

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

1. Sissejuhatus

1.1. Sisukokkuvõte

Eelnõu on töötatud välja, et **suurendada identiteedihalduse turvalisust, maandada julgeolekuriske ja ajakohastada tööprotsesse**, viies need vastavusse tänapäevaste vajaduste ja võimalustega ning vähendades seeläbi inimeste halduskoormust ja ametiasutuste töökoormust. 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 suurema rahapesu- või terrorismi rahastamise riskiga riigi või sellise riigi kodanik, millega puudub Eestil justiits-, julgeoleku- või õiguskaitsealane koostöösuhe (edaspidi *e-residentsuse 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 (edaspidi *dokument*) ja tekib põhjendatud kahtlus, et välisriigis väljaantud Eesti kodakondsust tõendav dokument ei ole ehtne või selle alusandmed ei ole õiged. Praktikas on saenenud olukorrad, kus Venemaa või Valgevene kodanik soovib tõendada, et ta põlvneb Eesti kodanikust, kuid esitatud tõendites või andmetes on põhjust kahelda.
- 4) Luuakse võimalus **kontrollida isikusamasust Eesti teabevärava mobiilirakenduse vahendusel**.
- 5) **Lõpetatakse:**
 - turvalisuse kaalutlustel 15. novembrist 2025 **võimalus dokumendi sertifikaatide** (edaspidi *sertifikaadid*) **kehtivust peatada ja taastada**, kuna sellest kuupäevast hakatakse rakendama uusi ID-1 formaadis dokumentide¹ tootmise ja usaldusteenuse osutamise lepinguid², ning
 - vähese vajaduse ja kulude optimeerimise tõttu **võimalus anda välja ID-1 formaadis teiseseid digitaalseid isikutunnistusi**.
- 6) **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.

² ID-1 formaadis isikut tõendavate dokumentide plankide ostmise ning isikustamisteenuse ja teiste teenuste tellimine (riigihangete registri viitenumber 254499); sertifitseerimisteenuse ja kvalifitseeritud usaldusteenuse osutamine (riigihangete registri viitenumber 256281).

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);
- nõunik Ele Russak (ele.russak@siseministeerium.ee) – väljasõidukohustuse ja sissesõidu-keelu seaduse (edaspidi *VSS*) muudatused;
- õigusnõunik Maret Saanküll (maret.saankyll@siseministeerium.ee);
- õigusnõunik Kaspar Lepper (kaspar.lepper@siseministeerium.ee) – politsei ja piirivalve seaduse (edaspidi *PPVS*) ja *VSS*-i muudatused.

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

Eelnõu ja seletuskirja juriidilist kvaliteeti on kontrollinud Siseministeeriumi õiguskonkonna õigusnõunikud Gerly Herm (teenistussuhe lõppenud) ja Kertu Nurmsalu (tel 612 5084, kertu.nurmsalu@siseministeerium.ee).

Eelnõu ja seletuskirja, välja arvatud lisad, on keeleliselt toimetanud Siseministeeriumi õiguskonkonna keeleteimetaja Heike Olmre (tel 612 5241, heike.olmre@siseministeerium.ee).

1.3. Märkused

Eelnõu ei ole seotud muu menetluses oleva eelnõuga ega Euroopa Liidu õiguse rakendamisega. Eelnõu § 9 punktidega 1 ja 2 täpsustatakse õigusselguse huvides vaid juba Eesti õigusesse üle võetud tagasisaatmisdirektiivi³ rakendamise regulatsiooni *VSS*-is.

Eelnõu § 1 punkt 41, millega võimaldatakse kontrollida isikusamasust Eesti teabevärava mobiilirakenduse vahendusel, on seotud **Vabariigi Valitsuse tegevusprogrammi 2023–2027**⁴ eesmärgiga 3.2.4 „Loome e-riigi mobiilirakenduse, mille kaudu riik jõuab informatsiooni ja teenustega personaalselt iga eestimaalaseeni“.

Eelnõuga muudetakse järgmisi seadusi:

- 1) isikut tõendavate dokumentide seadus (edaspidi *ITDS*) – RT I, 26.04.2024, 13;
- 2) kodakondsuse seadus (edaspidi *KodS*) – RT I, 06.07.2023, 44;
- 3) konsulaarseadus (edaspidi *KonS*) – RT I, 29.06.2024, 17;
- 4) kriminaalmenetluse seadustik (edaspidi *KrMS*) – RT I, 21.06.2024, 34;
- 5) *PPVS* – RT I, 29.06.2024, 22;
- 6) riigilõivuseadus (edaspidi *RLS*) – RT I, 17.08.2024, 13;
- 7) vangistuseseadus (edaspidi *VangS*) – RT I, 21.06.2024, 32;
- 8) välismaalasele rahvusvahelise kaitse andmise seadus (edaspidi *VRKS*) – RT I, 06.07.2023, 119;

³ 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](#).

⁴ Vabariigi Valitsuse 18. mai 2023. aasta korralduse nr 131 „„Vabariigi Valitsuse tegevusprogrammi 2023–2027“ kinnitamine“ [lisa](#).

9) VSS – RT I, 21.06.2024, 33;

10) vääртеomenetluse seadustik (edaspidi *VTMS*) – RT I, 22.03.2024, 11.

Eelnõu on seotud:

- **siseturvalisuse arengukava 2020–2030**⁵ 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**⁶ 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**⁷, milles on toodud ühe riskimaandusviisina välja, et e-residentsust ei pakuta üldjuhul nende riikide kodanikele, millest tuleneb ulatuslik julgeoleku- või e-residenti digi-ID väärkasutuse oht, ja et e-residentidena on eriti eelistatud taotlejad riikidest, millega on Eestil justitiis-, julgeoleku- või õiguskaitsealane koostöö.

Eelnõu vastuvõtmiseks on vaja Eesti Vabariigi põhiseaduse (edaspidi *PS*) § 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 lahendusettepanekud

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 **kolm peamist eesmärki**:

- 1) suurendada identiteedihalduse turvalisust;
- 2) maandada julgeolekuriske ning
- 3) 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**

⁵ Siseministeerium. [Siseturvalisuse arengukava 2020–2030](#).

⁶ Riigi Infosüsteemi Amet 2018. [Valge Raamat. Identiteedihaldus ja isikut tõendavad dokumendid 1.0](#).

⁷ MKM. [E-residentsuse jätkustrateegia 2022–2025](#).

valdkonna riskihaldust, võimaldades riigil rakendada julgeolekukaalutlustel tugevamaid meetmeid, tagamaks, et riiklik identiteet antakse vaid õiguskuulekale isikule, kellel on sellele õigus.

Lisaks täpsustatakse eelnõuga õigusselguse huvides tagasisaatmisdirektiivist tulenevat lahku-missetekirjutuse regulatsiooni ning korrastatakse ABIS-e ja teiste andmekogude regulatsiooni, et tagada ühetaoline lähenemine ja **vastavus isikuandmete kaitse üldmäärusele**⁸. Eelnõuga ei muudeta andmete töötlemise põhimõtteid.

2.3. Eelnõu põhiseaduspärasus

Isikuandmete töötlemine

Õigus eraelu puutumatus on inimõigusena sätestatud erinevates rahvusvahelistes konvent-sioonides, Euroopa Liidu põhiõiguste hartas ja PS-is. Inimõigusena sisaldab see erinevaid hube ja põhiõigusi: kodu puutumatus, isikuandmete kaitse, sõnumisaladus jne. Põhiõigus kontrollida enda kohta käivat teavet ehk informatsioonilise enesemääramise õigus on isikuandmete kaitse põhimõtete alus nii Euroopa Liidu kui ka Eesti õigusaktides.

PS-i § 26 kohaselt on igaühel õigus perekonna- ja eraelu puutumatus. Riigiasutused ja kohaliku omavalitsuse üksused ning nende ametiisikud ei tohi kellegi perekonna- ega eraellu sekkuda muidu, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks.

