave kehtetuks tunnistatud dokumendi kohta saadetakse ka rahvusvahelistesse andmebaasidesse: Schengeni infosüsteemi ning INTERPOL-i varastatud, kaotatud ja kehtetuks tunnistatud isikut tõendavate dokumentide andmebaasi.

Lõike 3 kehtetuks tunnistamisega lihtsustatakse inimese jaoks protsessi, sest ta ei pea edaspidi uue dokumendi kätte saamiseks tingimata esitama samaliigilist dokumenti. Näiteks ei teki passi ja isikutunnistuse koos taotlemisel edaspidi olukorda, kus inimesele, kes on võtnud kaasa vaid ühe kehtiva dokumendi, ei väljastata teist dokumenti. Sama kehtib olukorras, kus inimene on taotlenud passi ja sellele järele minnes ei ole talle võimalik seda kätte anda, kuna tal on kaasas vaid isikutunnistus ja kehtiv pass on ununenud koju. Kui aga inimene siiski esitab uue dokumendi väljastamisel kehtiva samaliigilise dokumendi, teeb menetleja selle endiselt kasutamiskõlbmatuks.

ITDS-i § 14 lõike 5 kohaselt tuleb praegu dokumendi kasutaja surma või surnuks tunnistamise korral tagastada dokument selle väljaandjale. See on samuti ajale jalgu jäänud nõue, sest dokumendi kasutaja surma või surnuks tunnistamise korral tunnistatakse tema dokument

³⁰ Näiteks sages nimevahetus pärast Ukraina-vastase sõja algust, kuna sooviti võtta eestipärasem nimi.

automaatselt kehtetuks. Oht, et kehtetuks tunnistatud füüsilist dokumenti kuritarvitatakse või kasutatakse võltsimiseks, on tänapäevase dokumendi turvaelementide ja kehtivuse digitaalse kontrollimise võimekuse tõttu minimaalne. Seetõttu tunnistatakse lõige 5 kehtetuks.

3.2.6. Dokumendi kontrollimine (§ 1 p-d 41 ja 42)

Eelnõu § 1 punktiga 41 loetakse ITDS-i § 16 tekst lõikeks 1 ja täiendatakse paragrahvi lõikega 2.

Kui garantii- ja veamenetluses kontrollitakse dokumendi terviklikkust ning selgub, et dokument tuleb välja vahetada vea tõttu, mis ei ole tingitud dokumendi kasutajast, vaid näiteks dokumendi tootmisel tekkinud vea või praagi tõttu, antakse dokumendi kasutajale välja sama kehtivusajaga uus dokument. Muudatusega viiakse ITDS kooskõlla praktikaga.

PPA võib kasutada garantii- ja veamenetluses uue dokumendi välja andmise korral biomeetrilisi andmeid, mis on võetud väljavahetatava dokumendi taotlemisel, või võtta dokumendi kasutajalt uued biomeetrilised andmed. Seetõttu ei pea dokumendi kasutaja tingimata esitama uut fotot ega andma uusi sõrmejälgi, vaid uus dokument antakse välja samade andmetega nagu eelmine. Vajadusel võib aga PPA võtta dokumendi kasutajalt ka uued biomeetrilised andmed, näiteks kui varasem näokujutis või sõrmejäljed ei ole enam võrreldavad või kui isik soovib ise anda uued biomeetrilised andmed või kui varem ei olnud dokumendi kasutajal kohustust anda biomeetrilisi andmeid.

Garantii- ja veamenetlusi registreeriti 2021. aastal 1406, 2022. aastal 1498 ja 2023. aastal 31. oktoobri seisuga 842.

Eelnõu § 1 punktiga 42 täiendatakse ITDS-i § 17 lõikega 3². ITDS-i § 17 lõike 1 kohaselt võib PPA või KAPO põhjendatud kahtluse korral võtta dokumendi selle kehtivuse kontrollimiseks ja § 17 lõike 3 punkti 1 kohaselt anda selle kohta kasutajale allkirjastatud tõendi. PPA kohaldab seda ka garantii- ja veamenetluses dokumendi terviklikkuse kontrollimisel, kui dokument on vaja saata füüsilisse ekspertiisi. Garantii- ja veamenetluses koostab PPA menetleja garantiitaotluse, mis sisaldab samuti dokumendi kasutaja isikuandmeid, ning selle allkirjastab nii dokumendi kasutaja kui ka PPA menetleja. Samas menetluses ei ole vaja küsida andmeid kaks korda ega allkirjastada kahte tõendit. Dokumendi kasutajale antakse allkirjastatud garantiitaotlus, mis tõendab, et dokument on PPA-s. Seega täpsustatakse lõikega 3², et ITDS-i § 17 lõike 3 punktis 1 nimetatud tõendit ei anta, kui dokumendi kasutaja esitab ise dokumendi selle kehtivuse kontrollimiseks dokumendi väljaandjale.

3.2.7. mRiik (§ 1 p 43)

Eelnõu § 1 punktiga 43 täiendatakse ITDS-i § 18¹ lõikega 1¹, et luua võimalus isikusamasuse kontrollimiseks mRiigi kaudu.

mRiigis kuvatakse isikutunnistust, passi ja juhiluba ning teenuseid, mille leiab ka eesti.ee-st, näiteks andmed laste, retseptide, töövõimetuslehtede ja sõidukite kohta. Dokumentivaade on mRiigis infoteenusena sarnaselt eesti.ee-ga, st inimesele kuvatakse tema dokumendi andmed. Lisafunktsioonina võimaldab mRiik esitada isikusamasuse kontrollimiseks oma dokumendi füüsilises keskkonnas, näiteks poes oma vanuse tõendamisel. Muudatus annab mRiigi kaudu isikusamasuse kontrollimisele samaväärse õigusliku tähenduse, nagu on füüsilise dokumendi alusel isikusamasuse kontrollimisel. mRiiki sisselogimisel kasutaja autenditakse ja talle kuvatakse tema dokument. Isikusamasuse kontrollimiseks teeb teenuseosutaja dokumendi ruutkoodi, triipkoodi või lähiväljaside abil kontrollpäringu X-tee kaudu riiklikusse andmekogusse,

mis on isikutunnistuse ja passi puhul ITDAK. Dokumendi näitamisel ja valideerimisel saab dokumendi kasutaja valida, kas ta jagab teenuseosutajaga kõiki dokumendi andmeid või ainult osa, näiteks ainult sünniaega ja fotot vanuse kontrolliks või isikukoodi kliendisoodustuse saamiseks.

Muudatus on seotud Vabariigi Valitsuse tegevusprogrammi 2023–2027³¹ eesmärgiga 3.2.4 „Looma e-riigi mobiilirakenduse, mille kaudu riik jõuab informatsiooni ja teenustega personaalselt iga eestimaalasele“.

3.2.8. Digitaalsete andmete kehtivusaeg (§ 1 p-d 44 ja 61)

Eelnõu § 1 punktidega 44 ja 61 muudetakse ITDS-i § 20 lõiget 3 ja § 34³ lõiget 3. Mõlema lõike esimeses lauses on volitusnorm, mille kohaselt võib valdkonna eest vastutav minister kehtestada määrusega isikutunnistusele või elamisloakaardile kantavate digitaalsete andmete kehtivusaja. Dokumenti kantud digitaalsete andmete kehtivusaeg on sätestatud seaduse tasandil, mistõttu ei ole volitusnorme vaja. Lisaks ei tohi digitaalsete andmete kehtivusaeg kehtivate lõigete kohaselt ületada dokumendi kehtivusaega. See ei ole päris korrektne, sest seda on võimalik tõlgendada nii, et digitaalsete andmete kehtivusaeg võib olla lühem kui dokumendi kehtivusaeg. Seega täpsustatakse ka, et digitaalsete andmete kehtivusaeg on sama nagu dokumendi oma.

3.3. Dokumendi väljaandmise menetlus ja andmetöötlus

3.3.1. Isikunime dokumenti kandmine (§ 1 p-d 5 ja 6)

Eelnõu § 1 punktiga 5 muudetakse ITDS-i § 9¹ lõiget 2. Uue ID-1 formaadis dokumentide tootmise lepingu rakendamisega tekib võimalus kirjutada perekonnanimi pikemalt dokumendile välja. Praegu saab dokumenti kirjutada perekonnanimeks kuni 28 tähemärki. Kui perekonnanimi on pikem, kantakse see dokumenti nii, et nime lõpust jäetakse kirjutamata tähed, mis andmeväljale ei mahu. Muudatuse tulemusel on edaspidi võimalik nii ees- kui ka perekonnanime puhul kanda dokumenti 30 tähemärki.

Eelnõu § 1 punktiga 6 muudetakse ITDS-i § 9¹ lõiget 3. ITDS-i § 9¹ lõikes 1 on sätestatud, et kui isikunimes on võõrtähti, kantakse see dokumenti Rahvusvahelise Tsiviillennundusorganisatsiooni (ICAO) ümberkirjutusreeglite kohaselt, ja lõikes 2, et kui isikunimi ei mahu andmeväljale, jäetakse selle lõpust tähed kirjutamata. Nendel juhtudel kantakse ITDS-i § 9¹ lõike 3 kohaselt isikunimi algupärasel kujul reisidokumendi märkustehele ja kanne kinnitatakse pitsatiga. Praktikas kantakse algupärane isikunimi küll endiselt reisidokumendi märkustehele, kuid kannet ei kinnitata pitsatiga. Seetõttu jäetakse muudatusega lõikest 3 välja sõnad „ning kanne kinnitatakse pitsatiga“.

3.3.2. Dokumendi taotleja DNA-ekspertiis (§ 1 p-d 7 ja 21)

Eelnõu § 1 punktidega 7 ja 21 täiendatakse ITDS-i § 9² lõigetega 6¹–6³ ja § 11⁷ lõikega 3.

Kehtiva õiguse³² kohaselt peab dokumendi taotleja, kellele ei ole antud varem välja Eesti kodaniku passi ega isikutunnistust, lisama taotlusele Eesti kodakondsusesse kuulumise tuvastamist

³¹ Vabariigi Valitsuse 18. mai 2023. aasta korralduse nr 131 „Vabariigi Valitsuse tegevusprogrammi 2023–2027“ kinnitamine“ [lisa](#).

³² Siseministri 18. detsembri 2015. aasta määruse nr 77 „[Isikutunnistuse, elamisloakaardi, digitaalse isikutunnistuse, Eesti kodaniku passi, meremehe teenistusraamatu, välismaalase passi, ajutise reisidokumendi, pagulase](#)

võimaldava dokumendi ning oma mõlema vanema nime, kodakondsuse, isikukoodi või sünniaja ja -koha.

- 1) ITDS-i § 9² lõikega 6¹ antakse PPA-le õigus nõuda piiratud juhtudel lisaks eelnimetatud andmetele DNA-ekspertiisi. DNA-ekspertiisi võib nõuda juhul, kui isik taotleb esimest korda Eesti kodaniku dokumenti ja PPA-l tekib põhjendatud kahtlus, et välisriigis väljaantud Eesti kodakondsuse õigust tõendav dokument ei ole ehtne või selle alusandmed ei ole õiged. PPA nõuab DNA-ekspertiisi vaid üksikutel juhtudel, kui isadus on tuvastatud aastaid pärast välismaalase sünni registreerimist või vahetult enne dokumendi taotlemist ja PPA-l on alust kahelda esitatud lisaandmete õigsuses või tõendite ehtsuses. Kui välismaalane keeldub DNA-ekspertisist, keeldub PPA dokumendi väljaandmisest.

Praktikas on sagenenud olukorrad, kus Venemaa või Valgevene kodanik soovib hilisema isaduse tuvastamisega tõendada, et ta põlvneb Eesti kodanikust, kuid esitatud andmetes või tõendites on põhjust kahelda. Muudatus puudutab väga väikest rühma välismaalasi, kes esitavad PPA-le dokumendi esmataotluse, tõendades Eesti kodakondsuse õigust hilisema isaduse tuvastamise kaudu, ja kelle suhtes tekib PPA-l põhjendatud kahtlus, kas Eesti kodakondsuse õigust tõendav dokument või selle alusandmed on õiged. Selliseid juhtumeid on seni olnud kümnekond, kuid need on viimastel aastatel sagenenud. Kõik sellised juhtumid on seotud Venemaa või Valgevene kodanikega. Esitatud on nii Venemaa kohtuotsuseid kui ka isaduse tuvastamise tunnustusi. Kohtumenetluses on seni suudetud valeandmete ja -tõendite esitamist tõendada.

Kõikides senistes kohtuasjades on Eesti kodanikku mõjutatud end isaks tunnistama, kuid oli ka kohtuasi, kus oli esitatud Venemaa kohtule võltsitud volikiri ja tehtud kohtuotsus Eesti kodaniku teadmata. Kahtluse korral küsib PPA menetluses lisaandmeid ja tõendeid ning saab praegu üksnes soovitada dokumendi taotlejal esitada isaduse kohta DNA-ekspertiisi tulemus. Kui välismaalane sellest keeldub, suurendab see selgelt kahtlust, kas tal on õigus Eesti kodakondsusele ja dokumendile. Kui välismaalane ei esita lisaandmeid ega tõendeid, jätab PPA dokumendi taotluse läbi vaatamata. Dokumendi taotluse läbi vaatamata jätmise korral pöörduvad dokumendi taotlejad sageli kohtusse. Kohtumenetlus on aga riigile ressursi- ja ajamahukas. Muudatusega on võimalik säästa nii PPA kui ka kohtute ressursi.