→ Esemeline kaitseala. Riigikohtu hinnangul kaitseb PS-i § 26 kõiki eraelu valdkondi, mis ei ole kaitstud eriõigustega⁹, ja tagab seega tugevama kaitse. Eraelu kaitse üks oluline valdkond on isikuandmete kaitse, sest informatsioonilise enesemääramise õigus tagab igaühele õiguse ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse. Riigikohtu halduskolleegium on märkinud: „Eraelu puutumatus riivena käsitatakse muu hulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist.“¹⁰ Andmete, sealhulgas isikuandmete hulk ja teabe ulatus üha suurenevad ning sekkumine isikuandmete sfääri üha laieneb. Isikuandmete kaitse üldmäärus lubab isikuandmeid töödelda muu hulgas andmesubjekti nõusolekul (art 6 lg 1 p a). Avalik-õiguslikus suhtes andmete töötlemiseks peab siiski olema ka seadusest tulenev alus, kuna andmesubjekti nõusolek ei muuda olematuks formaalseid nõudeid põhiõiguse riiveks.

→ Isikuline kaitseala. Õigus perekonna- ja eraelu puutumatus on igaühe õigus. See tähendab, et PS-i § 26 kaitseb nii Eesti kodanikke kui ka Eestis viibivat välisriigi kodanikke ja kodakondsuseta isikut (PS-i § 9 lg 1).

→ Piiriklausel. PS-i § 26 teise lause kohaselt võib sekkuda perekonna- ja eraellu tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. See on kvalifitseeritud seadusereservatsioon, mis lubab perekonna- ja eraelu riivata üksnes seadusega või seaduse alusel PS-i § 26 teises lauses kindlaks määratud eesmärgil.

⁸ 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](#).

⁹ [RKPJKo, 25.06.2009, 3-4-1-3-09](#), p 16; [RKPJKo, 19.12.2019, 5-19-38/15](#), p 96. RKPJKo = Riigikohtu põhiseaduslikkuse järelevalve kolleegium.

¹⁰ [RKHKo, 12.07.2012, 3-3-1-3-12](#), p 19.

Kvalifitseeritud seadusereservatsiooni korral on põhiõiguse piirang legitiimne üksnes PS-is loetletud eesmärgil. Riigikohus on korduvalt kontrollinud, kas perekonna- või eraellu sekkumise eesmärk on hõlmatud PS-i § 26 teise lausega.¹¹ Õigust perekonna- ja eraellu puutumatusel võib seadusega piirata juhul, kui piirangu kehtestamisel on lisaks eesmärgi legitiimsusele järgitud PS-i §-s 11 sätestatud proportsionaalsuse põhimõtet, mille kohaselt peavad piirangud olema demokraatlikus ühiskonnas vajalikud ning ei tohi moonutada piiratavate õiguste ja vabaduste olemust. Seega võib seadusandja PS-i § 26 teises lauses nimetatud eesmärgil piirata isiku õigust perekonna- ja eraellu puutumatusel, kuid piirang peab olema proportsionaalne ehk sobiv, vajalik ja mõõdukas.

Sobivus

Meede on sobiv ehk kohane, kui see aitab kaasa legitiimse eesmärgi saavutamisele. Eelnõu eesmärk on muu hulgas suurendada identiteedihalduse turvalisust ning tagada avalikku korda ja julgeolekut. Eesmärgi saavutamiseks võetakse eelnõuga järgmisi meetmeid, millega piiratakse õigust perekonna- ja eraellu puutumatusel.

- 1) PPA-le antakse **õigus nõuda DNA-ekspertiisi** juhul, kui isik taotleb esimest korda Eesti kodaniku dokumenti ja tekib põhjendatud kahtlus, et välisriigis väljaantud Eesti kodakondsust tõendav dokument ei ole ehtne või selle alusandmed ei ole õiged. Praktikas on sagenenud olukorrad, kus Venemaa või Valgevene kodanik soovib tõendada, et ta põlvneb Eesti kodanikust, kuid esitatud tõendites või andmetes on põhjust kahelda.

PPA nõuab DNA-ekspertiisi vaid üksikutel juhtudel, kui isadus on omaks võetud aastaid pärast isiku sünni registreerimist või vahetult enne dokumendi taotlemist ja PPA-l on alust kahelda esitatud tõendite ehtsuses või andmete õigsuses. Kui PPA-l on võimalik tuvastada põlvnemine muu meetodiga, siis DNA-ekspertiisi kui kõige riivavamat meetodit ei kasutata ja Eesti kodakondsus tuvastatakse näiteks lisatõendite või -andmete alusel või Eesti kodakondsust tõendava dokumendi ekspertiisiga.

Praktikas on esinenud juhtumeid, kui Eesti kodanikku on mõjutatud end isaks tunnistama, kuid on olnud ka kohtuasi, kus oli esitatud Venemaa kohtule võltsitud volikiri ja tehtud kohtuotsus Eesti kodaniku teadmata. Kõikide selliste juhtumite korral on seni õnnestunud tõendada tõendi võltsimine või valeandmete esitamine ja isikud, kellel ei ole Eesti kodakondsusele õigust, ei ole seda ka saanud.

Eesti kodaniku õigused on sätestatud PS-is. Need on eeskätt õigus riigi kaitsele, sealhulgas välismaal viibides, isikupuutumatusel ja eneseväljendusele, aga ka poliitilised õigused. Kodanikustaatus annab peale õiguse riigi ja seaduse kaitsele ka õiguse riiki ise kaitsta, valida ja olla valitud ning moodustada erakondi. Samuti ei tohi Eesti kodanikku Eestist välja saata ega takistada Eestisse asumast. Teisalt kaasneb kodanikule kohustus alluda Eesti põhi-seaduslikule korrale, näiteks on meestel vanuses 16–60 aastat kohustus võtta osa riigi-kaitsest.

Arvestades Eesti kodaniku staatusega kaasnevaid õigusi, julgeolekuolukorda ning Riigikogus 20.03.2024 vastu võetud Eesti Vabariigi ja Vene Föderatsiooni lepingu õigusabi ja õigussuhete kohta tsiviil-, perekonna- ja kriminaalasjades denonsseerimise seadust¹², mille tõttu muutub ametlik dokumendivahetus Venemaaga praegusest veelgi keerukamaks, on otstarbekas lahendada Eesti kodakondsuse tõendamine kahtluse korral vähem aeganõudvas

¹¹ RKÜKo, 11.06.2019, 5-18-8/19, p 60; RKPJKo, 04.04.2011, 3-4-1-9-10, p 50; RKPJKo, 16.11.2016, 3-4-1-2-16, p 97. RKÜK = Riigikohtu üldkogu.

¹² [RT II, 03.04.2024, 1.](#)

menetluses kui kohtumenetlus. Seetõttu antakse eelnõuga 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. DNA-ekspertiisi eksperdiarvamus salvestatakse ITDAK-i, kus töödeldakse ja säilitatakse Eesti kodaniku dokumendi väljaandmise esmataotlemise andmeid tähtajatult.

2) **EIS-ile antakse õigus töödelda e-residendi digi-ID väljaandmise menetluses kogutud isikuandmeid ja e-residendi digi-ID andmeid.**

E-resident on välismaalane, kellele on Eesti hüvena loonud tema kodakondsusjärgse riigi identiteedi alusel digitaalse identiteedi ja andnud välja digitaalse isikutunnistuse: e-residendi digi-ID. E-residendi digi-ID on digitaalne dokument, mida saab kasutada üksnes e-keskkonnas isiku tuvastamiseks ja digiallkirja andmiseks. E-residendi digi-ID võimaldab välismaalasel osaleda Eestis avalik-õiguslikus ja eraõiguslikus asjaajamises, olenemata tema füüsilisest viibimiskohast, kuid ei anna õigust Eestisse saabuda ega Eestis viibida.

Eesti e-residendiks saamine on välismaalasele privileeg, mitte õigus. ITDS-i § 20⁶ kohaselt on e-residendi digi-ID väljaandmise eeldus olemasolev seos Eestiga või põhjendatud huvi Eesti e-teenuseid kasutada. Eesti kasutab kaalutusõigust ja taustakontrolli, et anda e-residendi digi-ID välja ainult usaldusväärsetele ja õiguskuulekatele välismaalastele. Eestil on õigus jätta e-residendi digi-ID välja andmata, selle kehtivus peatada või see kehtetuks tunnistada.

E-residendi digi-ID antakse välja kindlal eesmärgil ja taotleja plaanitavast tegevusest lähtudes. E-residendi digi-ID taotleja on kohustatud taotluse esitamisel tõendama või põhistama e-residendi digi-ID väljaandmise aluseks olevaid asjaolusid. Seega antakse e-residendi digi-ID igal juhul välja konkreetseks tegevuseks ja e-resident on sellega edaspidi seotud. EIS seirab riske, mis takistavad või mõjutavad muul viisil negatiivselt e-residendi digi-ID väljaandmise eesmärgi saavutamist, ja vajaduse korral pakub e-residendile eesmärgi saavutamiseks vajalikke personaalseid teenuseid. Kui personaalse teenuse osutamisel saab EIS-ile teatavaks asjaolu, mis võib olla e-residendi digi-ID kehtivuse peatamise või kehtetuks tunnistamise alus, peab EIS teavitama sellest PPA-d.¹³ Kui PPA menetluses selgub, et e-residendi digi-ID-d ei kasutata eesmärgipäraselt, on see e-residendi digi-ID kehtetuks tunnistamise alus, sest välismaalane ohustab seeläbi avalikku korda ja riigi julgeolekut.

3) **PPA-le antakse õigus kasutada isiku viimase dokumendi taotluses esitatud kontaktandmeid**, et saata talle teateid taotluse alusel väljaantud dokumendi ja ITDS-is sätestatud menetluste kohta. Näiteks võib PPA saata dokumendi kasutajale teate, et dokumendi kehtivusaeg hakkab lõppema ja vaja on taotleda uut dokumenti. Teate saatmise õigus võimaldab inimesele meelde tuletada, et ta taotleks õigel ajal uut dokumenti. Praktikast tuleb tihti ette, et inimene ei jälgi pidevalt dokumendi kehtivusaega ja avastab, et dokument on kehtivuse kaotanud, vahetult enne, kui ta läheb reisile või tal on vaja seda näiteks e-teenuste kasutamiseks või valimistel osalemiseks.

Teateid on oluline saata selleks, et välistada olukord, kus paljudel inimestel puudub kehtiv dokument. Eesti kodanikel ja elanikel on kohustus omada kehtivat isikutunnistust või elamisloakaarti. Kehtiva dokumendi omamine on oluline riigi julgeoleku tagamiseks, sest

¹³ [EIS-i põhikirja](#) p 2.2.11.

seeläbi on võimalik kontrollida riigis viibijate isikusamasust. Teate saatmine aitab ennetada ka seda, et inimesed enda teadmata seadust ei täida. Sanktsiooni sellise rikkumise eest ei ole ette nähtud ja inimesi ei karistata, kui dokument on kaotanud kehtivuse, kuid kohustust tuleb sellegipoolest täita.

Lisaks võib olla vaja saata dokumendi kasutajale teade turvaintsidendi korral, mille tõttu peab dokumendi väljaandja tunnistama sertifikaadid kehtetuks. Näiteks tekkis selline olukord 2017. aasta septembris, kui avastati ajavahemikul 16.10.2014–26.10.2017 väljastatud isikutunnistuste kiipide tarkvaras turvaviga. Seetõttu tuli isikutunnistuse kasutajal sertifikaate uuendada, ja kui ta seda ettenähtud kuupäevaks ei teinud, tunnistati need kehtetuks.

Järeldus. Arvestades eelnõu eesmärki suurendada identiteedihalduse turvalisust ning tagada avalikku korda ja riigi julgeolekut, on loetletud meetmed sobilikud ja aitavad eesmärgi saavutamisele kaasa.

Vajalikkus

Meede on vajalik, kui eelnõu eesmärki ei ole võimalik muul leebemal viisil vähemalt sama hästi saavutada.

- 1) **PPA õigus nõuda DNA-ekspertiisi ning EIS-i õigus töödelda e-residendi digi-ID väljandmise menetluses kogutud isikuandmeid ja e-residendi digi-ID andmeid.** Mõlemal juhul on sihtrühmas isikud, kellel ei ole seni Eestiga erilist seost olnud.
 - Avaliku korra ja riigi julgeoleku tagamiseks on hädavajalik teha selgeks, mis on Eesti kodaniku dokumendi taotlemise tegelik põhjus ning kas isikul on õigus Eesti kodakondsusele ja dokumendile, kui tal ei ole selle vastu seni huvi olnud. Sellisel juhul on kõige kindlam ja kiirem viis teha tema õigus Eesti kodakondsusele kindlaks DNA-ekspertiisiga, kui seda ei õnnestu teha muu meetodiga. Kui isikul on õigus Eesti kodakondsusele, on selle kindlaks tegemine ka tema huvides, sest DNA-ekspertiisi eksperdiarvamust säilitatakse tähtajatult ja see võib tõendada ka tema järglase õigust Eesti kodakondsusele.
 - E-resident seevastu on välismaalane, kellel ei ole e-residendi digi-ID alusel õigust Eestisse siseneda ega Eestis viibida. Küll aga saab e-resident kasutada Eesti e-teenuseid, e-keskkonnas enda isikut tuvastada ja anda digiallkirja.

Mõlemal juhul on sihtrühmas isikud, kelle kohta ei ole Eestil üldjuhul palju infot ja seda on keeruline ka välisriigist saada. Samuti soovivad mõlemal juhul isikud saada või kasutada Eestis hüvesid. See on nende vaba valik, st kui nad ei soovi Eestis hüvesid kasutada, ei pea nad seda tegema ja sel juhul puudub ka vajadus töödelda nende isikuandmeid.

- 2) **PPA õigus kasutada isiku viimase dokumendi taotluses esitatud kontaktandmeid.** Isikuandmete töötlemine teate saatmiseks on kõige lihtsam meede, mis koormab isikuid kõige vähem. Teate saab isik, keda see puudutab. Näiteks oleks dokumendi kehtivusaja lõppemisest avalikult teavitamine veelgi riivavam, sest sellest oleksid teadlikud ka need, keda teade ei puuduta. Ka turvaintsidendi korral saadetakse teade vaid isikule, kelle dokumenti see puudutab ja kellele kaasneb vajadus tegutseda. Teade saadetakse e-posti aadressil ja SMS-iga mobiiltelefonile. Rohkem dokumendi taotluses esitatud kontaktandmeid ei kasutata. Kui dokumendi taotluses on märgitud nii e-posti aadress kui ka mobiiltelefoni number, saadetakse teade mõlemale, sest nii on paremini tagatud, et isik saab teate õigel ajal kätte isegi juhul, kui üks neist on muutunud.

Järeldus. Loetletud meetmetele ei ole alternatiive, mis oleksid identiteedihalduse turvalisuse suurendamiseks ning avaliku korra ja riigi julgeoleku tagamiseks sama tõhusad, kuid vähem koormavad. Olukorras, kus ei ole võrreldavaid ja eelnõu eesmärgi saavutamiseks sama tulemuslikke alternatiive, tuleb meetmeid pidada vältimatult vajalikuks.

Mõõdukus

Meetme mõõdukuse hindamisel tuleb kaaluda ühelt poolt põhiõigusse sekkumise ulatust ja intensiivsust, teiselt poolt aga eesmärgi tähtsust. Seega tuleb kaaluda, kas eelnõu eesmärk suurendada identiteedihalduse turvalisust ning vältida ebasoovitavat mõju avalikule korrale ja riigi julgeolekule kaalub üles perekonna- ja eraelu puutumatus riive.