- 2) ITDS-i § 9² lõike 6² kohaselt tellib DNA-ekspertiisi ja katab selle kulud isik. Kohtu-ekspertiisiseaduse § 11 lõike 5 alusel kehtestatava korra³³ kohaselt maksab tasuline DNA-ekspertiis 70 eurot.
- 3) ITDS-i § 9² lõikega 6³ antakse PPA-le õigus saada Eesti Kohtuekspertiisi Instituudilt DNA-ekspertiisi andmeid ja neid töödelda ning edastada Eesti Kohtuekspertiisi Instituudile DNA-ekspertiisiga seotud isiku ees- ja perekonnanime ning isikukoodi või selle puudumise korral sünniaja. DNA-ekspertiisi andmeid ei või kasutada muudes menetlustes.
- 4) ITDS-i § 11⁷ lõike 3 kohaselt jäetakse dokumendi taotlus läbi vaatamata, kui isik ei läbi PPA nõudmisel DNA-ekspertiisi 90 päeva jooksul. Muudatus puudutab väikest hulka välismaalasi, kes esitavad PPA-le Eesti kodaniku dokumendi väljaandmise esmataotluse ja soovivad tõendada Eesti kodakondsuse õigust hilisema isaduse tuvastamise kaudu. Kui

[reisidokumendi või meresõidutunnistuse väljaandmise taotlemisel esitatavate tõendite ja andmete loetelu, väljastamise kord ning väljaandmise tähtajad](#)“ § 10, § 13 lõige 1 ja § 26 lõige 1.

³³ Volitusnormi alusel ei ole veel määrust kehtestatud, kuid selle kehtestamisel viidatakse edaspidi Vabariigi Valitsuse 31. augusti 2023. aasta määruse nr 82 „[Ekspertiisiasutuses ja selle lepingupartneri tehtavate ekspertiside ja uuringute hinnad](#)“ § 1 lõike 1 punktis 3 kehtestatud hinnale.

PPA-l tekib põhjendatud kahtlus Eesti kodakondsuse õigust tõendava dokumendi või selle alusandmete õigsuses, annab PPA taotluse kohta puuduste kõrvaldamise määru, milles nõuab, et isik läbiks 90 päeva jooksul DNA-ekspertiisi. Kui selle aja jooksul ei ole isik DNA-ekspertiisi läbinud, jätab PPA dokumendi taotluse ITDS-i § 11⁷ lõike 2 alusel läbi vaatamata. 90 päeva arvestatakse alates dokumendi taotlejale puuduste kõrvaldamise määru kätetoimetamisest.

3.3.3. Isikuandmete töötlemine teavituse saamiseks (§ 1 p 8)

Eelnõu § 1 punktiga 8 täiendatakse ITDS-i § 9² lõikega 7¹. ITDS-i § 9² lõike 7 kohaselt on haldusorganil õigus töödelda ITDS-i menetlustes isikuandmeid, sealhulgas eriliiki isikuandmeid. Lõikega 7¹ antakse PPA-le selge õigus töödelda isikuandmeid ka selleks, et saata ITDS-i menetluste kohta teavitusi, näiteks dokumendi väljaandmise menetluse staatuse või kehtivuse lõpptähtaja kohta, kasutades selleks varasema dokumendi väljaandmise menetluse andmeid.

3.3.4. Dokumendi taotlemine vanglas (§ 1 p-d 14 ja 17–20)

Eelnõu § 1 punktiga 14 muudetakse ITDS-i § 11³ lõiget 3 ja § 12² lõiget 2, et asendada ITDS-is termin „vanglatöötaja“ VangS-i terminiga „vanglaametnik“. Muudatus on tehniline.

Eelnõu § 1 punktidega 17–20 muudetakse ITDS-i § 11⁵ lõikeid 4 ja 6, täiendatakse paragrahvi lõigetega 4^{1–4} ning tunnistatakse kehtetuks lõige 5.

ITDS-i § 11⁵ lõigetes 4–6 on reguleeritud dokumendi taotluse vastuvõtmist vanglas. Kinnipeetavale kohaldatakse ITDS-i §-s 7¹ sätestatud dokumendikohustuse erisust, mille kohaselt ei pea tal olema isikutunnistust, elamisloakaarti ega Eesti reisidokumendi. PPA võib aga võtta kinnipeetava dokumendi taotluse vastu vanglas juhul, kui taotlus on põhjendatud, kinnipeetav vajab vanglas viibimise ajal dokumenti piiriületuseks ja vangla direktor tõendab piiriületuse vajadust. Põhjendatud vajaduseks loetakse ka kinnipeetava vanglast vabanemist. Kui kinnipeetaval ei ole kehtivat dokumenti, võimaldatakse tal paremaks taasühiskonnastumiseks taotleda kohustuslikku dokumenti ja toimetatakse see talle tema vabanemise ajaks kätte.

1) Lõiget 4 muudetakse nii, et edaspidi ei pea PPA minema kinnipeetava taotluse vastuvõtmiseks, isiku tuvastamiseks või isikusamasuse kontrollimiseks ja biomeetriliste andmete võtmiseks vanglasse kohapeale, vaid vanglaametnik edastab kinnipeetava dokumendi taotluse PPA-le. Samuti kontrollib vanglaametnik edaspidi kinnipeetava isikusamasust ja võib võtta tema biomeetrilised andmed.

Ka praegu edastab vangla kinnipeetava allkirjastatud dokumenditaotluse PPA-le posti või e-posti teel ja kontrollib isikusamasust. PPA peab minema vanglasse vaid kinnipeetava sõrmejälgede võtmiseks. Muudatusega võimaldatakse vanglaametnikul edaspidi võtta dokumendi väljaandmise menetluses ise kinnipeetava sõrmejäljed. Vanglaametnik on läbinud daktüloskopeerimiskoolituse ning tal on vajalik pädevus, tehnilised oskused ja hõiveseadmed. Vanglas kasutatakse biomeetriliste andmete võtmiseks hõiveseadmeid, mille kaudu saab andmed edastada ABIS-esse.

2) Lõigetega 4¹ ja 4² täpsustatakse, et:

- dokumendi väljaandmise menetluses biomeetriliste andmete võtmisel kohaldab vanglaametnik ITDS-i § 15 lõike 6 alusel kehtestatud sõrmejälgede võtmise korda³⁴;
- vanglaametniku võetud kinnipeetava biomeetrilised andmed kantakse ABIS-esse.

³⁴ Siseministri 30. novembri 2015. aasta määrus nr 56 „[Elamisloa ja elamisõiguse menetluses ning isikut tõendava dokumendi väljaandmise menetluses sõrmejälgede võtmise kord](#)“.

- 3) Sõrmejälgede võtmine dokumendi väljaandmise menetluses saab võimalikuks tänu ABIS-e valdkonnaülesele rakendamisele, kuid eeldab infotehnoloogilisi arendustöid. Seega luuakse lõike 4 muudatusega õiguslik võimalus, mida saab hakata kohaldama pärast arendustöid. Arendustööd peaksid valmima hiljemalt 2025. aasta lõpuks. Seetõttu jäetakse lõikega 4³ PPA-le alles võimalus võtta kinnipeetava biomeetrilised andmed vanglas.

Kinnipeetava dokumendi taotlusi ei ole palju: 2023. aastal on neid augusti lõpu seisuga olnud 89.

- 4) Lõige 5 tunnistatakse kehtetuks, kuna see kordab sisult lõiget 4. ITDS-i § 11⁵ lõigete 4–6 algeesmärk oli reguleerida eraldi kohustusliku isikutunnistuse ja elamisloakaardi (lg 4) ning piiriületuseks reisidokumendi (lg-d 5 ja 6) taotlemist. Kehtiv lõige 5 jõustus 1. jaanuaril 2011, kui Euroopa Liidus võeti kasutusele elamisloakaart. Siis asendati sõna „reisidokument“ sõnaga „dokument“, nagu on lõikes 4. Kuivõrd praegu on võimalik reisida Euroopa Liidu ja Schengeni konventsiooni liikmesriikides ka isikutunnistusega ning arvestades, et eelnõuga soovitakse anda dokumendi taotlejale võimalus valida kohustuslikuks dokumendiks ka pass, ei ole vaja säilitada nii lõiget 4 kui ka 5. Seega tunnistatakse lõige 5 kehtetuks.
- 5) Lõiget 6 muudetakse nii, et edaspidi võtab PPA kinnipeetava dokumendi taotluse vastu juhul, kui vanglaametnik lisab taotlusele põhjendatud kinnituse kinnipeetava vajaduse kohta dokumenti taotleda. Kehtivas lõikes on, et juhul, kui kinnipeetav taotleb dokumenti piiriületuseks, annab põhjendatud kinnituse dokumendi vajaduse kohta vangla direktor. Arvestades, et kinnipeetaval on võimalik taotleda dokumenti ka vabanemise korral, ei ole põhjendatud siduda kinnitus vajadusega ületada riigipiiri. Samuti, kuna kinnipeetava vajadust dokumenti taotleda tuleb edaspidi põhjendada igal juhul ja kinnipeetavaga suhtleb otse vanglaametnik, oskab dokumendi taotlemise vajadust hinnata ja põhjendada kõige paremini just vanglaametnik. Seega ei ole otstarbekas koormata dokumendi taotlemise vajaduse kinnitamisega vangla direktorit.

3.3.5. Volitatud esindaja määramine dokumendi taotluse menetlemise ajal (§ 1 p 22)

Eelnõu § 1 punktiga 22 muudetakse ITDS-i § 12¹ lõiget 2¹. Kehtiva lõike kohaselt on dokumendi taotlejal võimalik määrata dokumendi kättesaamiseks volitatud esindaja vaid dokumendi taotlemisel. Muudatusega võimaldatakse edaspidi määrata volitatud esindaja ka dokumendi taotluse menetluse ajal. Praktikast on väga sagedased olukorrad, kui volitamise vajadus selgub hiljem ja dokumendi taotlejal võib erinevatel põhjustel olla keeruline minna ise dokumendile järele, kuid seda on reisimiseks, e-teenuste kasutamiseks või digiallkirjastamiseks viivitamata vaja. Ka vanematel või maal elavatel inimestel on sageli keeruline minna ise dokumendile järele ja hilisem volitamine loob paindliku võimaluse lubada enda esindajal tuua dokument koju kätte. Dokumendi taotleja edastab dokumendi väljaandjale lihtkirjaliku volituse, milles volitab oma esindajat dokumenti vastu võtma. Dokumendi taotleja esindaja peab dokumendile järele minnes esitama dokumendi väljaandjale enda kehtiva dokumendi.

3.3.6. Dokumendi väljastamine (§ 1 p-d 23–26 ja 58) ja väljaandja termin (§ 1 p-d 29 ja 31)

Eelnõu § 1 punktidega 23 ja 24 muudetakse ITDS-i § 12¹ lõikeid 2² ja 2⁴. Lõigetest jäetakse välja sõnad „posti teel“ ja „postiteenuse pakkuja“ ning asendatakse need terminiga „turvalise teenuse osutaja“.

Dokumendi väljastamisel peab olema tagatud, et see antakse vahetult üle vaid selle vastu võtmise õigusega isikule ega jäeta järelevalveta postkasti. Sõnad „posti teel“ ja „postiteenuse

pakkuja“ võivad jätta vale mulje võimalikust kättetoimetamise viisist. PPA toimetab välismaal elavatele Eesti kodanikele reisidokumente kätte kullerteenuse osutaja vahendusel. Turvalise teenuse osutaja valib PPA riigihankega. Uue ID-1 formaadis dokumentide tootmise lepingu rakendamise saab võimalikuks ka ID-1 formaadis dokumentide kulleriga kättetoimetamine ja siis toimetatakse dokumente kulleriga kätte nii välismaal kui ka Eestis. Seetõttu on regulatsiooni täpsustamine vältimatult vajalik.

Eelnõu § 1 punktiga 25 täiendatakse ITDS-i § 12¹ lõikega 2⁶. Uue ID-1 formaadis dokumentide tootmise lepingu rakendamine 1. novembrist 2025 toob dokumendi väljaandmise menetluses kaasa mitmeid uuendusi. Lõikega 2⁶ võetakse uue lepingu rakendamise järel³⁵ kasutusele mugav lahendus, mille abil saab dokumendi taotleja, autentides end elektroonilises keskkonnas kehtiva eID-vahendiga³⁶, aktiveerida ise oma dokumendi ja sertifikaadid. Seega, kui näiteks välismaal elaval Eesti elanikul on kehtiv eID-vahend, ei pea ta enam minema dokumendi kättesaamiseks isiklikult Eesti välisesindusse kohale, vaid dokumendi toimetab talle kätte näiteks kuller ning dokument ja sertifikaadid aktiveeritakse ning sertifikaatide turvakoodid toimetatakse kätte elektrooniliselt.

Eelnõu § 1 punktidega 26 ja 58 muudetakse ITDS-i § 12¹ lõikeid 3 ja 4 ning § 20¹⁵ lõiget 4, mille kohaselt tuleb praegu 15–17-aastase dokument väljastada talle isiklikult, mitte tema seadusliku esindaja kaudu, välja arvatud juhul, kui ta on taotlemise ajal andnud selleks volituse. ITDS-i § 10 lõikes 3 on sätestatud, et vähemalt 15-aastane võib teha ITDS-is sätestatud menetsustoiminguid iseseisvalt. ITDS-i § 12¹ lõiked 3 ja 4 ning § 20⁵ lõige 4 on aga imperatiivsed. Kuigi 15-aastaselt on Eesti õiguse kohaselt piiratud teovõime, ei ole dokumendi väljastamiseks isiklikult kohale ilmumise nõue selles vanuserühmas põhjendatud ja on tekitanud praktikas segadust. Muudatusega ühtlustatakse regulatsiooni nii, et edaspidi kohaldatakse ka 15–17-aastase dokumendi väljastamisel ITDS-i § 10 lõiget 3 ning dokumendi võib väljastada 15–17-aastasele isiklikult või tema seaduslikule esindajale.

Eelnõu § 1 punktidega 29 ja 31 muudetakse ITDS-i § 13¹, § 14 lõikeid 2 ja 4, § 17 lõike 3 punkti 3 ning § 25 lõiget 2, et võtta ITDS-is kasutusele termin „dokumendi väljaandja“ seniste erinevate terminite asemel. Muudatus on tehniline.

3.3.7. Välismaalase passi väljaandmise alus (§ 1 p-d 59 ja 60)

Eelnõu § 1 punktidega 59 ja 60 muudetakse ITDS-i § 27 lõiget 3 ja täiendatakse paragrahvi lõikega 4.

ITDS-i §-s 27 on reguleeritud välismaalase passi väljaandmise alust. Selle lõike 1 kohaselt on õigus anda välismaalase pass välja välismaalasele, kellel on kehtiv Eesti elamisluba või -õigus, kui on tõendatud, et välismaalasel puudub välisriigi reisidokument ja tal ei ole võimalik seda saada. Lisaks saab kehtiva lõike 3 alusel anda välismaalase passi välja välisriigi kodanikule, kes esitab oma kodakondsusriigi pädeva ametiasutuse nõusoleku talle välismaalase passi väljaandmise kohta või tõendab, et nõusolekut ei ole võimalik saada.

Lõiget 3 muudetakse ja paragrahvi täiendatakse lõikega 4 nii, et edaspidi ei nõuta kodakondsusriigi pädeva ametiasutuse nõusolekut vaid välisriigi kodanikult, kes on täiendava kaitse saaja VRKS-i § 4 lõike 3 tähenduses. Eesmärk on täpsustada välismaalase passi saajate sihtrühma. Eestis viibivale välismaalasele, kes vajab reisimiseks dokumenti, kuid kellele ei kohaldata

³⁵ Muudatus eeldab vähemalt kuuekuulist arendusaega pärast ID-1 formaadis dokumentide tootmise lepingu rakendamist.

³⁶ Isikutunnistus, elamisloakaart ja digitaalne isikutunnistus, sealhulgas mobiil-ID.

välismaalase passi regulatsiooni ja kes ei saa oma kodakondsusriigi reisidokumenti, on võimalik anda välja ajutine reisidokument.

2023. aasta augusti seisuga on kehtivaid välismaalase passe 52 678. Ajutisi reisidokumente antakse aastas välja umbes 150.

3.3.8. Isiku daktüloskopeerimine tagasipöördumisdokumendi taotlemise korral (§ 1 p-d 62–64)

Eelnõu § 1 punktidega 62–64 täiendatakse ITDS-i § 35 lõikega 5, § 36¹ lõikega 3 ja § 36⁴ lõikega 3.

ITDS-i § 11⁶ lõike 3 kohaselt daktüloskopeeritakse dokumendi taotleja taotluse esitamisel. Seega tuleks kõik dokumendi taotlejad daktüloskopeerida. Erand on diplomaatilise isikutunnistuse taotleja (ITDS-i § 20¹⁵ lg 3) ja sõrmejäljekujutisteta Eesti kodaniku passi taotleja juhul, kui on täidetud ITDS-i § 21¹ lõikes 1 sätestatud tingimused (ITDS-i § 21¹ lg 3).

Uute lõigetega sätestatakse, et dokumendi taotleja daktüloskopeerimise nõue ei kehti ka juhul, kui taotleja taotleb tagasipöördumistunnistust, tagasipöördumise luba või Euroopa Liidu tagasipöördumistunnistust, sest praktikas ei daktüloskopeerita nende taotlejaid ka praegu. Sellised dokumendid antakse välja paberil ja neile ei kanta andmeid digitaalselt. Neile kleebitakse foto. Need on dokumendid, mis antakse välja erandolukorras, näiteks kui inimene on reisil olles oma dokumendi ära kaotanud või dokument on rikutud. Nende dokumentide väljaandmise menetlus kestab üldjuhul kolm tööpäeva ja nende taotlemiseks ei pea inimene minema tingimata Eesti välisesindusse isiklikult kohale. Sageli antakse tagasipöördumistunnistus, tagasipöördumise luba ja Euroopa Liidu tagasipöördumistunnistus välja ka ootetöona. Eesti välisesindusse on sellise dokumendi taotlejal vaja minna üksnes selle kättesaamiseks.

3.4. Andmete töötlemine riiklikes andmekogudes

Eelnõu § 1 punktidega 34–40, §-ga 2, § 3 punktidega 1 ja 2 ning §-dega 4, 5 ja 7–10 muudetakse ITDS-i §-e 15² ja 15⁴, KodS-i §-e 2¹ ja 2⁴, KonS-i §-e 12¹ ja 48, KrMS-i § 109², PPVS-i 3. peatükki, VangS-i § 5⁵, VRKS-i § 13⁷, VSS-i §-e 33, 33¹, 33¹⁴ ja 33¹⁵ ning VTMS-i § 31⁶, tuues muu hulgas põhimäärusest seaduse tasandile andmekogudes andmete säilitamise maksimaalse tähtaja ning nende andmete koosseisu, mida töödeldakse ABIS-ses, Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogus, Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogus, ITDAK-is ning sissesõidukeeldude riiklikus registris.

3.4.1. ITDAK-i andmekoosseis ja ITDAK-i andmete säilitamise tähtjad (§ 1 p-d 34–38)

Praegu on ITDAK-i täpne andmekoosseis sätestatud ITDAK-i põhimääruses³⁷. Samuti on ITDAK-i andmete säilitamise tähtjad sätestatud ITDAK-i ja ABIS-e põhimääruses³⁸. Dokumendi väljaandmise menetluses võetud biomeetrilised andmed kantakse ITDAK-i kaudu ABIS-esse, kus neid ka säilitatakse (vt seletuskirja p 3.4.2).

Andmete säilitamise maksimaalse tähtaja määramisel tuleb lähtuda sellest, kui kaua on neid vaja selle eesmärgi täitmiseks, milleks need koguti. ITDAK-i pidamise eesmärk ei ole vaid

³⁷ Siseministri 18. detsembri 2015. aasta määrus nr 78 „[Isikut tõendavate dokumentide andmekogu pidamise põhimäärus](#)“.

³⁸ Vabariigi Valitsuse 23. detsembri 2021. aasta määrus nr 125 „[Automaatse biomeetrilise isikutuvastuse süsteemi andmekogu põhimäärus](#)“.

menetleda dokumendi taotlusi, vaid tagada ka avalik kord ja riigi julgeolek, võimaldades tuvastada riikliku identiteedi saanud. ITDAK on üks riigi peamine andmekogu, mille andmetele tuginevad nii riigiasutused, notarid ja muud vabade kutsete esindajad kui ka erasektor.

Kuna ITDAK-i andmeid on vaja kasutada läbi kogu inimese elu ning teatud juhtudel ka pärast tema surma, näiteks põlvnemis- ja kodakondsusküsimustes või identiteedikonflikti lahendamisel, säilitatakse ITDAK-i andmeid **kõige kauem alaliselt** ITDAK-i kandmisest arvates. Alaliselt säilitatakse vaid Eesti kodaniku dokumendi esmataotlemisel kogutud andmeid, kuna isiku sünnijärgne Eesti kodakondsus määratletakse Eesti kodaniku passi ja/või isikutunnistuse väljaandmise menetluses, mille andmeid töödeldakse ITDAK-is. Selleks, et tagada õigus Eesti kodakondsusele ka mitmenda põlve järeltulijale, on vaja neid andmeid säilitada alaliselt. Kui ITDAK-i andmeid säilitada lühemalt, ei ole võimalik ITDAK-i pidajal täita selle pidamise põhieesmärgi tagada avalik kord ja riigi julgeolek. **Muude ITDAK-i andmete säilitamise tähtajad on lühemad** ja need kehtestatakse ITDAK-i põhimääruses.

Isikuandmete säilitamist käsitatakse eraelu puutumatusena. Konkreetse säilitustähtaja sätestamine seaduse tasandil aitab kaasa läbipaistvale andmetöötlusele. Eelnõuga sätestatakse ITDS-is ka ITDAK-i andmekoosseis, mis on praegu ITDAK-i põhimääruses. Seega ei ole andmekoosseisu ITDS-is sätestamisel andmesubjekti õigustele vahetut mõju. Edaspidi on andmesubjektil võimalik saada ITDS-i lugedes aru, et andmeid, mille ta on dokumendi taotluses esitanud, töödeldakse ITDAK-is. Andmekoosseisu seaduse tasandil kehtestamisega ei muutu asjaolu, et isikuandmeid töödeldakse jätkuvalt seaduses sätestatud alusel ehk isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti e tähenduses. Samuti ei muutu andmete töötlemise laad, ulatus, kontekst ega eesmärk isikuandmete kaitse üldmääruse artikli 35 lõike 1 tähenduses.

3.4.2. ABIS-e andmete säilitamise tähtajad (§ 1 p-d 39 ja 40, § 2 p-d 7 ja 8, § 3 p-d 1 ja 2, §-d 4, 7 ja 8, § 9 p-d 13 ja 14 ning § 10)

- 1) **ITDS-i** alusel ITDAK-i kaudu ABIS-esse kantud andmeid säilitatakse **kuni 75 aastat**. ABIS-e andmete säilitamise tähtajad võivad olla ka lühemad ja need kehtestatakse ABIS-e põhimääruses. ABIS-e põhimääruse § 38 lõikes 1 on täpsustatud, et fotot või näokujutist ja sõrmejälgi säilitatakse aktiivselt 15 aastat, pärast mida kantakse need ABIS-e arhiivi, kus neid säilitatakse 50 aastat. ABIS-e põhimäärusest on kavas pärast eelnõu jõustumist muuta, et kehtestada nende andmete maksimaalseks säilitustähtajaks 75 aastat.
- 2) **KodS-i** alusel ABIS-esse kantud andmeid võib säilitada **alaliselt**. ABIS-e põhimääruse § 40 lõikes 1 on täpsustatud, et neid andmeid säilitatakse aktiivselt 20 aastat, pärast mida kantakse need ABIS-e arhiivi, kus neid säilitatakse alaliselt. KodS-i alusel ABIS-esse kantud andmeid peab säilitama alaliselt, kuna need võivad olla asjakohased ka pärast inimese surma. ABIS-es hoitakse biomeetrilisi andmeid kõigi inimeste kohta, kes on saanud Eesti kodakondsuse naturalisatsiooni korras, kelle Eesti kodakondsus on taastatud või kes on Eesti kodakondsuse kaotanud.

Eesti peab teadma, kes on tema kodanikud, sest Eesti Vabariigi põhiseaduse §-s 8 on sätestatud kodakondsuse alusena põhimõte, et igal lapsel, kelle vanematest üks on Eesti kodanik, on õigus Eesti kodakondsusele sünnilt. Et kellegi kodakondsuse üle otsustada, on oluline teada, kas tema vanemad olid tema sünni ajal Eesti kodanikud. Andmed Eesti kodakondsuse saamise, taastamise või kaotamise kohta on olulised ka pärast inimese surma, et hiljem määrata tema järeltulijate staatus. Eesti kodaniku laps saab samuti Eesti kodakondsuse. Kuna Eesti kuulub Euroopa Liitu, omandab Eesti kodanik ka Euroopa Liidu

kodaniku õigused. Seega on kodakondsuse andmete säilitamine ühtlasi kodanikkonna kujunemise ajaloo säilitamine praegusest põlvkondi edasi. Kõiki KodS-i alusel ABIS-esse kantud andmeid ei edastata rahvastikuregistrile, mistõttu on samuti oluline säilitada andmeid alaliselt. Lisaks on Rahvusarhiiv kuulutanud Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu toimikud arhiiviväärtuslikuks ning neid säilitatakse riigiarhiivis.

- 3) **KonS-i** alusel ABIS-esse kantud andmeid säilitatakse **neli kuud** pärast dokumendi taotluse edastamist PPA-le. Enne ABIS-e kasutusele võtmist kanti need andmed konsulaarametniku ametitoimingute ja diplomaatiliste passide andmekogusse, kus neid säilitati samuti neli kuud pärast dokumendi taotluse edastamist PPA-le.
- 4) **KrMS-i, VangS-i ja VTMS-i** alusel ABIS-esse kantud andmeid säilitatakse **kuni 75 aastat** ABIS-esse kandmisest arvates. Lühema säilitustähtaja võib kehtestada ABIS-e põhimääruses. Kõnealuseid andmeid töödeldi varem riiklikus sõrmejälgede registris (edaspidi *RSR*). *RSR* ja riiklik DNA-register ühendati riiklikuks süüteomenetluse biomeetriaregistriks (edaspidi *RSBR*). ABIS-e biomeetrilisi andmeid peab olema võimalik viia kokku *RSBR*-i biograafiliste andmetega kogu nende töötlemise jooksul. See on vajalik, et täita andmete kogumise eesmärki. *RSBR*-i biograafilised andmed ja ABIS-e andmed võetakse samas menetluses ning ka nende säilitamise tähtajad on samad. **KrMS-i, VangS-i ja VTMS-i** alusel ABIS-esse kantud andmete säilitamise regulatsioon ühtib kohtuekspertiisiseaduses ja *RSBR*-i põhimääruse³⁹ §-s 16 sätestatud andmete säilitamise regulatsiooniga.
- 5) **VRKS-i** alusel ABIS-esse kantud andmeid säilitatakse **kuni 50 aastat**. Säilitustähtaja määramisel on lähtunud vajadusest tagada riigi julgeolek ja siseturvalisus, kuivõrd Eestis suureneb iga aastaga rahvusvahelise kaitse taotlejate arv. Rahvusvahelise kaitse taotlejaid kontrollivad põhjalikult Eesti pädevad asutused. Oluline on tuvastada välismaalane nii riigipiiril kui ka järgnevates menetlustes. Tuleb arvestada, et välismaalase kohta, kes reisib või saabub Euroopa Liitu, sealhulgas Eestisse, ebaseaduslikult või varjupaigataotlejana, ei ole Eestil sageli rohkem andmeid, kui välismaalase ütlused enda päritolu kohta, tema esitatud dokumendid ja foto ning temalt võetud sõrmejäljed. Sellisel välismaalasel on õigus esitada perekonna taasühendamise taotlusi ja korduvtaotlusi ning elamisloa taotlusi eri alustel.