1) **PPA õigus nõuda DNA-ekspertiisi ning EIS-i õigus töödelda e-residendi digi-ID väljaandmise menetluses kogutud isikuandmeid ja e-residendi digi-ID andmeid.** Arvestades, et sihtrühmas on isikud, kes soovivad saada või kasutada Eestis hüvesid, ja et hüvede kasutamine on nende vaba valik, saavad nad ise otsustada ka selle üle, kas nende isikuandmeid Eestis töödeldakse. Kuna isikuandmeid töödeldakse identiteedihalduse turvalisuse suurendamiseks ning avaliku korra ja riigi julgeoleku tagamiseks, on eelnõu meetmed sihtrühmale proportsionaalsed.

- Kui isik ei soovi, et tema isikuandmeid eelnõus kavandatud viisil töödeldakse, ei ole tal kohustust taotleda Eesti kodaniku dokumenti. Sel juhul ei ole tal vaja ka Eesti kodakondsust tõendada ja ta võib jätkata oma senist elu. Kui Eesti kodaniku dokumendi väljaandmise menetluses tehakse kindlaks isiku õigus Eesti kodakondsusele, säilitatakse andmeid selle kohta tähtajatult ja neid saab kasutada ka tema järglase puhul, sest PS-i § 8 lõike 1 kohaselt on igal lapsel, kelle vanematest üks on Eesti kodanik, õigus Eesti kodakondsusele sünnilt.
- Samuti ei ole välismaalasel kohustust tarbida Eesti e-teenuseid. Kui välismaalane siiski otsustab taotleda e-residendi digi-ID-d, peab ta arvestama selle kehtivusajal isikuandmete töötlemisega, et vältida e-residendi digi-ID väärkasutust.

2) **PPA õigus kasutada isiku viimase dokumendi taotluses esitatud kontaktandmeid.** Teateid saadetakse isikule eelkõige tema enda huvides, sealhulgas teavitatakse turva-identsidentidest, et vältida dokumendi väärkasutust, ja tuletatakse meelde dokumendi kehtivusaja lõppemist, et aidata täita seadusjärgset dokumendikohustust. Dokumendi kehtivusaja lõppemise kohta saadetakse teade 60 ja 30 päeva enne dokumendi kehtivuse kaotamist. Rohkem teateid PPA ei saada ja isik saab ise otsustada uue dokumendi taotluse esitamise üle. Teadete saatmisega ei kaasne isikule kahjulikke tagajärgi.

Järeldus. Loetletud meetmed on proportsionaalsed, sest aitavad kaasa eelnõu eesmärgi saavutamisele ning kaaluvad üles perekonna- ja eraelu puutumatus riive.

2.4. Eelnõu väljatöötamise kavatsus

2.4.1. Siseministeriumi väljatöötamiskavatsus

ITDS-i muutmise seaduse eelnõu väljatöötamise kavatsus¹⁴ e-residentsuse riskiriigi kodaniku e-residendi digi-ID taotluse vastuvõtmisest keeldumise kohta oli eelnõude infosüsteemis kooskõlastamisel 24.05.–07.06.2023. Selle kooskõlastasid Justiitsministeerium (edaspidi *JUM*), Rahandusministeerium (edaspidi *RAM*) ja Välisministeerium (edaspidi *VÄM*) märkustega. Teised ministeeriumid kooskõlastuskirja ei esitanud. Arvamust avaldasid Andmekaitse

¹⁴ Eelnõude infosüsteemi toimiku nr [23-0622](#).

Inspeksioon, 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 e-residentsuse riskiriigi kodanikele kehtestatavate piirangute kohta ja ajakohastatud statistikat.

VÄM-i ettepanek jätta e-residentsuse riskiriikide loetelust välja Saudi Araabia

VÄM tegi ITDS-i muutmise seaduse eelnõu väljatöötamise kavatsuse kooskõlastamisel ettepaneku jätta e-residentsuse riskiriikide seast välja Saudi Araabia põhjusel, et Saudi Araabia on Eesti äridiplomaatia prioriteetne sihtriik, selle 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 liikmete¹⁵ vahele.

Ettepanekut kaaludes on Siseministeerium 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 koosõlas demokraatlike lääneriikide arusaamadega. Saudi Araabia toimib endiselt usuäärmusluse koolituskeskusena, mille mõju Eestis võib erandsoodustada. Saudi Araabia on riik, kes toetab mittedemokraatlikku ideoloogiat ja vaigistab kriitikat monarhia vastu muu hulgas terrorismivastase seadustiku alusel.¹⁶

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. aastal¹⁷. Samuti kuulub Saudi Araabia suurema terrorismi rahastamise riskiga riikide hulka. Saudi Araabia kodanike kohta kehtivad samad erisused nagu teiste e-residentsuse riskiriikide kodanike kohta. Neil 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.

2.4.2. MKM-i väljatöötamiskavatsus

MKM-i ITDS-i muutmise seaduse eelnõu väljatöötamise kavatsus¹⁸, 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, Siseministeerium ja VÄM. Teised ministeeriumid kooskõlastuskirja ei esitanud. Arvamust avaldas Statistikaamet. Seletuskirja koostamisel on arvestatud JUM-i märkustega.

¹⁵ Araabia Ühendemiraadid, Bahrein, Katar, Kuveit, Omaan ja Saudi Araabia.

¹⁶ 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.

¹⁷ [Saudi Araabia tunnistas, et Khashoggi mõrvati](#) 2018. – ERR/BNS, 22. oktoober.

¹⁸ Eelnõude infosüsteemi toimiku nr [22-1522](#).

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

2.4.3. 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 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 põhimääruse tasandilt seaduse tasandile. Sisulisi muudatusi andmekogude regulatsioonis eelnõuga ei tehta, mistõttu ei kaasne selle rakendamise ega muud olulist mõju.

2.4.4. Lahkumisettekirjutuse ja välismaalase kinnipidamise regulatsiooni korrastamine

Lahkumisettekirjutuse ja välismaalase kinnipidamise 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 ega muud olulist mõju.

- 1) Lahkumisettekirjutuse regulatsiooni korrastatakse selleks, et oleks üheselt arusaadav, et viibimisalusetult 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. Eelnõuga ei muudeta lahkumisettekirjutuse regulatsiooni põhimõtteid. Lahkumisettekirjutuses märgitakse ka praegu ära, millisesse riiki viibimisalusetult 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 tagasisaatmisdirektiivi täpse sõnastusega.
- 2) Välismaalase kinnipidamise regulatsiooni korrastatakse Riigikohtu halduskolleegiumi otsuste¹⁹ põhjal selleks, et tagada VSS-i §-s 15 sätestatud välismaalase kinnipidamise aluste õigusselgus. Riigikohtu hinnangul peab kinnipidamine ajast, millal asutus on enda hinnangul tuvastanud välismaalase ebaseadusliku Eestis viibimise, vastama tagasisaatmisdirektiivi artikli 15 nõuetele. Seejuures on Euroopa Liidu liikmesriikidel jätkuvalt võimalik reguleerida riigisisiseses õiguses kolmandate riikide kodanike kinnipidamist, et teha kindlaks, kas ta viibib riigis seaduslikult või mitte.

¹⁹ [RHKHo, 12.04.2024, 3-23-2232](#), p 22; [RHKHo, 12.04.2024, 3-23-2204](#), p 21.

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 **kaheksaks alapeatükiks**.