Et vältida varjupaigasüsteemi kuritarvitamist ning tagada välismaalase ja temaga seotud isiku tuvastamine, arvestades vajadust tagada riigi julgeolek ja siseturvalisus, on oluline välismaalase kohta kogutud andmeid säilitada võimalikult kaua. Andmete pikk säilitamine tagab, et õiguskaitse- ja julgeolekuasutustel on piisavad võimalused julgeolekuohtude ennetamiseks ning avastamiseks. Kuna **VRKS-i** alusel ABIS-esse kantud andmete säilitamise tähtaeg on sätestatud **VRKS-i** § 13⁷ lõikes 7¹, tuleb eelnõu §-ga 8 jätta sama paragrahvi lõikest 7 välja osa, mille kohaselt nähakse ABIS-e andmete säilitamise tähtaeg ette ABIS-e põhimääruses.

- 6) **VSS-i** alusel alalise sissesõidukeelu kohaldamise menetluses **sissesõidukeeldude riikliku registri** kaudu ABIS-esse kantud alalise sissesõidukeelu andmeid säilitatakse **alaliselt**. Tähtajalise sissesõidukeelu andmeid säilitatakse aktiivselt **kümme aastat** pärast tähtajalise sissesõidukeelu tähtaja lõppemist, pärast mida need arhiveeritakse. Arhiveeritud andmeid säilitatakse **40 aastat**.

³⁹ Vabariigi Valitsuse 28. septembri 2023. aasta määrus nr 87 „[Riikliku süüteomenetluse biomeetriaregistri põhimäärus](#)“.

VSS-i alusel **Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu** kaudu ABIS-esse kantud andmeid säilitatakse aktiivselt **kümme aastat** välismaalase lahkumiskohustuse täitmise päevast arvates, pärast mida need arhiveeritakse. Arhiveeritud andmeid säilitatakse **40 aastat**.

VSS-i § 33¹⁵ lõike 7¹ kohaselt võib VSS-i alusel ABIS-esse kantud andmeid säilitada alaliselt. Eelnõu § 9 punktiga 14 täpsustatakse, et lühema säilitustähtaja võib näha ette ABIS-e põhimääruses. Kuna VSS-i alusel ABIS-esse kantud andmete säilitamise tähtaeg on sätestatud VSS-i § 33¹⁵ lõikes 7¹, tuleb eelnõu § 9 punktiga 13 jätta sama paragrahvi lõikest 7 välja osa, mille kohaselt nähakse ABIS-e andmete säilitamise tähtaeg ette ABIS-e põhimääruses.

3.4.3. Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu andmekoosseis ja andmete säilitamise tähtajad (§ 2 p-d 3–6)

Praegu on Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu täpne andmekoosseis ja andmete säilitamise tähtajad sätestatud andmekogu põhimääruses⁴⁰. Isikuandmete säilitamist käsitatakse eraelu puutumatusena. Konkreetse säilitustähtaja sätestamine seaduse tasandil aitab kaasa läbipaistvale andmetöötlusele. Eelnõuga sätestatakse Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu täpne andmekoosseis ja andmete säilitamise maksimaalne tähtaeg KodS-is. Andmekoosseisu ja andmete säilitamise tähtaja KodS-is sätestamisel ei ole andmesubjekti õigustele vahetut mõju. Sellega ei muutu asjaolu, et isikuandmeid töödeldakse jätkuvalt seaduses sätestatud alusel ehk isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti e tähenduses. Samuti ei muutu andmete töötlemise laad, ulatus, kontekst ega eesmärk isikuandmete kaitse üldmääruse artikli 35 lõike 1 tähenduses.

3.4.4. Sissesõidukeeldude riikliku registri ning Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu andmekoosseis ja andmete säilitamise tähtajad (§ 9 p-d 5–7 ja 10–12)

Eelnõu § 9 punktidega 5–7 muudetakse VSS-i § 33 lõikeid 3 ja 8 ning täiendatakse paragrahvi lõigetega 8¹ ja 8². **Punktidega 10–12** muudetakse VSS-i § 33¹⁴ lõikeid 3 ja 7 ning täiendatakse paragrahvi lõikega 7¹. Muudatustega sätestatakse VSS-is nende andmete koosseis ja säilitamise tähtajad, mida töödeldakse sissesõidukeeldude riiklikus registris (VSS-i § 33) ning Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogus (VSS-i § 33¹⁴). Lisaks säilitatakse **punktidega 6 ja 11** võimalus täpsustada nende andmekogude andmekoosseisu andmekogude põhimäärustes, arvestades VSS-is sätestatud andmekoosseisu.

Välismaalasele võib kohaldada sissesõidukeeldu erinevatel eesmärkidel.

- Rahvusvahelise sanktsioonina võib sissesõidukeeld olla **välispoliitiline meede**, et toetada rahu säilitamist või taastamist, rahvusvahelist julgeolekut, demokraatiat ja õigusriigi põhimõtet, inimõiguste ja rahvusvahelise õiguse järgimist või muude Ühinenud Rahvaste Organisatsiooni põhikirja või Euroopa Liidu ühise välis- ja julgeolekupoliitika eesmärkide saavutamist.
- Sissesõidukeeldu võib kohaldada välismaalasele karistusseadustiku alusel **lisakaristuse** juhul, kui välismaalane on mõistetud süüdi tahtlikult toime pandud kuriteo eest ja teda on karistatud vangistusega.

⁴⁰ Siseministri 18. detsembri 2015. aasta määrus nr 75 „[Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu põhimäärus](#)“.

- Sissesõidukeeldu võib kohaldada välismaalasele ka **tõkendina**, et vältida tema Eestisse saabumist või siin viibimist avaliku korra või riigi julgeoleku kaalutlustel.
- Lisaks tuleb sissesõidukeeldu kohaldada Eestis **ebaseaduslikult viibivale kolmanda riigi kodanikule**, keda on ettekirjutusega kohustatud Eestist lahkuma.

Sissesõidukeeldude riiklik register

Sõltumata sissesõidukeelu kohaldamise eesmärgist kantakse kõik sissesõidukeelu kohaldamise andmed sissesõidukeeldude riiklikusse registrisse. Kui välismaalasele kohaldatakse Schengeni sissesõidukeeldu, luuakse Schengeni infosüsteemis sissesõidukeeldude riikliku registri andmete alusel automaatselt sissesõidukeeldu käsitlev hoiatusteade vastavalt määrusele (EL) 2018/1861. Schengeni infosüsteemist saavad liikmesriikide pädevad piiri- ja immigratsiooniasutused kontrollida, kas kolmanda riigi kodanik, kes Schengeni alale siseneb või siin viibib, täidab Schengeni piirieskirjades⁴¹ sätestatud sisenemis- ja viibimisnõudeid. Kui kolmanda riigi kodanikule on kohaldatud Schengeni sissesõidukeeldu, on see alus keelduda teda riiki lubamast või tunnistada tema viibimisõigus või elamisluba kehtetuks ja saata ta riigist välja.

Seetõttu töödeldakse sissesõidukeeldude riiklikus registris andmeid, mis on vajalikud, et tuvastada, kas välismaalasel, kes soovib Eestisse siseneda või siin viibida, on kehtiv sissesõidukeeld. Lisaks töödeldakse sissesõidukeeldude riiklikus registris andmeid, mis on vajalikud, et luua määruse (EL) 2018/1861 alusel sissesõidukeeldu käsitlev hoiatusteade ja seda ajakohastada. VSS-i § 27¹ lõike 1 kohaselt võib sissesõidukeeld olla alaline või tähtajaline. Andmeid, mis kantakse sissesõidukeeldude riiklikusse registrisse alalise sissesõidukeelu kohaldamise menetluses, säilitatakse alaliselt. Tähtajalise sissesõidukeelu andmeid säilitatakse aktiivselt kümme aastat pärast tähtajalise sissesõidukeelu tähtaja lõppemist, pärast mida need arhiveeritakse. Arhiveeritud andmeid säilitatakse 40 aastat.

Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu

Andmed, mida töödeldakse Eestis seadusliku aluseta viibiva ja viibinud välismaalase Eestis viibimise ja Eestist lahkumise kohustuse täitmise seotud menetluses, toetavad samuti Schengeni infosüsteemi pidamise eesmärkide täitmist. Määruse (EL) 2018/1860 kohaselt tuleb sarnaselt Schengeni sissesõidukeelu kohaldamisele luua Schengeni infosüsteemis tagasisaatmist käsitlev hoiatusteade, kui ebaseaduslikult riigis viibivale välismaalasele on tehtud lahkumissettekirjutus, millega kohustatakse teda Euroopa Liidust lahkuma. Määruse (EL) 2018/1860 artiklis 4 on sätestatud, mis andmete põhjal tagasisaatmist käsitlev hoiatusteade luuakse. Kuigi tagasisaatmist käsitleva hoiatusteade andmehulk on üsna piiratud, peab Euroopa Liidu liikmesriik vajadusel olema valmis teise liikmesriigi palvel edastama ka muid andmeid, mis on kogutud välismaalase Eestis viibimise ja Eestist lahkumise kohustuse täitmise seotud menetluses.

Seadusliku aluseta Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu andmeid säilitatakse aktiivselt kümme aastat välismaalase lahkumiskohustuse täitmise päevast arvates, pärast mida need arhiveeritakse. Arhiveeritud andmeid säilitatakse 40 aastat.

3.4.5. Piirikontrolli andmekogu biomeetriliste andmete võrdlemine (§ 5 p 1)

Euroopa Liidu liikmesriikide vaheliste sisepiiride ja Euroopa Liidu välispiiride ületamisele kohaldatakse Schengeni piirieskirju. Pärast seda, kui Eesti ühines Schengeni alaga 2007. aasta

⁴¹ Euroopa Parlamendi ja nõukogu 9. märtsi 2016. aasta määrus (EL) 2016/399, mis käsitleb isikute üle piiri liikumist reguleerivaid liidu eeskirju (Schengeni piirieskirjad). – [ELT L 77, 23.3.2016, lk 1–52](#).

lõpus maismaa- ja merepiiril ning 2008. aasta algul õhupiiril, avanes isikutel võimalus ületada riigipiiri ilma piirikontrollita liikmesriikidevahelistel riigipiiridel ehk sisepiiridel. Usaldust sisepiirideta ala toimimisse peab tagama tõhus piirikontroll välispiiridel ja välispiiride valve. Schengeni piirieskirjade järgi peab piirikontroll aitama võidelda ebaseadusliku sisserände ja inimkaubandusega ning vältida ohtu liikmesriikide sisejulgeolekule, avalikule korrale, rahvatervishoiule ja rahvusvahelistele suhetele.

Kuna rändevoog Euroopa Liidu välispiiridel on üha suurenenud ja suureneb ka edaspidi, on üha olulisem tagada välispiiride tõhus valve ja piirikontrolli kvaliteet. Rändevoogu suurenemist arvestades tuleb piiripunktides piiriületajate paremaks kontrollimiseks ja tuvastamiseks võtta kasutusele kaasaegne ajasäästlik tehnoloogia, mis toetab piirikontrolli. Üha enam kasutatakse piiriületaja biomeetrilisi andmeid: sõrmejälgi ja näokujutist. Selleks on muudetud Schengeni piirieskirju ja võetud vastu uusi õigusakte või muudetud kehtivaid õigusakte, milles on reguleeritud muu hulgas piirikontrolli toetavaid IT-süsteeme: riiki sisenemise ja riigist lahkumise süsteemi, viisainfosüsteemi ja Schengeni infosüsteemi.

Piirivalve kasutab Eesti välispiiril piirikontrolliks piirikontrolli andmekogu (edaspidi *PIKO*). PIKO toetub biomeetriliste andmete võrdlemiseks teistele andmekogudele, sest PIKO-l ei ole tehnilist võimekust biomeetrilisi andmeid võrrelda.

Eelnõu § 5 punktiga 1 täiendatakse PPVS-i §-ga 19², mille lõikes 2 sätestatakse, et PIKO kasutab ABIS-e tehnilist lahendust, et võrrelda piirikontrollis PIKO-sse kantud biomeetrilisi andmeid. Samuti sätestatakse lõikes 3, et piirivalvur võib PIKO kaudu kasutada isiku tuvastamiseks või isikusamasuse kontrollimiseks ka ABIS-e andmeid. Lõike 4 kohaselt kustutatakse need andmed PIKO-st ja ABIS-est pärast isiku piiriületuse kohta otsuse tegemist.

Schengeni piirieskirjade artikli 6 lõike 1 punkti f kohaselt annab välispiiri ületaja biomeetrilised andmed, kui see on nõutud selleks, et:

- 1) koostada isiklik toimik riiki sisenemise ja riigist lahkumise süsteemis;
- 2) teha piiril isiku tuvastamiseks või isikusamasuse kontrollimiseks päringuid asjaomastesse andmekogudesse, eelkõige Schengeni infosüsteemi ja viisainfosüsteemi;
- 3) võrrelda reisidokumendi näokujutist või sõrmejäljekujutisi piiriületaja tegeliku näo või sõrmejälgedega.