Võrdleva analüüsi sisukord

3. Eelnõu sisu ja võrdlev analüüs	11
3.1. E-residendi digi-ID väljaandmine	12
3.1.1. Haldusorgani õigus edastada ja koguda isikuandmeid järelevalvemenetluses (§ 1 p-d 8 ja 11).....	12
3.1.2. PPA õigus edastada andmeid EIS-ile ja EIS-i õigus neid töödelda (§ 1 p 10).....	12
3.1.3. E-residendi kohustus hoida oma kontaktandmed ajakohasena (§ 1 p 31).....	16
3.1.4. RAB-i õigus töödelda e-residendi andmeid (§ 1 p-d 48 ja 49).....	16
3.1.5. E-residentsuse riskiriigi kodanikule e-residendi digi-ID väljaandmise piiramine (§ 1 p 45).....	17
3.1.6. E-residendi digi-ID taotlemine ainult PPA iseteeninduses ja isikliku ilmumise kohustus (§ 1 p-d 47 ja 51–54)	21
3.1.7. E-residendi digi-ID riigilõiv (§ 6)	22
3.1.8. Viitemuudatus e-residendi digi-ID väljaandmise aluses (§ 1 p 44).....	23
3.2. Dokumendiliigid ja isikusamasuse kontrollimine	23
3.2.1. Sertifikaatide kehtivuse peatamise ja taastamise lõpetamine (§ 1 p-d 2, 3, 9, 12, 13, 25, 46 ja 50).....	23
3.2.2. Digitaalse isikutunnistuse väljaandmise lõpetamine (§ 1 p-d 14 ja 43, § 3 p-d 8–10 ning § 6 p-d 2 ja 4).....	24
3.2.3. Mobiil-ID väljaandmise volitusnormide kehtetuks tunnistamine (§ 1 p 43).....	25
3.2.4. Uue dokumendi taotlemine andmete muutumise korral (§ 1 p 28)	25
3.2.5. Lühendikasutuse ühtlustamine (§ 1 p 1) ning samaliigilise dokumendi esitamise ja surma korral dokumendi tagastamise nõude kaotamine (§ 1 p-d 26 ja 30).....	25
3.2.6. Dokumendi kontrollimine (§ 1 p-d 39 ja 40).....	26
3.2.7. Isikusamasuse kontrollimine Eesti teabevärava mobiilirakenduse vahendusel (§ 1 p 41)	27
3.2.8. Digitaalsete andmete kehtivusaeg (§ 1 p-d 42 ja 58).....	30
3.3. Dokumendi väljaandmise menetlus ja andmetöötlus	31
3.3.1. Isikunime dokumenti kandmine (§ 1 p-d 4 ja 5)	31
3.3.2. Dokumendi taotleja DNA-ekspertiis (§ 1 p-d 6 ja 20)	31
3.3.3. Isikuandmete töötlemine teate saatmiseks (§ 1 p 7).....	33
3.3.4. Dokumendi taotlemine vanglas (§ 1 p-d 15 ja 16–19)	33
3.3.5. Dokumendi väljastamine (§ 1 p-d 21–24 ja 55) ja väljaandja termin (§ 1 p-d 27 ja 29).....	34
3.3.6. Välismaalase passi väljaandmise alus (§ 1 p-d 56 ja 57)	35
3.3.7. Isiku daktüloskopeerimine tagasipöördumisdokumendi taotlemise korral (§ 1 p-d 59–61)	36
3.4. Andmete töötlemine riiklikes andmekogudes	36
3.4.1. ITDAK-i andmekoosseis ja ITDAK-i andmete säilitamise tähtajad (§ 1 p-d 33 ja 35).....	36
3.4.2. ABIS-e andmete säilitamise tähtajad (§ 1 p 38, § 2 p 9, § 3 p 4, § 4 p 3, § 7 p 3, § 9 p-d 16, 25 ja 26 ning § 10 p 3).....	41
3.4.3. Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu andmekoosseis ja andmete säilitamise tähtaeg (§ 2 p-d 3 ja 6)	43

3.4.4. Sissesõidukeeldude riikliku registri ning Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu andmekoosseis ja andmete säilitamise tähtajad (§ 9 p-d 13, 15, 19, 21 ja 22).....	43
3.4.5. Piirikontrolli andmekogu biomeetriliste andmete võrdlemine (§ 5 p 1)	45
3.4.6. Andmekogude põhimääruste volitusnormide täpsustamine (§ 1 p-d 34, 36 ja 37, § 2 p-d 4, 5, 7 ja 8, § 3 p-d 2 ja 3, § 4 p-d 1 ja 2, § 5 p 5, § 7 p-d 1 ja 2, § 8, § 9 p-d 14, 15, 20, 21, 23 ja 24 ning § 10 p-d 1 ja 2)	47
3.4.7. Andmekogude regulatsiooni tehnilised muudatused (§ 1 p 32, § 2 p-d 1 ja 2, § 3 p 1, § 5 p-d 2–4 ning § 9 p-d 11, 12, 17 ja 18)	47
3.5. KonS-i tehnilised muudatused (§ 3 p-d 5–7 ja 11).....	48
3.6. Lahkumisettekirjutus (§ 9 p-d 1 ja 2)	49
3.7. Välismaalase kinnipidamine (§ 9 p-d 3–10).....	49
3.8. Seaduse jõustumine (§ 11).....	51

3.1. E-residendi digi-ID väljaandmine

3.1.1. Haldusorgani õigus edastada ja koguda isikuandmeid järelevalvemenetluses (§ 1 p-d 8 ja 11)

Eelnõu § 1 punktidega 8 ja 11 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 kodakondsusjärgse riigi pädevatesse asutustesse, et veenduda tema õiguskuulekuses ja esitatud andmete õigsuses. Andmetöötlus on piiritletud andmekogu andmekoosseisuga. 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 kriminaal-karistus 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 sertifikaatide kehtivuse peatamise või 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 10)

Eelnõu § 1 punktiga 10 täiendatakse ITDS-i § 9² lõigetega 8¹–8⁴.

Lõikega 8¹ täpsustatakse ITDS-i § 9² lõike 8 alusel kolmandale isikule edastatud isikuandmete töötlemise lubatavust ja pannakse nende kustutamise kohustus. Kolmas isik peab kustutama isikuandmed viivitamata pärast dokumendi väljaandmise või kehtetuks tunnistamise menetluses, sertifikaatide kehtivuse peatamise või kehtetuks tunnistamise menetluses või e-residendi

digi-ID kasutamise üle järelevalve menetluses tähtsust omavate asjaolude väljaselgitamist ja nendest haldusorganile teada andmist.

Lõikega 8² 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 või selle puudumise korral sünniaeg, sugu, kodakondsus ja kontaktandmed;
- e-residendi digi-ID väljastamise koht, väljaandmise aeg ja kehtivusaeg;
- 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 määrust²⁰ 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 8³ antakse EIS-ile õigus töödelda lõikes 8² nimetatud andmeid selleks, et seirata riske, mis takistavad või mõjutavad muul viisil negatiivselt ITDS-i § 20⁵ lõikes 2 nimetatud eesmärgi saavutamist, ja vajadusel pakkuda e-residendile tema soovil eesmärgi saavutamiseks vajalikke personaalseid teenuseid. Et tagada e-residentsuse jätkusuutlik usaldusväärsus, analüüsitakse äriprotsesside ja infosüsteemide riske ning pakutakse personaalseid teenuseid. Seejuures ei ole personaalsed teenused turundustegevus – turundustegevuseks ja tavapäraste infokirjade saatmiseks ei tohi EIS e-residendi isikuandmeid lõike 8³ alusel töödelda. Samuti vaadatakse üle ja hinnatakse pidevalt e-residendi programmi riske, et koordineerida nende maandamist.

Isikuandmete töötlemise põhimõtted on kättesaadavad EIS-i veebilehel²¹. Andmete säilitamise tähtaja kohta on öeldud, et juhul, kui see on määratud õigusaktiga, lähtutakse sellest.

Lõikega 8⁴ kehtestatakse, kui kaua võib EIS lõikes 8² nimetatud andmeid säilitada. E-residendi digi-ID kehtib viis aastat, seega võib EIS lõikes 8² nimetatud andmeid säilitada viis aastat e-residendi digi-ID väljaandmisest arvates või kuni e-residendi digi-ID kehtetuks tunnistamiseni.

E-residentsuse programmi eesmärgi 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.

²⁰ 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.

²¹ EIS 2023. [Isikuandmete töötlemine](#).