Eelnõuga ei reguleerita PPVS-is riiki sisenemise ja riigist lahkumise süsteemis isikliku toimiku loomist, kuna selleks on PPVS-is õiguslik alus juba olemas. Küll aga tuleb õigusselguseks reguleerida biomeetrilist võrdlusuuringut selliste Euroopa Liidu andmekogudega, millesse tehtud päringu tulemus ei ole lõplik, vaid võimalik tabamus.

Schengeni infosüsteemi kasutamist piirikontrolli valdkonnas on reguleeritud määruses (EL) 2018/1861. Selle artikli 33 lõike 2 kohaselt tuleb teha isiku tuvastamiseks daktüloskoopiliste andmete ehk sõrmejälgedega päring, kui isikusamasust ei saa kindlaks teha muul viisil. Artikli 3 punkti 8 järgi käsitatakse päringutabamusena biomeetriliste andmete võrdlemise tulemust, kui selle on kinnitanud kooskõlas riigisiseste menetlustega pädev asutus ehk PPA.

Näide. Eestisse soovib siseneda välismaalane, kes esitab välispiiril reisidokumendi, mille foto ei ühti tema välimusega. Välismaalane ütleb oma nime, kuid tähtnumbriline päring andmekogudes on tulemusteta. PPA võtab välismaalase tuvastamiseks sõrmejäljekujutised, kannab need PIKO-sse ja võrdleb ABIS-e võrdlusmootorit kasutades neid sõrmejäljekujutistega reisidokumendi kiibil. Reisidokumendi kiibi sõrmejäljekujutised ei ühti välismaalasel võetutega. PPA teeb päringu andmekogudesse ja saab Schengeni infosüsteemist

võimaliku tabamuse. Tabamuse kontrollimiseks tuleb välismaalaselt võetud sõrmejäljekujutisi ja Schengeni infosüsteemi võimalikku tabamust võrrelda ABIS-e võrdlusmootori abil. Alles siis võib väita, et välismaalane on või ei ole tõsikindlalt tuvastatud.

Põhjalik kontroll riiki sisenemisel ja riigist lahkumisel tuleb läbida ainult kolmanda riigi kodanikel. Muudatus ei puuduta Eesti ja muude Euroopa Liidu liikmesriikide kodanikke. Oluline on ka, et ABIS-e andmeid PPVS-i § 19² lõike 2 kohases võrdlusuuringus ei töödelda.

Samuti on Schengeni piireeskirjade kohaselt kohustuslik teha päringud Schengeni infosüsteemi, viisainfosüsteemi ning INTERPOL-i varastatud, kaotatud ja kehtetuks tunnistatud isikut tõendavate dokumentide andmebaasi.

Schengeni piireeskirjade kohaselt ei ole piiratud liikmesriigi õigus teha päringuid riigisisestes andmekogudes. Seega sätestatakse PPVS-i § 19² lõikes 3, et piirikontrollis võetud biomeetrilisi andmeid võib isiku tuvastamiseks või isikusamasuse kontrollimiseks võrrelda ABIS-e biomeetriliste andmetega. See täiendus on samuti õiguselguseks. Praegu ei päri PIKO andmeid ABIS-est, kuid seda vajadust ei saa välistada.

ITDS-i § 15⁵ lõigetes 6 ja 7 on reguleeritud, millal võib ABIS-e andmeid töödelda isiku tuvastamiseks ja isikusamasuse kontrollimiseks. Piirikontrollis tehtav päring vastab üldjuhul ITDS-is sätestatud tingimustele. Küll aga rakendatakse piirikontrollis korrakaitseaduses sätestatud riikliku järelevalve erimeetmeid ja ABIS-e loomisel on antud hinnang, et isiku tuvastamiseks võib teha korrakaitseaduses sätestatud riikliku järelevalve erimeetme rakendamisel päringu juhul, kui see on vältimatult vajalik ohu tõrjumiseks.

Võimalike vaidluste ennetamiseks sätestatakse seega lõikes 3, et juhul kui piiriületajat ei ole võimalik tuvastada või tema isikusamasust kontrollida, võib kasutada ABIS-e andmeid. Ei saa välistada elulisi olukordi, kus piiriületaja isikut ei ole võimalik tuvastada muude andmekogude kui ABIS-e andmete põhjal. Kvaliteetse piirikontrolli tagamiseks on mõistlik kasutada ka ABIS-st, mille loomise üks eesmärk oli isiku tuvastamine ja isikusamasuse kontrollimine. See puudutab vaid neid piiriületajaid, kelle isikut ei ole võimalik tuvastada või kelle isikusamasuses on kahtlusi, näiteks kui isik üritab Eestisse siseneda võõra või võltsitud reisidokumendiga või ilma dokumendita. Biomeetrilised andmed kustutatakse pärast isiku riiki lubamist või sisene miskeelu otsust.

PPVS-i uue § 19² eesmärk on isikuandmete kaitset silmas pidades ja õiguselguse huvides sätestada, et piiriületusel võetud biomeetrilisi andmeid võrreldakse ABIS-e võrdlusmootorit kasutades. Seega **ei ole muudatusel olulist mõju**, kuna PPA peab rakendama Schengeni piireeskirju ja kontrollib ka praegu välispiiri ületajaid. Samuti võib piirikontrollis võetud sõrmejälgi võrrelda ABIS-e andmetega, kui piiriületajat ei ole võimalik tuvastada või tema isikusamasuses on kahtlusi. Muudatus ei ole põhimõtteline, sest sellised juhtumid läbivad praegu teise astme kontrolli⁴² ja Eestisse ei lubata kolmanda riigi kodanikku, keda ei ole võimalik tuvastada või kelle isikusamasuses on kahtlusi. ABIS-e andmete kasutamine on lisavõimalus teise astme kontrollis isiku tuvastamiseks või tema isikusamasuse kontrollimiseks.

3.4.6. Andmekogude regulatsiooni tehnilised muudatused (§ 2 p-d 1 ja 2, § 5 p-d 2–4 ning § 9 p-d 3, 4, 8 ja 9)

Eelnõu § 2 punktidega 1 ja 2 muudetakse KodS-i § 2¹ pealkirja ja lõiget 1.

⁴² Schengeni piireeskirjade artikli 2 punkti 13 kohaselt on see lisakontroll, mida võib teha spetsiaalselt selleks ettenähtud kohas eemal kohast, kus kontrollitakse kõiki isikuid.

- 1) Punktiga 1 asendatakse paragrahvi pealkirjas sõna „ja“ sõnaga „või“, et ühtlustada Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogule viitamist.
- 2) Punktiga 2 täpsustatakse, et andmekogu lühendit kasutatakse vaid KodS-i §-s 2¹.

Eelnõu § 5 punktidega 2–4 asendatakse PPVS-i 3. peatüki 6. jao pealkirjas ning § 25⁷ pealkirjas ja lõikes 1 ABIS-e täisnimetus lühendiga. Muudatus on vajalik, sest eelnõu § 9 punktiga 1 võetakse ABIS-e lühend kasutusele PPVS-i § 19² lõikes 2.

Eelnõu § 9 punktidega 3, 4 ja 9 ühtlustatakse lühendikasutust.

- 1) Punktiga 3 muudetakse VSS-i § 33 lõiget 1 ja antakse sissesõidukeeldude riikliku registri lühend, mida edaspidi paragrahvis kasutatakse.
- 2) Punktiga 4 muudetakse VSS-i § 33 lõiget 2 ja kasutatakse selles sissesõidukeeldude riikliku registri täisnimetuse asemel lühendit.
- 3) Punktiga 9 muudetakse VSS-i § 33¹⁴ lõiget 1 ning antakse Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu lühend, mis on paragrahvis juba kasutusel.

Eelnõu § 9 punktiga 8 jäetakse VSS-i § 33¹ lõikest 2 välja täisviide määrusele (EL) 2018/1861, sest kuna sissesõidukeeldude riikliku registri andmekoosseis tuuakse seaduse tasandile, antakse see edaspidi VSS-i § 33 lõike 3 punktis 6.

3.5. Lahkumisettekirjutus (§ 9 p-d 1 ja 2)

Eelnõu § 9 punktidega 1 ja 2 muudetakse VSS-i § 7, et täpsustada VSS-is välismaalase lahkumiskohustuse territoriaalset ulatust. Euroopa Komisjon on Schengeni hindamisel juhtinud Euroopa Liidu liikmesriikide tähelepanu sellele, et tagasisaatmisdirektiivi reguleerimisel on nii Schengeni konventsiooni kui ka Euroopa Liidu liikmesriikide territoorium. See tähendab, et välismaalane, kelle vastuvõttev riik on kolmas riik, peab lahkuma mitte üksnes lahkumisettekirjutuse tegija territooriumilt, vaid ka teiste Schengeni konventsiooni ja Euroopa Liidu liikmesriikide territooriumilt.

3.6. Seaduse jõustumine (§ 11)

Eelnõu §-ga 11 sätestatakse seaduse jõustumine. Seadus jõustub üldises korras, sest selle rakendamiseks ei ole vaja valmistuda ega tööd ümber korraldada.

Muudatused, mille rakendamiseks on vaja teha infotehnoloogilisi arendustöid, jõustuvad pärast nende valmimist.

- Eelnõu § 1 punkt 48, millega reguleeritakse e-residentsuse riskiriike, jõustub 2024. aasta 1. augustil.
- Eelnõu § 1 punktid 2, 4, 5, 10, 13, 27, 45, 49 ja 53, § 3 punktid 3–5 ning § 6 punktid 1 ja 4, millega lõpetatakse digitaalse isikutunnistuse väljaandmine ning sertifikaadi kehtivuse peatamine ja taastamine ning suurendatakse perekonnanime tähemärkide arvu dokumendil, jõustuvad 2025. aasta 1. novembril.
- Eelnõu § 1 punkt 25, millega võimaldatakse dokumendi taotlejal aktiveerida ID-1 formaadis dokument ja sertifikaadid elektrooniliselt, jõustub 2026. aasta 1. juunil.

4. Eelnõu terminoloogia

Eelnõuga võetakse kasutusele termin „**turvalise teenuse osutaja**“. See on teenuseosutaja, kelle on PPA riigihankega valinud ja kelle vahendusel toimetatakse dokument selle taotlejale kätte. Termin kasutusele võtmine on oluline, sest dokumendi kättetoimetamisel peab olema tagatud, et see antakse vahetult üle vaid selle vastuvõtmise õigusega isikule ja seda ei jäeta järelevalveta

postkasti. Seega on oluline tagada, et dokument, mis toimetatakse kätte teenuseosutaja vahendusel, jõuab kindlasti selle õige kasutajani.

Eelnõuga asendatakse ka termin „vanglatöötaja“ terminiga „vanglaametnik“, et viia ITDS kooskõlla VangS-iga, ja ühtlustatakse lühendikasutust.

5. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu ei ole seotud Euroopa Liidu õiguse ülevõtmisega. Eelnõu koostamisel on arvestatud isikuandmete kaitse üldmääruse põhimõtteid.

Eelnõu § 9 punktidega 1 ja 2 täpsustatakse juba Eesti õigusesse üle võetud tagasisaatmis-direktiivist tulenevat regulatsiooni selliselt, et oleks üheselt arusaadav, et viibimisalusetas Eestis viibivale välismaalasele tehakse lahkumisettekirjutus lahkumiseks VSS-i §-s 17 nimetatud vastuvõtvasse riiki, ning kui see on kolmas riik, peab välismaalane lahkuma lisaks Eestile ka teistest Schengeni konventsiooni ja Euroopa Liidu liikmesriikidest.

6. Seaduse mõjud

6.1. E-residendi digi-ID väljaandmine

6.1.1. E-residendi andmete töötlemine

- 1) Eelnõuga antakse PPA-le õigus e-residendi digi-ID kasutamise üle järelevalve menetluses:
 - edastada isikuandmeid kolmandatele isikutele;
 - koguda andmeid tähtsust omada võivate asjaolude kohta andmekogudest, teistelt avalik-õiguslikke ülesandeid täitvatelt asutustelt ja isikutelt ning eraõiguslikelt isikutelt.
- 2) Lisatakse RAB tema pädevuse piires e-residendi digi-ID kasutamise üle riikliku järelevalve teostajate loetellu.
- 3) Antakse PPA-le õigus edastada EIS-i e-residentsuse programmi meeskonnale e-residendi digi-ID väljaandmise menetluses kogutud andmeid: e-residendi digi-ID taotleja ees- ja perekonnanimi, isikukood, sünniaeg, sugu, kodakondsus ja kontaktandmed, taotlemise eesmärk ja põhjendus, plaanitava tegevuse kirjeldus ning e-residendi digi-ID väljastamise koht, väljaandmise aeg, kehtivusaeg ja kehtetuks tunnistamise aeg. E-residendi andmeid võib EIS töödelda vaid selleks, et analüüsida ITDS-i § 20⁵ lõikes 2 nimetatud eesmärgi täitmise tulemuslikkust ja mõju ning osutada selle eesmärgi täitmiseks vajalikke personali-seeritud teenuseid ning tuvastada ja maandada e-residendiga seotud riske.
- 4) Kehtiv õigus viiakse kooskõlla praktikaga, et e-residendi digi-ID taotluse saab esitada vaid PPA iseteeninduses.

6.1.1.1. Sotsiaalne, sealhulgas demograafiline mõju

Sihtrühm: e-residendi digi-ID taotlejad. E-residente on 1. juuli 2023. aasta seisuga 105 000.

Tabel 4. E-residendi digi-ID taotlejate prognoositud arv aastatel 2024–2028

	2024	2025	2026	2027	2028

E-residendi digi-ID taotlejate arv	16 600	15 200	16 300	17 000	18 700
---	--------	--------	--------	--------	--------

Allikas: PPA

Võrreldes teiste PPA väljaantavate dokumentide⁴³ taotlejatega, st Eesti elanikega, keda on 2023. aasta seisuga 1 365 884⁴⁴, on sihtrühm **väike**.