EIS-i õiguslik alus isikuandmeid töödelda on isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt e: avalikes huvides oleva ülesande täitmine. Vabariigi Valitsus andis 4. detsembri 2014. aasta protokollilise otsusega²² MKM-ile ülesandeks luua Ettevõtluse Arendamise Sihtasutuse²³ juurde 1. veebruariks 2015 e-residentsuse programmi meeskond. EIS-i üks ülesanne on majandus- ja infotehnoloogiainistri 8. märtsi 2024. aasta käskkirjaga nr 23 kinnitatud põhikirja²⁴ 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 liiki;
- andmesubjekte;
- üksuseid, kellele võib isikuandmeid avaldada, ja avaldamise põhjuseid ning
- töötlemise eesmärgi piirangut.

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. 1. jaanuari 2024. aasta seisuga on 60 629 inimesel kehtiv e-residendi digi-ID. Ehkki EIS-i põhikirja kohaselt on EIS-il andmete töötlemise õigus²⁵, vajab ta õigusselguse põhimõtte²⁶ 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 raueks.

E-residendi digi-ID taotlemise eesmärgi ja plaanitava tegevuse andmete töötlemine aitab EIS-il ka täiustada e-residentidele teenuse osutajate võrgustikku „e-Residency Marketplace“,

²² Kättesaadav Riigikantseleist.

²³ 2022. aastal moodustati Ettevõtluse Arendamise Sihtasutusest ja KredExist EIS.

²⁴ [EIS-i põhikirja](#).

²⁵ Sealsamas, p 2.2.11: „oma vastutusvaldkondades andmete ja informatsiooni kogumine, süstematiseerimine, analüüsimine ja edastamine“.

²⁶ Õigusselguse põhimõtte tuleneb PS-i § 13 lõikest 2.

võimaldades aru saada, kas ja milliseid teenuseid on vaja võrgustikku juurde. Näiteks, kui 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 saadab PPA e-residendile teateid 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

EIS-ile e-residendi andmete töötlemise õiguse andmine on riskihalduse tõhustamiseks praeguses julgeolekuolukorras väga vajalik meede. EIS-i e-residentsuse programmi meeskonnal on vahetu kontakt e-residentidega ja 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. Näiteks, kui personaalsete teenuste osutamisel saab EIS-ile teatavaks asjaolu, mis võib olla e-residendi digi-ID kehtivuse peatamise või kehtetuks tunnistamise alus, peab EIS teavitama sellest PPA-d.²⁷ Kui PPA menetluses selgub, et e-residendi digi-ID-d ei kasutata eesmärgipäraselt, on see e-residendi digi-ID kehtetuks tunnistamise alus, sest välismaalane ohustab seeläbi avalikku korda ja riigi julgeolekut.

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 riskihinnangus²⁸ kui ka Euroopa Nõukogu rahapesu ja terrorismi rahastamise tõkestamise meetmeid hindava eksperdikomitee (edaspidi *Moneyval*) hindamisaruandes²⁹.

EIS-i tegevus ei ole järelevalve. EIS toetab e-residenti, lähtudes tema profiilist ning e-residendi digi-ID taotlemise eesmärgist ja plaanitavast tegevusest, näiteks aitab tal alustada Eestis ettevõtlusega sõltuvalt e-residendi tegevusvaldkonnast. Kuna EIS-i e-residentsuse programmi meeskonnal on e-residendiga Eestis kõige vahetum kontakt terve e-residentsuse jooksul, on EIS loogiline kontaktpunkt riigi ja e-residendi vahel, et vajadusel selgitada välja, mis takistab e-residendil liikuda soovitud eesmärgi poole, mille saavutamiseks ta e-residendiks hakkas. Kui EIS avastab oma tavapärasest tegevusest võimalikke e-residendi digi-ID väärkasutuse mustreid ja e-residendi profiilist tulenevaid riske, teavitab ta sellest järelevalveasutust. EIS ise järelevalveasutus ei ole ja järelevalvet ei teosta.

EIS-i tegevus 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. EIS-ile e-residendi andmete edastamiseks luuakse automatiseeritud andmevahetus üle infosüsteemide andmevahetuskirji (edaspidi *X-tee*). Andmed liiguvad ITDAK-ist kord

²⁷ [EIS-i põhikirja](#) p 2.2.11.

²⁸ RAM 2020. [Rahapesu ja terrorismi rahastamise riiklik riskihinnang](#).

²⁹ 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](#).

ööpäevas e-residentsuse andmebaasi, kus neid säilitatakse kuni viis aastat e-residendi digi-ID väljaandmisest arvates või kuni e-residendi digi-ID kehtetuks tunnistamiseni. Seetõttu edastatakse EIS-ile ka andmed e-residendi digi-ID kehtetuks tunnistamise kohta. E-residentsuse andmebaas on majutatud riigipilve, mida haldab EIS-i IT-haldus. E-residentsuse andmebaasi andmetele on juurdepääs 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.

Andmekaitsealane mõjuhindang

Isikuandmete kaitse üldmääruse artikli 35 lõike 3 kohaselt peab andmekaitsealase mõjuhindangu tegema järgmistel juhtudel:

- a) füüsiliste isiklike aspektide süstemaatiline ja ulatuslik hindamine, mis põhineb automaatsel isikuandmete töötlemisel, sealhulgas profiilianalüüsil, ja millel põhinevad otsused, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut;
- b) artikli 9 lõikes 1 osutatud andmete eriliikide või artiklis 10 osutatud süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud andmete ulatuslik töötlemine;
- c) avalike alade ulatuslik süstemaatiline jälgimine.

EIS-ile e-residendi andmete edastamisel ja nende andmete töötlemisel ei esine ühtegi nendest olukordadest. Seega ei ole andmekaitsealane mõjuhindang kohustuslik.

3.1.3. E-residendi kohustus hoida oma kontaktandmed ajakohasena (§ 1 p 31)

Eelnõu § 1 punktiga 31 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 teateid. Kohustus pannakse e-residentidele, kuna praktikas on just nendega kõige keerulisem saada vajadusel kontakti.

Eesti e-residendiks saamine on välismaalase privileeg, mitte õigus. ITDS-i § 20⁶ kohaselt on e-residendi digi-ID väljaandmise eeldus välismaalase olemasolev seos Eesti riigiga või põhjendatud huvi Eesti e-teenuseid kasutada. Kuna e-residendi digi-ID ei anna välismaalasele Eestisse saabumise ega Eestis viibimise õigust, ei ole üldjuhul e-residendi elukoht Eestis. Samas annab e-residendi digi-ID juurdepääsu Eesti e-teenustele ning riik võiks teada, kes, kus ja milleks neid teenuseid kasutab. Avaliku huvi eesmärk seisneb ka avaliku korra ja riigi julgeoleku tagamise kaalutlustel e-residendi digi-ID kehtetuks tunnistamises. Järelevalvemenetluses soovitakse e-residendile tagada ärakuulamisõigus, kuid sageli on e-residendi e-posti aadress selleks ajaks muutunud ja teda ei ole võimalik enne e-residendi digi-ID kehtetuks tunnistamist ära kuulata. Aktuaalseks võivad kontaktandmed muutuda ka siis, kui e-residendi digi-ID tunnistatakse kehtetuks ja välismaalasele on vaja toimetada kätte sellekohane otsus.

3.1.4. RAB-i õigus töödelda e-residendi andmeid (§ 1 p-d 48 ja 49)

Eelnõu § 1 punktidega 48 ja 49 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.

Rahapesu ja terrorismi rahastamise tõkestamise seaduse (edaspidi *RahaPTS*) § 53 lõike 1 kohaselt kuulub RAB RAM-i valitsemisalaselle ning teostab riiklikku järelevalvet ja kohaldab riiklikku sundi *RahaPTS*-is ette nähtud alustel ja ulatuses autonoomselt. RAB-i täpsed ülesanded on sätestatud *RahaPTS*-i §-s 54. RAB-i järelevalvepädevus tuleneb *RahaPTS*-i § 60 lõikest 5¹, mille kohaselt on RAB-il õigus edastada sama paragrahvi lõikes 4 nimetatud teavet³⁰ PPA-le, et PPA saaks otsustada e-residendi digi-ID väljaandmise, kehtivuse peatamise ja kehtetuks tunnistamise üle ning suurinvestorile ettevõtluseks tähtajalise elamisloa andmise või pikendamise, andmisest või pikendamisest keeldumise ja kehtetuks tunnistamise üle.