Mõju ulatus ja esinemise sagedus on **väikesed**, kuna muudatustega ei kaasne e-residendile lisategevusi ega kohanemiskursusi. Andmeid töödeldakse e-residenti vahetult kaasamata ja lisaandmeid küsimata. Seega, e-residendi koormus andmeid esitada ei suurene. Muudatustel on e-residendile positiivne mõju, sest tänu sellele, et EIS-il on põhjalikum teave e-residentide ja nende eesmärkide kohta, on e-residendile mõeldud tegevused ja teenused paremini analüüsitud ja sihistatud.

Ebasoovitava mõju kaasnemise risk on **väike**. E-residendi andmeid võivad töödelda seaduses toodud eesmärkidel selleks volitatud isikud ja andmeid töödeldakse andmekaitsereeglite järgi.

Seega on muudatustel sihtrühmale **väheoluline mõju**.

6.1.1.2. Mõju riigiasutuste ja EIS-i töökorraldusele

Sihtrühm

- 1) PPA ametnikud, kes edastavad EIS-ile e-residendi digi-ID väljaandmise menetluses kogutud andmeid. Neid on üks-kaks.
 - 2) EIS-i töötajad, kellel on õigus PPA edastatud andmeid töödelda. Neid on kolm.
 - 3) RAB-i teenistujad, kes teostavad järelevalvet e-residendi digi-ID kasutamise üle⁴⁵.
- PPA-s töötab umbes 5000 ja EIS-is 550 inimest. Seega on sihtrühm **väike**.

Mõju ulatus ja esinemise sagedus on **väikesed**, sest muudatused ei too sihtrühmale kaasa vajadust korraldada ümber oma tööd ega ümber õppida. Edaspidi vahetab PPA EIS-iga andmeid automaatselt, mistõttu on võimalik rakendada seni käsitsi andmeid edastanud PPA ametnikke ja EIS-i töötajaid otstarbekamalt. Muudatus, mille kohaselt esitatakse e-residendi digi-ID taotlus PPA iseteeninduses, PPA töökorraldust ei mõjuta, kuna praktikas see selliselt juba toimibki. Samuti ei mõjuta järelevalvemuudatus märgatavalt RAB-i töökorraldust, kuna RAB teostab riiklikku järelevalvet endiselt oma pädevuse piires.

Ebasoovitava mõju kaasnemise risk on samuti **väike**. Muudatustega ei kaasne negatiivset mõju. PPA ametnike ja EIS-i töötajate töömaht väheneb ning tänu automatiseeritud andmevahetusele kasvab andmetöötluse turvalisus.

Seega on muudatustel sihtrühmale positiivne, kuid **väheoluline mõju**.

6.1.2. Riskiriigi kodaniku e-residendi digi-ID taotluse tagastamine läbi vaatamata

Eelnõuga luuakse õiguslik alus **tagastada** seletuskirja tabelis 1 nimetatud **riskiriigi kodaniku e-residendi digi-ID taotlus läbi vaatamata** juhul, kui talle ei kohaldata ITDS-i § 20⁶ lisatava lõike 1² alusel kehtestatud erisusi. Seeläbi kaotab riskiriigi kodanik võimaluse kasutada Eesti

⁴³ Ajutine reisidokument, digitaalne isikutunnistus, Eesti kodaniku pass, elamisloakaart, isikutunnistus, meremehe teenistusraamat, meresõidutunnistus, pagulase reisidokument ja välismaalase pass.

⁴⁴ Statistikaamet. [Rahvaarv](#).

⁴⁵ RahaPTS-i § 53 lõike 4 kohaselt on RAB-i teenistus- ja töökohtade koosseis ning isikkoosseis asutusesiseseks kasutamiseks mõeldud teave avaliku teabe seaduse tähenduses.

e-teenuseid, sealhulgas kasutada e-residendi digi-ID-d äritegevuseks Eestis ja Euroopa Liidus. Eestil ei ole kohustust anda e-residendi digi-ID-d välja. E-residendi digi-ID väljaandmisega annab Eesti välismaalasele õiguse siseneda Eesti infoühiskonda ja kasutada Eesti e-teenuseid. See on ajutine hüve, mille andmise tingimused võivad olenevalt Eesti ja rahvusvahelisest julgeolekuolukorrast ning välispoliitilistest eesmärkidest muutuda. Seega on Eestil pädevus otsustada, kellele ja mis tingimustel e-residendi digi-ID välja antakse, ning mitte kellelgi ei ole subjektiivset õigust seda saada.

Muudatuse mõju hindamisel tuleb võtta arvesse nii otsest mõju sihtrühmale kui ka laiemat, sealhulgas kaudset, ehk teisest mõju Eesti mainele. Samuti tuleb arvestada võimalike tagajärgedega, mis võivad järgneda muudatuse kohaldamata jätmise korral, näiteks võimalus sattuda Moneyvali hindamisel riskiriikide nimekirja ning selle mõju Eesti majandusele ja elanikele. E-residentsuse programmi eesmärk on tagada võimalikult ulatuslik positiivne mõju Eestile. Seega on muudatusel oluline positiivne mõju Eesti julgeolekule ja siseturvalisusele, majandusele ning mainele, vaatamata sellele, et sotsiaalse ja demograafilise mõju ulatus on väike, kuna e-residendi digi-ID-ga ei kaasne sihtrühmale olulisi eeliseid.

6.1.2.1. Sotsiaalne, sealhulgas demograafiline mõju

Sihtrühm: riskiriigi kodanikud, kes soovivad taotleda e-residendi digi-ID-d. 1. juuli 2023. aasta seisuga on riskiriigi kodanikest e-residente 8097. Arvestades kavandatavaid erisusi, puudutab muudatus tõenäoliselt 53% riskiriigi kodanikest e-residendi digi-ID taotlejaid. E-residendi staatus on alates 2014. aastast saanud kokku üle 105 000 inimese. 1. juuli 2023. aasta seisuga oli kehtivaid e-residendi digi-ID-sid 62 430. Tõenäoliselt jääb riskiriigi kodanikest e-residendi digi-ID taotlejate arv ligikaudu samaks ja sihtrühm on võrreldes e-residentide koguarvuga **keskmine**.

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

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

Ebasoovitava mõju kaasnemise risk on **väike**. Muudatuse tulemusel ei ole riskiriigi kodanikul edaspidi võimalik taotleda e-residendi digi-ID-d, välja arvatud juhul, kui talle kohalduvad kavandatavad erisused, ega seeläbi kasutada Eesti e-teenuseid. Enamasti kasutatakse e-residendi digi-ID-d äritegevuseks. Ühe erisusena kavandatakse anda riskiriigi kodanikule võimalus taotleda e-residendi digi-ID-d, kui tal on Eestis tõestatav majandustegevus. Lisaks saab praegu riskiriigi kodanik luua ettevõtte notari vahendusel. Sellega kaasneb talle suurem halduskoormus, kuna tal puudub võimalus kasutada ettevõtte loomiseks, asjaajamiseks ja aruandluseks e-residendi digi-ID-d ja Eesti e-teenuseid.

Seega on muudatusel sihtrühmale **väheoluline mõju**.

6.1.2.2. Mõju riigiasutuste töökorraldusele

Sihtrühm: PPA ametnikud, kes menetlevad e-residendi digi-ID taotlusi. Neid on kaheksa. PPA-s töötab umbes 5000 inimest. Seega on sihtrühm **väike**.

Mõju ulatus ja esinemise sagedus on **väikesed**, kuna muudatus ei too PPA ametnikele kaasa vajadust korraldada ümber oma tööd ega ümber õppida.

Ebasoovitava mõju kaasnemise risk on samuti **väike**. PPA ametnike töömaht ei suurene, vaid pigem väheneb nende e-residendi digi-ID taotlejate võrra, kes on riskiriigi kodanikud ja kellele ei kohaldu kavandatavad erisused.

Seega on muudatusel sihtrühmale **väheoluline mõju**.

6.1.2.3. Mõju riigi julgeolekule, siseturvalisusele ja välissuhetele

Sihtrühm: Eesti elanikud. 2023. aasta alguse seisuga elas Eestis 1 365 884 inimest.⁴⁶ Sihtrühm on seega **suur**.

Muudatus avaldab **olulist positiivset mõju** Eesti julgeolekule ja siseturvalisusele, arvestades majanduslikke ja välispoliitilisi huve. Positiivse mõju saavutamiseks peab riik võtma tõhusaid meetmeid oma elanike turvatunde tagamiseks ja riskide maandamiseks. Riikide puhul, kellega Eestil puudub justiits-, julgeoleku- või õiguskaitsealane koostöö, ei ole e-residentsuse riskide maandamist võimalik tagada muul moel, kui piirata nende riikide kodanikele e-residendi digi-ID väljaandmist. Riskiriigi kodanikele e-residentsuse võimaldamine on vastuolus e-residentsuse eesmärgiga ning kahjustab Eesti julgeolekut ja mainet, sealhulgas välissuhteid.

Riskiriigi kodanikud võivad kasutada e-residendi digi-ID-d erinevate küber- ja majanduskuritegude toimepanemiseks või hüppelaua ja abivahendina viisa või elamisloa taotlemisel. E-residentsust on kasutatud immigratsioonipettustes. Seeläbi on varjatud eesmärkidega isikul lihtsam siseneda rändemenetlusse, mille tulemusena suurenevad julgeoleku- ja ränderiskid. Näiteks taotlevad Iraani kodanikest e-residendid tihti ka luba Eestisse saabumiseks ja siin viibimiseks. Iraani avalike allikate põhjal⁴⁷ annab Eesti e-residentsus võimaluse siseneda Euroopa Liitu ja teha rahvusvahelist äri, kuna lihtsustab viibimisaluse saamist Eestis ja Euroopa Liidus. PPA statistika kohaselt on või on olnud 15%-l Iraani kodanikest e-residentidel muid viibimisaluseid, näiteks elamisloa. See on riskiriikide kodanike seas suurim osakaal.

Tabel 5. Iraani kodanike e-residendi digi-ID taotlused aastatel 2014–2022

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

Allikas: PPA

Muudatus aitab maandada ja ennetada riigi julgeolekut ja siseturvalisust ohustavaid riske ning nendega kaasnevaid ühiskondlikke tagajärgi, mis tulenevad riskiriigi kodanike kogukondade suurenemisest. Need riskid on vaenulik mõjutustegevus, terrorism, radikaliseerumine, raske ja organiseeritud kuritegevus, eriti majanduskuritegevus, korruptsioon, rahapesu, terrorismi rahastamine ja küberkuritegevus. Muudatus mõjub positiivselt elanike turvatundele ja elukeskkonna turvalisusele.

Muudatus avaldab olulist positiivset mõju Eesti julgeolekule ja siseturvalisusele, kuigi mõju ulatus, esinemise sagedus ja ebasoovitava mõju kaasnemise risk on sihtrühmale **väikesed**. Muudatus ei mõjuta Eesti elanike igapäevast elukorraldust ega senist tegevust ega eelda neilt

⁴⁶ Sealsamas.

⁴⁷ [Iraani avalikud allikad Eesti e-residentsuse kohta.](#)

sihiteadlikku ümberkohanemist. Samuti on Eesti elanike kokkupuude muudatusega eba-regulaarne ja juhuslik. Ebasoovitava mõju kaasnemise risk Eesti elanike elukorraldusele ja turvalisusele suureneksid, kui jätta muudatus tegemata.

Seega on muudatusel sihtrühmale **positiivne oluline mõju**.

6.1.2.4. Mõju majandusele

Sihtrühm: Eesti elanikud. 2023. aasta alguse seisuga elas Eestis 1 365 884 inimest.⁴⁸ Sihtrühm on seega **suur**.

Riskiriigi kodanikest e-residentide ettevõtted ning nende käive ja töøjõumaksud

16.06.2023 oli kehtiva e-residenti digi-ID-ga riskiriigi kodanikest e-residentidel seos 1121 ettevõttega. See on 4,5% kõikidest e-residenti ettevõtetest, millest omakorda oli maksumaksjaid, st käibega ettevõtteid, umbes 18%.

Tabel 6. Riskiriigi kodanikest e-residentide ettevõtete arv riskiriigi kaupa

	Riik	Ettevõtete arv
1	Afganistani Islamivabariik	7
2	Alžeeria Demokraatlik Rahvavabariik	53
3	Burkina Faso	4
4	Egiptuse Araabia Vabariik	166
5	Iraagi Vabariik	16
6	Iraani Islamivabariik	192
7	Jeemeni Vabariik	15
8	Jordaania Hašimiidi Kuningriik	34
9	Kongo Demokraatlik Vabariik	6
10	Liibanoni Vabariik	68
11	Liibüa Riik	15
12	Lõuna-Sudaani Vabariik	0
13	Mali Vabariik	4
14	Maroko Kuningriik	100
15	Mosambiigi Vabariik	0
16	Nigeeria Liitvabariik	67
17	Nigeri Vabariik	0
18	Pakistani Islamivabariik	137
19	Palestiina Omavalitsus	10
20	Korea Rahvademokraatlik Vabariik	0
21	Saudi Araabia Kuningriik	8
22	Somaalia Liitvabariik	1
23	Sudaan	12
24	Süüria Araabia Vabariik	40
25	Tuneesia Vabariik	121
26	Usbekistan	52
27	Valgene Vabariik	449
28	Venemaa Föderatsioon	2039
	KOKKU	3609

Allikas: PPA

⁴⁸ Statistikaamet. [Rahvaarv](#).

2022. aasta III kvartalist kuni 2023. aasta I kvartalini deklareeris käivet või maksis tööjõumakse 158 riskiriigi kodanikust e-residendi ettevõtet. Neist 121 deklareeris käibe ja 42 maksis tööjõumakse.

- Riskiriigi kodanikest e-residentide ettevõtete deklareeritud käive oli 39 miljonit. Sellest 30% ehk 11,6 miljonit oli selliste ettevõtete käive, millega seotud riskiriigi kodanikust e-resident elab väljaspool riskiriiki.
- Riskiriigi kodanikest e-residentide ettevõtted tasusid tööjõumaksudena 281 840 eurot. Sellest 36,5% ehk 102 872 eurot tasusid riskiriigi kodanikest e-residendid, kes elavad väljaspool riskiriiki. See teeb 0,07% kõigist e-residentide ettevõtete tööjõumaksudest.

Mõju kirjeldus ja järeldus mõju olulisuse kohta

Muudatuse tulemusena võib väheneda e-residentsuse programmi võimalik tulu riigile, kuid arvestades, et riskiriigi kodanikest e-residente on vähe, on võimalik saamata jääv tulu marginaalne ega kaalu üles muudatuse rakendamata jätmise võimalikku kahju Eesti julgeolekule. E-residentsuse programmi kogutulu on 1. juuli 2023. aasta seisuga 179 miljonit eurot.

Hoolimata võimalikust saamata jäävast tulust avaldab muudatus Eesti majandusele **olulist positiivset mõju**. Ühe suurima e-residentsuse programmi riskina toodi Moneyvali hindamise aruandes välja, et e-residentsuse programm võimaldab välismaalasel kasutada e-residentsust ebasoovitavaks ettevõtluseks ning varjata ettevõtluse tegelikku sisu ja eesmärki ning sellest kasu saajaid. See on eriti probleemne riskiriikide kodanike puhul. Moneyvali hindamise tulemusena võib hinnatav riik sattuda riskiriikide halli või musta nimekirja⁴⁹. See tooks kaasa ulatusliku mõju Eesti kodanikele ja ettevõtjatele, sest sellise nimekirja riigi ettevõtete ja eraisikute suhtes tuleb kõikidel välispankadel ja teistel asutustel rakendada täiendavaid ettevaatusabinõusid.

Eesti tegi Moneyvali hindamisel tõsiseid pingutusi, et selgitada rahvusvahelistele ekspertidele e-residentsuse programmi olemust ja põhjendada, miks Eesti ei ole juba kehtestanud riskiriigi kodanikele piiranguid. Moneyvali hindamise ekspertide tõsiste kahtluste korral on Eesti riskiriikide nimekirja sattumise tõenäosus suur. Selle tulemusena viiksid Eestis tegutsevad rahvusvahelised ettevõtjad suure tõenäosusega oma ettevõtted mujale ning Eesti ettevõtjatel ja eraisikutel oleks pangakonto avamine keerulisem ning tõuseks laenuintress. Ka üldine asjaajamine ja arveldamine oleks Eesti ettevõtjatega raskem, kuna maksed peaksid läbima tihedama sõela. Ettevõtjad peaksid täpsemalt tõestama raha päritolu ja kinnitama, et tehing pole teeseldud. Seega on muudatuse mõju ulatus ja esinemise sagedus suured.

Ebasoovitava mõjuna võib väheneda riskiriigi kodanikest e-residentide ettevõtetest Eestile laekuv tulu. Kui riskiriigi kodanik soovib end Eestiga siduda ja siin ettevõtte luua, jääb talle nagu kõikidele mitteresidentidele võimalus luua ettevõtte notari vahendusel. Ebasoovitava mõju kaasnemise risk on seega **väike**.

Kokkuvõtvalt on muudatusel sihtrühmale **positiivne oluline mõju**.

6.2. Dokumendiliigid, dokumendikohustus ja isikusamasuse kontrollimine

⁴⁹ Mustas nimekirjas on kõrge riskiga riigid, kus on tõsiseid strateegilisi puudujääke võitluses rahapesu, terrorismi rahastamise ja massihävitusselvade leviku rahastamisega. Kõrge riskiga riikide suhtes rakendatakse tõhustatud hoolsuskohustust ja tõsisematel juhtudel kutsutakse teisi riike üles rakendama vastumeetmeid, et kaitsta rahvusvahelist finantsüsteemi. Hallis nimekirjas on riigid, kes on rahapesuvastase töökontra tugevdatud järelevalve all. Rahapesuvastane töökond (FATF) töötab välja rahapesu ja terrorismi rahastamise vastase võitluse standardeid ning meetodeid ja edendab sellealast poliitikat.

Eelnõuga **ajakohastatakse dokumendiliikide, dokumendi omamise kohustuslikkuse ja isikusamasuse kontrollimise** regulatsiooni:

- 1) luuakse võimalus kontrollida füüsilises keskkonnas isikusamasust digitaalselt mRiigi kaudu;
- 2) antakse Eesti kodanikule valikuvabadus, kas omada kohustusliku dokumendina isikutunnistust või passi;
- 3) kaotatakse kohustus esitada dokumendi kättesaamisel samaliigiline kehtiv dokument;
- 4) kaotatakse nõue tagastada isiku surma või surnuks tunnistamise korral dokument selle väljaandjale;
- 5) karmistatakse kohustust taotleda andmete, näiteks nime muutumise korral uus kohustuslik dokument: edaspidi peab seda tegema ühe kuu jooksul, pärast mida tunnistatakse valede andmetega dokument kehtetuks;
- 6) lõpetatakse Eesti kodanikule ja elanikule digitaalse isikutunnistuse väljaandmine;
- 7) lõpetatakse sertifikaadi kehtivuse peatamise ja taastamise võimalus.

6.2.1. Sotsiaalne, sealhulgas demograafiline mõju

Sihtrühm: dokumentide taotlejad. Need võivad olla kõik Eesti elanikud. Eestis elab 1 365 884 inimest.⁵⁰ Osa muudatusi, näiteks pass kohustusliku dokumendina ja mRiigi kasutuselevõtt, puudutab vaid Eestis elavaid Eesti kodanikke. 1. augusti 2023. aasta seisuga on rahvastiku registri kohaselt Eesti kodanikke, kelle elukoht on registreeritud Eestis või registreerimata, 1 146 789. Kuna sihtrühm võib olla kogu Eesti elanikkond, on see **suur**.

PPA prognoos aastatel 2024–2028 dokumentide taotlejate arvu kohta on toodud tabelis 8.

Mõju ulatus ja esinemise sagedus on **väikesed**. Muudatused ei too sihtrühmale kaasa erilisi uusi kohustusi ja puudub tarvidus nendega kohaneda. Kohustus teavitada PPA-d oma andmete muutumisest on ITDS-i § 14 lõikes 1 ka praegu, kuid kui inimene ei taotle uute andmetega dokumenti, kehtib valede andmetega dokument kuni kehtivusaja lõpuni. Muudatuse tulemusel teavitab PPA edaspidi inimest kohustusest taotleda uus dokument ja kui inimene seda kohustust tähtajal ei täida, tunnistab valede andmetega dokumendi automaatselt kehtetuks. PPA teavitab inimest korduvalt, enne kui tunnistab dokumendi kehtetuks.

Digitaalsed isikutunnistused, mis on antud välja enne muudatuse jõustumist, kehtivad kuni nende kehtivusaja lõpuni. Endiselt jääb alles võimalus kasutada e-keskkondadesse sisselogimisel isikutunnistust ehk ID-kaarti. Dokumenti, sealhulgas kohustuslikku dokumenti, taotleb sihtrühm regulaarselt: üldjuhul iga 5–10 aasta tagant.

Turvalisuse kaalutlustel lõpetatakse sertifikaadi kehtivuse peatamise ja taastamise võimalus, kuid endiselt jääb alles võimalus tunnistada sertifikaat kehtetuks näiteks juhul, kui isikutunnistus või elamisloakaart on läinud kaduma. Ajavahemikul 01.01.–31.10.2023 peatati sertifikaadi kehtivus 6368 ja taastati 1704 korral.

Ebasoovitava mõju kaasnemise risk on **väike**. Enamik muudatusi on positiivsed. Võimalikud riskid või turvalisusküsimused on maandatud kaasaegsete infotehnoloogiliste lahenduste ja tänapäevaste füüsiliste dokumentide tugeva turvalisusega. Digitaalse isikutunnistuse väljaandmise lõpetamine võib tuua sihtrühma üksikutele inimestele kaasa ebamugavusi, kui nad on harjunud kasutama digitaalset isikutunnistust. Selle asemel saab aga endiselt kasutada isikutunnistust või mobiil-ID-d.

⁵⁰ Sealsamas.

Seega on muudatusel sihtrühmale **väheoluline mõju**.

6.2.2. Mõju riigiasutuste töökorraldusele

Sihtrühm: PPA ametnikud, kes menetlevad dokumentide taotlusi. Neid on umbes 160. PPA-s töötab umbes 5000 inimest. Seega on sihtrühm **väike**.

Mõju ulatus ja esinemise sagedus on **väikesed**. Muudatused ei too PPA ametnikele kaasa vajadust korraldada ümber oma tööd ega ümber õppida. Muudatused võivad osaliselt vähendada töökoormust, näiteks seetõttu, et PPA ei anna enam välja digitaalseid isikutunnistusi või menetleb vähem isikutunnistuse taotlusi tänu sellele, et edaspidi on võimalik taotleda kohustusliku dokumendina ka passi. Kuna digitaalse isikutunnistuse väljaandmine lõpetatakse, ei ole PPA-l edaspidi vaja hankida selle isikustamiseks spetsiifilist riistvara. Töökoormus väheneb ka seetõttu, et lõpetatakse sertifikaadi kehtivuse peatamine ja taastamine.

Ebasoovitava mõju kaasnemise risk on **väike**. PPA ametnike töökorraldus ei muutu oluliselt. Tänu sellele, et vähenevad dokumendiliikide arv ning sertifikaadi kehtivuse peatamise ja uuendamisega seotud ülesanded, PPA ametnike töömaht pigem väheneb.

Seega on muudatusel sihtrühmale **väheoluline mõju**.

Tabel 7. Väljastatud dokumentide arv aastatel 2019–2023

	2019	2020	2021	2022	2023 (8 kuud)
Eesti kodaniku pass	188 121	103 347	119 870	106 036	7213
Välismaalase pass	15 811	15 814	7955	3235	1620
Digitaalne isikutunnistus	5103	4762	5019	4136	2746
Eesti kodaniku isikutunnistus	281 495	185 284	204 120	263 397	198 267
Euroopa Liidu kodaniku isikutunnistus	6616	6001	6253	5728	3293
Elamisloakaart	52 627	48 213	44 351	78 363	63 509

Allikas: PPA

Tabel 8. Dokumentide taotluste prognoositud arv aastatel 2024–2028

	2024	2025	2026	2027	2028
Eesti kodaniku pass	87 000	56 000	82 000	191 000	191 000
Välismaalase pass	2000	2000	1900	8600	9600
Eesti kodaniku isikutunnistus	270 000	210 000	227 000	268 000	285 000
Euroopa Liidu kodaniku isikutunnistus	7000	7000	7100	7000	7000
Elamisloakaart	71 000	68 000	64 000	61 000	

Allikas: PPA

6.3. Dokumendi väljaandmise menetlus ja andmetöötlus

Eelnõuga **muudetakse dokumendi väljaandmise menetlust**, et suurendada identiteedihalduse menetlustõhusust ja turvalisust ning kohandada õigusruumi ühiskonna arenguga. Riiklike dokumentide väljaandmise üks põhimõtte on, et iga riik dokumenteerib oma kodanikud ise. Selle põhimõtte ja Eesti identiteedihalduspoliitika turvalisuse tagamiseks:

- 1) antakse PPA-le piiratud õigus nõuda DNA-ekspertiisi välismaalaselt, kes taotleb esimest korda Eesti kodaniku dokumenti;
- 2) täpsustatakse välismaalase passi saajate sihtrühma;
- 3) võimaldatakse volitada dokumenti kätte saama ka pärast dokumendi taotluse esitamist;
- 4) võimaldatakse 15–17-aastase isiku dokumendi väljastamist tema seaduslikule esindajale;
- 5) antakse vanglaametnikule õigus võtta sõrmejäljed dokumendi väljaandmise menetluses;
- 6) luuakse dokumendi taotlejale võimalus aktiveerida oma dokument ja sertifikaadid ise.

6.3.1. Sotsiaalne, sealhulgas demograafiline mõju

Sihtrühm: dokumentide taotlejad. Need võivad olla kõik Eesti elanikud. Eestis elab 2023. aasta alguse seisuga 1 365 884 inimest.⁵¹ Kuna muudatused võivad mõjutada kõiki Eesti elanikke, on sihtrühm **suur**.

Mõju ulatus on **väike** ja esinemise sagedus **keskmise**. Enamik muudatustest on positiivsed ja ei too sihtrühmale kaasa uusi kohustusi ega vajadust kohaneda.

Näiteks võimaldatakse uue ID-1 formaadis dokumentide tootmise lepingu rakendamisega dokumendi taotlejal aktiveerida oma dokument ja sertifikaadid ise. Seega, kui näiteks välismaal elaval Eesti kodanikul on kehtiv eID vahend, ei pea ta enam minema isiklikult Eesti välisesindusse kohale – dokumendi toimetab talle kätte kuller, dokumendi ja sertifikaadid aktiveerib ta ise, autentides end kehtiva eID vahendiga, ning sertifikaatide turvakoodid saab ta kätte elektrooniliselt.