Eelnõuga lisatakse RAB ITDS-i § 20⁸ lõikes 1 loetletud riikliku järelevalve teostajate hulka, et oleks üheselt selge, et tal on pädevus teostada järelevalvet e-residendi digi-ID kasutamise üle. Praegu edastab PPA RAB-ile e-residendi digi-ID kasutamise üle järelevalveks andmeid ITDS-i § 9² lõike 8 alusel.

Lõikega 2¹ sätestatakse RAB-i kui järelevalveasutuse pädevuse piirid. RAB-ile ei anta eelnõuga lisaülesandeid, vaid õigus töödelda riiklikus järelevalves e-residendi digi-ID väljaandmise menetluses kogutud andmeid ja e-residendi digi-ID kasutamise andmeid, et RAB saaks täita oma *RahaPTS*-i § 54 lõike 1 punktis 1 sätestatud ülesannet tõkestada rahapesu ja terrorismi rahastamist ning võtta vastu, koguda, nõuda välja, registreerida, töödelda, analüüsida ja edastada sellele viitavat teavet.

RahaPTS-i § 58 lõike 1 kohaselt on RAB-il õigus oma seadusjärgsete ülesannete täitmiseks saada enda määratud tähtajaks teavet teistelt riigiasutustelt. E-residendi digi-ID kasutamise andmetest, sealhulgas logiandmetest, on RAB-il võimalik kontrollida oma seadusjärgsete ülesannete täitmisel näiteks seda, kas e-residendi digi-ID-d on kasutatud e-residentsuse riskiriigis. E-residendi digi-ID kasutamise andmed, sealhulgas logiandmed, aitavad tõendada rahapesu tõkestamise ja terrorismi rahastamise kahtlustusi. Neid andmeid on RAB-il võimalik küsida vajaduse järgi ametliku päringuga PPA lepinguliselt partnerilt, kes osutab e-identimiseks ja e-tehinguteks vajalikku sertifitseerimisteenust ja kvalifitseeritud usaldusteenust. Vastus päringule edastatakse krüpteeritult.

3.1.5. E-residentsuse riskiriigi kodanikule e-residendi digi-ID väljaandmise piiramine (§ 1 p 45)

Eelnõu § 1 punktiga 45 täiendatakse **ITDS-i § 20⁶ lõigetega 1¹ ja 1²**, millega luuakse õiguslik alus tagastada e-residentsuse riskiriigi kodaniku e-residendi digi-ID taotlus läbi vaatamata ning volitatakse siseministrit kehtestama määrusega e-residentsuse riskiriikide nimekirja (edaspidi *e-residentsuse riskiriikide nimekiri*) ja e-residentsuse riskiriigi kodanikule e-residendi digi-ID väljaandmise erisused. Muudatus ei mõjuta kehtiva e-residendi digi-ID-ga e-residentsuse riskiriigi kodanikke. Kehtiv e-residendi digi-ID kehtib kuni kehtivusaja lõpuni või järelevalve-menetluse 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

³⁰ *RahaPTS*-i § 60 lõike 4 kohaselt võib RAB teavitada pädevat järelevalveasutust sellest, et kohustatud isik on rikkunud *RahaPTS*-i nõudeid, või edastada asjakohase taotluse alusel RAB-is registreeritud andmeid, analüüse ja hinnanguid ulatuses, mis ei riku seaduse, välislepingu või rahvusvahelise koostöö raames kehtestatud piiranguid, kui see on vajalik rahapesu või terrorismi rahastamise või sellega seonduvate kuritegude tõkestamiseks ning pädeva järelevalveasutuse seadusest tulenevate ülesannete täitmiseks või *RahaPTS*-i eesmärkide saavutamiseks.

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 õiguskuulekad välismaalased. E-residendi digi-ID taotluse esitamisel peab välismaalane 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 menetlustoiminguid, 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 e-residendi digi-ID esmataotluse kohta negatiivse otsuse tegemise ja digi-ID kehtetuks tunnistamise arv. Kui 2018. aastal oli negatiivsete otsuste osakaal 2%, siis 2023. aastal 8%. Järelokrolli tulemusena tunnistati 2023. aastal kehtetuks 267 e-residendi digi-ID-d, 2020. aastal 29, 2021. aastal 89 ja 2022. aastal 224. Alates 2022. aasta juunist kasutab PPA ka järelokrolli 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 laenupõhise 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 riiklikus 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 eesmärgi ning sellest kasu saajaid.

Eriti probleemne on see selliste kolmandate riikide puhul, kellega puudub Eestil justiits-, julgeoleku- või õiguskaitsealane koostöö, st koostöö ei ole reguleeritud näiteks rahvusvahelise konventsiooni, kahepoolse lepingu ega vastastikuse mõistmise memorandumiga. Koostöö puudumine tähendab, et Eestil ei ole võimalik kontrollida e-residendi digi-ID taotleja tausta tema kodakondsusjärgse riigi pädevast asutusest, et kontrollida tema esitatud andmete usaldusväärsust. Sageli on just e-residentsuse 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 koostöö. Eelnõuga kehtestatakse õiguslik alus, mis võimaldab PPA-l tagastada e-residentsuse

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 Moneyvali riskiriikide nimekirja, kuna e-residentsuse programmis nägid eksperdid haavatavusi nii terrorismi rahastamise kui ka rahapesu tõkestamises.

E-residentsuse riskiriikide määramisel lähtutakse RAB-i avaldatud nimekirjast „Kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid“³¹. Lisaks kohaldatakse erisusi, mis võtavad arvesse julgeolekukaalutlusi, Eesti majanduslikke ja välispoliitilisi huve ning e-residentsuse programmi eesmärke. E-residentsuse riskiriikide nimekiri on tabelis 1. E-residentsuse riskiriikide kodanikel on 1. jaanuari 2024. aasta seisuga 6886 kehtivat e-residendi digi-ID-d, mis on umbes 11% kõikidest kehtivatest e-residendi digi-ID-dest.

Tabel 1. E-residentsuse 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 2024. aasta 1. jaanuari seisuga

	E-residentsuse riskiriik	Kehtivate e-residendi digi-ID-de arv
1	Afganistani Islamivabariik	28
2	Alžeeria Demokraatlik Rahvavabariik	152
3	Burkina Faso	9
4	Egiptuse Araabia Vabariik	480
5	Iraagi Vabariik	55
6	Iraani Islamivabariik	582
7	Jeemeni Vabariik	39
8	Jordaania Hašimiidi Kuningriik	93
9	Kongo Demokraatlik Vabariik	20
10	Liibanoni Vabariik	136
11	Liibüa Riik	44
12	Lõuna-Sudaani Vabariik	0
13	Mali Vabariik	13
14	Maroko Kuningriik	237
15	Mosambiigi Vabariik	1
16	Nigeeria Liitvabariik	158
17	Nigeri Vabariik	1
18	Pakistani Islamivabariik	670
19	Palestiina Omavalitsus	33
20	Korea Rahvademokraatlik Vabariik	0
21	Saudi Araabia Kuningriik	21
22	Somaalia Liitvabariik	1
23	Sudaan	35
24	Süüria Araabia Vabariik	109
25	Tuneesia Vabariik	327
26	Usbekistan	80
27	Valgene Vabariik	621
28	Venemaa Föderatsioon	2941
	KOKKU	6886

Allikas: PPA

³¹ RAB 2022. Juhend kahtlaste tehingute tunnuste kohta. Lisa: [kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid](#).