Muudatus, millega antakse PPA-le õigus nõuda DNA-ekspertiisi isikult, kes taotleb esimest korda Eesti kodaniku dokumenti, toob väikesele osale sihtrühmast kaasa DNA-ekspertiisi kohustuse. Muudatuse sihtrühm ning neile avalduva mõju ulatus ja esinemise sagedus on väikesed, sest seni on selliseid isikuid olnud umbes kümnekond ja DNA-ekspertiis on ühekordne. Muudatus puudutab valdavalt Venemaa ja Valgevene kodanikke, kes soovivad omandada Eesti dokumendi taotlemise kaudu Eesti kodakondsuse. Eestil on kohustus tõsikindlalt veenduda, et isikul on Eesti kodakondsuse õigus, ja välistada selle omandamine pettuse teel. Muudatus ei puuduta dokumendi taotlejaid, kelle esitatud andmetes või tõendites ei ole alust kahelda.

Samuti on vaid väga väike osa sihtrühmast neid, kellele antakse välismaalase pass välja ilma kodakondsusriigi nõusolekuta.

Üldiselt puutub sihtrühm muudatustega kokku regulaarselt, kuna Eesti elanikud taotlevad dokumenti iga 5–10 aasta tagant.

Ebasoovitava mõju kaasnemise risk on **väike**, sest muudatused on tänu menetluse tõhustamisele ja turvalisuse suurendamisele Eesti elanikele positiivsed.

Seega on muudatustel sihtrühmale **väheoluline mõju**.

6.3.2. Mõju riigiasutuste töökorraldusele

Sihtrühm

- 1) PPA ametnikud, kes menetlevad dokumentide taotlusi. Neid on umbes 160. PPA-s töötab umbes 5000 inimest.

⁵¹ Sealsamas.

- 2) Eesti välisesinduste töötajad, kes väljastavad dokumente. Neid on 73. Eesti välisesindustes töötab kokku 358 inimest.
 - 3) Eesti Kohtuekspertiisi Instituudi DNA-ekspertid. Neid on 13. Eesti Kohtuekspertiisi Instituudis töötab 138 inimest.
 - 4) Vanglaametnikud, kes võtavad kinnipeetavate sõrmejälgi. Neid on umbes 12. Vangla-teenistuses töötab 1176 inimest.
- Seega on sihtrühm **väike**.

Mõju ulatus ja esinemise sagedus on väikesed. Muudatused ei too sihtrühmale kaasa vajadust korraldada ümber oma tööd ega ümber õppida. Muudatused on positiivsed ning vähendavad Eesti välisesinduste, PPA ja vanglate töökoormust. Eesti välisesinduste töökoormus väheneb, sest välismaal elavad Eesti elanikud, kellel on kehtiv eID vahend, saavad oma dokumendi edaspidi kätte kulleriga ning saavad selle ja sertifikaadid ise aktiveerida. PPA töökoormus väheneb, sest PPA ametnik ei pea edaspidi minema sõrmejälgede võtmiseks vanglasse kohapeale, ja vangla töökoormus väheneb, sest vangla ei pea korraldama PPA ametniku sisenemist pääsles. 2023. aastal on kinnipeetavatele taotletud 89 dokumenti. Samuti võib PPA töökoormus väheneda tänu võimalike kohtumenetluste äralangemisele. Kui inimese tõsikindel õigus Eesti kodakondsusele ja dokumendi omamisele selgitatakse välja objektiiivsete tõendite alusel väljaspool kohtumenetlust, ei pea PPA ametnikud tegelema vaidlustatud otsustega. Eesti Kohtuekspertiisi Instituudi töökorraldust muudatused ei mõjuta, sest juhtumeid, kus on vaja kontrollida dokumendi taotleja õigust Eesti kodakondsusele, on alates Eesti taasiseseisvumisest 20. augustil 1991 olnud kümnekond.

Ebasoovitava mõju kaasnemise risk on väike, sest muudatused on tänu menetluse tõhustamisele ja turvalisuse suurendamisele sihtrühmale positiivsed.

Seega on muudatustel sihtrühmale **väheoluline mõju**.

6.4. Lahkumisettekirjutus

Eelnõu § 9 punktidega 1 ja 2 täpsustatakse juba Eesti õigusesse üle võetud tagasisaatmis-direktiivist tulenevat regulatsiooni selliselt, et oleks üheselt arusaadav, et viibimisaluseta Eestis viibivale välismaalasele tehakse lahkumisettekirjutus lahkumiseks VSS-i §-s 17 nimetatud vastuvõtvasse riiki, ning kui see on kolmas riik, peab välismaalane lahkuma lisaks Eestile ka teistest Schengeni konventsiooni ja Euroopa Liidu liikmesriikidest.

Tagasisaatmisdirektiiv võeti Eesti õigusesse üle 24. detsembril 2010 jõustunud **väljasõidukohustuse ja sissesõidukeelu seaduse muutmise seadusega**⁵², mille rakendamise mõju on hinnatud selle eelnõu seletuskirjas⁵³.

Eelnõuga kavandatud täpsustus **ei too kaasa lisamõju**. Lahkumisettekirjutuses märgitakse ka praegu ära, millisesse riiki peab viibimisaluseta Eestis viibiv välismaalane lahkuma. Samuti on lahkumisettekirjutuses märgitud, et kui vastuvõttev riik on kolmas riik, peab välismaalane lahkuma lisaks Eestile ka teistest Schengeni konventsiooni ja Euroopa Liidu liikmesriikidest. Eelnõuga viiakse regulatsioon kooskõlla praktika ja tagasisaatmisdirektiivi täpse sõnastusega.

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

⁵² [RT I, 29.11.2010, 2.](#)

⁵³ [793 SE](#) seletuskiri.

Eelnõu rakendamine toob kaasa infosüsteemide arendamise kulud. SMIT hindab arendusmahtu PPA esitatavate arendusvajaduste alusel ja kulud kaetakse SMIT-i eelarvest.

- 1) Muudatus, millega antakse vanglaametnikule **õigus võtta kinnipeetava sõrmejälgi**, eeldab väiksemaid arendustöid nii PPA (ABIS) kui ka vangla (kinnipeetavate, vahistatute, arestialuste ja kriminaalhooldusaluste andmekogu) infosüsteemides. Arenduskulud on veel väljaselgitamisel. Need kaetakse vanglate ja ABIS-e projekti eelarvest.
- 2) Muudatus, millega **piiratakse e-residendi digi-ID väljaandmist riskiriigi kodanikele**, toob samuti kaasa PPA iseteeninduse arenduskulud, mis kaetakse SMIT-i eelarvest. Arenduskulud on väljaselgitamisel.
- 3) Muudatus, millega **antakse EIS-ile e-residendi isikuandmete töötlemise õigus**, eeldab arendustöid, et võimaldada teha päringuid ITDAK-is ja e-residentsuse andmebaasis ning liidestada e-residentsuse andmebaas X-teega. Arendustööde hinnanguline maksumus on 60 000 eurot, millele lisandub käibemaks. Kulud kaetakse e-residentsuse programmi tegevuskuludest ja SMIT-i eelarvest.
- 4) **mRiigi suuremahulise rakendamisega** võivad tekkida lisakulud, kui mRiik võetakse laialdaselt kasutusele. Selleks, et katta ITDAK-i andmetega võrdlemise päringute mahtu, võib tekkida vajadus suurendada ITDAK-i andmekogu serverite jõudlust. Vajaduse ilmne-mise korral planeeritakse selleks raha SMIT-i eelarvesse.

8. Rakendusaktid

Eelnõu rakendamiseks on vaja **muuta järgmisi määrusi**:

- 1) Vabariigi Valitsuse 23. detsembri 2021. aasta määrus nr 125 „Automaatse biomeetrilise isikutuvastuse süsteemi andmekogu põhimäärus“;
- 2) siseministri 1. juuli 2020. aasta määrus nr 25 „Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu põhimäärus“;
- 3) siseministri 30. novembri 2015. aasta määrus nr 56 „Elamisloa ja elamisõiguse menetluses ning isikut tõendava dokumendi väljaandmise menetluses sõrmejälgede võtmise kord“;
- 4) siseministri 18. detsembri 2015. aasta määrus nr 78 „Isikut tõendavate dokumentide andmekogu pidamise põhimäärus“;
- 5) siseministri 18. detsembri 2015. aasta määrus nr 77 „Isikutunnistuse, elamisloakaardi, digitaalset isikutunnistuse, Eesti kodaniku passi, meremehe teenistusraamatu, välismaalase passi, ajutise reisidokumendi, pagulase reisidokumendi või meresõidutunnistuse väljaandmise taotlemisel esitatavate tõendite ja andmete loetelu, väljastamise kord ning väljaandmise tähtajad“;
- 6) siseministri 7. detsembri 2022. aasta määrus nr 40 „Sissesõidukeeldude riikliku registri põhimäärus“.

Siseministri 10. juuli 2009. aasta määruses nr 25 „Dokumendi taotleja isiku tuvastamise ja isikusamasuse kontrollimise kord“ tuleb eelnõu jõustumisel teha nii palju muudatusi, et otstarbekas on kehtestada uus terviktekst.

Samuti tuleb **kehtestada** ITDS-i § 20⁶ lõike 1² alusel **uus siseministri määrus** „Kõrgema rahapesu või terrorismi rahastamise riskiga riikide ja Eestiga justits-, julgeoleku- või õiguskaitsealase koostöösuheteta riikide loetelu ning nende riikide kodanikele e-residendi digitaalset isikutunnistuse väljaandmise erisused“. Volituspõhise vajalikkuse, selle eesmärgi, sisu ja ulatust ning selle alusel kavandatava rakendusakti vastavust Eesti Vabariigi põhiseadusele on

põhjustatud seletuskirja punktides 2.3.1. ja 3.1.5. Volitusnorm jõustub 2024. aasta 1. augustil, kuna selle rakendamiseks on vajalikud infotehnoloogilised arendustööd.

Rakendusaktide kavandid on seletuskirja lisas. Need on esialgsed ja võivad muutuda.

Volitusnormide (ITDS-i § 20 lg 3, § 20⁴ lg 8 ja § 34³ lg 3) kehtetuks tunnistamine

- 1) Eelnõuga tunnistatakse kehtetuks ITDS-i § 20⁴ lõige 8, mille kohaselt kehtestab valdkonna eest vastutav minister määrusega mobiil-ID väljaandmise üksikasjad, sealhulgas mobiil-ID:
 - lühema kehtivusaja kui viis aastat, kui mobiil-ID andmekandja tehniline lahendus ei vasta tingimustele, mis on vajalikud mobiil-ID turvaliseks kasutamiseks viie aasta jooksul;
 - kehtivusaja, kui hinnang mobiil-ID tehnilise lahenduse turvalisusele muutub ja mobiil-ID andmekandja tehniline lahendus võimaldab uue hinnangu kohaselt mobiil-ID turvalist kasutamist pikema aja vältel kui esialgne hinnang;
 - tehnilise lahenduse sama paragrahvi lõikes 7 sätestatud kooskõlastuse sisu ja ulatuse, kooskõlastuse andmise korra ja tähtaja ning tähtpäeva, alates millest on kooskõlastuse olemasolu kohustuslik.

See volitusnorm jõustus 1. mail 2014, kuid selle alusel ei ole määrust antud. Seetõttu ei ole seda otstarbekas säilitada.

- 2) Eelnõuga muudetakse ITDS-i § 20 lõiget 3. Selle tulemusena muutub kehtetuks volitusnorm, mille kohaselt määrab isikutunnistusele kantud digitaalsete andmete kehtivusaja valdkonna eest vastutav minister määrusega. Volitusnorm on ebavajalik, kuna eelnõuga sätestatakse ITDS-i § 20 lõikes 3, et isikutunnistuse ja sellele kantud digitaalsete andmete kehtivusaeg on samad. Volitusnormi alusel ei ole määrust antud.
- 3) Eelnõuga muudetakse ITDS-i § 34³ lõiget 3. Selle tulemusena muutub kehtetuks volitusnorm, mille kohaselt määrab elamisloakaardile kantud digitaalsete andmete kehtivusaja valdkonna eest vastutav minister määrusega. Volitusnorm on ebavajalik, kuna eelnõuga sätestatakse ITDS-i § 34³ lõikes 3, et elamisloakaardi ja sellele kantud digitaalsete andmete kehtivusaeg on samad. Volitusnormi alusel ei ole määrust antud.

9. Seaduse jõustumine

Enamik seadusest jõustub **üldises korras**, sest selle rakendamiseks ei ole vaja teha ettevalmistusi, arendada infosüsteeme ega korraldada ümber tööd.

Muudatused, mille rakendamiseks tuleb teha infotehnoloogilisi arendustöid, jõustuvad pärast arendustöid järgmiselt.

- Eelnõu § 1 punkt 48, millega reguleeritakse e-residentsuse riskiriike, jõustub 2024. aasta 1. augustil.
- Eelnõu § 1 punktid 2, 4, 5, 10, 13, 27, 45, 49 ja 53, § 3 punktid 3–5 ning § 6 punktid 1 ja 4, millega lõpetatakse digitaalse isikutunnistuse väljaandmine ning sertifikaadi kehtivuse peatamine ja taastamine ning suurendatakse perekonnanime tähemärkide piirarvu dokumendil, jõustuvad 2025. aasta 1. novembril.
- Eelnõu § 1 punkt 25, millega võimaldatakse dokumendi taotlejal aktiveerida ID-1 formaadis dokument ja sertifikaadid elektrooniliselt, jõustub 2026. aasta 1. juunil.

10. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitatakse eelnõude infosüsteemi (EIS) kaudu kooskõlastamiseks ministeeriumidele ning arvamuse avaldamiseks Andmekaitse Inspeksioonile, EIS-ile, KAPO-le, PPA-le, RAB-ile ja SMIT-ile.

Algatab Vabariigi Valitsus 2024