Võrreldes RAB-i avaldatud nimekirjaga „Kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid“ jäetakse e-residentsuse riskiriikide nimekirjast 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 ja RAB-i avaldatud nimekirja riskiriikidest on Türgil kõige suurem e-residentide kogukond. 1. jaanuari 2024. aasta seisuga on 2824 Türgi kodanikku, kellel on kehtiv e-residendi digi-ID. See on umbes 4,7% kõikidest kehtivatest e-residendi digi-ID-dest. Võrreldes teiste RAB-i avaldatud nimekirja riskiriikidega on Türgi e-residentide ettevõtted enim alustanud reaalsel majandustegevust Eestis. Kõikide RAB-i avaldatud nimekirja riskiriikide e-residentide ettevõtete tasutud maksudest on Türgi e-residentide ettevõtete riiklikud maksud umbes 86% ja tööjõumaksud 89%.
- **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. eksporditur, kus Eesti, sealhulgas e-residentide ettevõtetel on suurepärased äri võimalused, näiteks IT-sektoris. Araabia Ühendemiraatide e-residente on vähe: 1. jaanuari 2024. aasta seisuga on neil üheksa kehtivat e-residendi digi-ID-d.

E-residentsuse riskiriigiks määramine ei tähenda selle kodanikele, et nad ei saa üldse e-residendi digi-ID-d taotleda. Eelnõuga volitatakse siseministrit kehtestama **määrust, millega luuakse erisused e-residentsuse riskiriigi kodanikele, kes vastavad vähemalt ühele järgmistest tingimustest**³².

- 1) Välismaalane on elanud vahetult enne e-residendi digi-ID taotluse esitamist vähemalt kolm järjestikust aastat **Euroopa Majanduspiirkonna lepinguriigis** ja tal on selle riigi kehtiv elamis luba. Euroopa Majanduspiirkonna lepinguriikide vahel on toimivad koostöösuhted ja andmevahetusmudel, mis läbi on Eestil võimalik saada nendest riikidest välismaalase kohta usaldusväärset lisainfot. Neis riikides on kehtestatud ühtsed elamisloakaartide standardid, mis võimaldavad menetlejal veenduda välismaalase esitatud andmete ja dokumendi õigsuses. Kolmandates riikides on aga kasutusel erinevad elamisõigust tõendavad alusdokumendid, mille õigsuse tuvastamine ei pruugi olla võimalik.
- 2) Välismaalasel on **Eestis püsiv majandustegevus**. E-residendi digi-ID-d võimaldatakse taotleda e-residentsuse 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. Eestil on selle sihtrühma majandustegevuse kohta lisainfot, mida on võimalik kontrollida. Kui ettevõttel on nullkäive ja ettevõtja ei maksa makse, siis erisust ei kohaldata.
- 3) Välismaalane esitab **e-residendi digi-ID korduvtaotluse**. Korduvtaotluse menetlemisel on võimalik hinnata e-residendi senist tegevust ja seda, kas ta täidab e-residentsuse programmi eesmärgi, panustades Eesti majanduse, teaduse, hariduse või kultuuri arengusse. Erisust kohaldatakse juhul, kui e-resident tegeleb tõestatavalt Eestis majandustegevusega ja sellega kaasneb Eestile maksutululu, st nullkäibega ettevõttele erisust ei kohaldata.
- 4) Välismaalane on **Eesti välisesinduse töötaja või aukonsul**. Eestil on ka e-residentsuse riskiriikides, näiteks Egiptuses, välisesindusi ja ei ole välistatud, et välisesinduse töötaja, kes vajab oma tööülesannete täitmiseks e-residendi digi-ID-d, on sellise riigi kodanik. Kõik sellised välismaalased läbivad põhjaliku taustakontrolli ja riskide ilmnemise korral saab PPA e-residendi digi-ID taotluse tagastada seda läbi vaatamata.

³² Ukraina-vastase täiemahulise sõja tõttu ei kohaldata neid erisusi Venemaa ja Valgevene kodanikele, välja arvatud korduvtaotluse ja Eestis püsiva majandustegevuse erisus.

79% e-residentidest, kes on e-residentsuse riskiriigi kodanikud, ei ela Euroopa Liidus ega Ühendkuningriigis, sealhulgas ei ole neist 56%-l Eestis kehtivaid ärisuhteid. Seega puudutab eelnõu tõenäoliselt umbes 56% sellistest e-residentidest. Kõikidest kehtiva e-residendi digi-ID-ga e-residentidest on see *ca* 11%.

Tõhustatud eel- ja järelkontrolli ning muid juba juurutatud riskide maandamise meetmeid rakendatakse eriti rangelt e-residentsuse riskiriigi kodanike suhtes, kellele kohaldatakse erisusi, ja nende suhtes, kes ei ole küll e-residentsuse riskiriigi kodanikud, kuid märgivad selle, Türgi või Araabia Ühendemiraadid oma elukohariigiks. Julgeolekuolukorra muutumisest ja ilmnunud riskidest lähtuvalt on võimalik laiendada e-residentsuse riskiriigi kodanike erisusi ka e-residentidele, kes ei ole riskiriigi kodanikud, aga elavad seal. E-residentsuse nõukojas lepatakse kokku riskihaldusmeetmed ja seiratakse riskihaldust. E-residentsuse nõukoja liige on ka RAM.

E-residentsuse riskiriikide nimekirja, erisused e-residentsuse riskiriigi kodanikele ja jääkriskid on otsustatud e-residentsuse nõukotta kuuluvate ministriumide ja asutuste³³ ühisel kokkuleppel, et muudatus arvestaks laiapinnaliselt Eesti huve ja seisukohti. On äärmiselt tundlik ja keeruline väljakutse leida Eesti 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 ilmumise kohustus (§ 1 p-d 47 ja 51–54)

Eelnõu § 1 punktidega 47 ja 51–54 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 esitada e-residendi digi-ID taotluse Eesti konsulaarametnikule, kes edastab selle pärast taotleja isikusamasuse kontrollimist ja biomeetriliste andmete võtmist PPA-le läbivaatamiseks. Praktikas 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.
- 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 47 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

³³ E-residentsuse nõukotta kuuluvad JUM, MKM, RAM, Siseministeerium, VÄM, EIS, PPA ja alates 10.04.2024 RAB.

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. Lõige 2 on laiem ja võimaldab nõuda e-residendi digi-ID kasutaja ilmumist PPA-sse või Eesti välisesindusse ka pärast e-residendi digi-ID väljastamist. Selline vajadus võib tekkida näiteks juhul, kui on kahtlus, et on pandud toime identiteedivargus.

- 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)

Eelnõu § 6 punktiga 1 täiendatakse **RLS-i 2. peatüki 3. jagu §-ga 15¹** ning **punktidega 2 ja 5** tunnistatakse kehtetuks **§ 271 lõike 4 teine lause ja § 273 lõike 8 teine lause**.

RLS-i §-s 15¹ reguleeritakse riigilõivu tagastamata jätmist. Riigilõivu tagastamist on reguleeritud RLS-i 2. peatüki 3. jaos, seega on mõistlik koondada ka tagastamata jätmise regulatsioon samasse jaosse.

- 1) **Punktis 1** sätestatakse riigilõivu tagastamata jätmise, kui e-residendi digi-ID taotlus jäetakse läbi vaatamata. 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 töendamiskohustust, näiteks ei esita pärast korduvaid meeldetuletusi passi nõuetekohast koopiat, ei suuda põhjendada e-residendiks saamise motiive või ei esita oma kodakondsusjärgse riigi karistusregistri väljavõtet, on põhjust kahelda tema motiivides ja huvis saada e-residendiks.

E-residentsus on ajutine hüve, mille andmisel lähtutakse ühelt poolt riigi julgeolekulukorrast ja e-residentsuse programmi eesmärgist ning teiselt poolt e-residendi digi-ID taotleja motiividest ja tema panusest e-residentsuse programmi eesmärki. 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

jätmine põhjendatud, sest e-residendi digi-ID taotluse menetlemisel on tehtud tööd, mis on toonud riigile kaasa kulu.

- 2) **Punktis 2** sätestatakse riigilõivu tagastamata jätmine, kui riigilõiv on tasutud RLS-i § 271 lõike 4 või § 273 lõike 8 alusel, kuid dokumendi taotleja soovib muuta dokumendi taotluses märgitud väljastuskohta pärast väljaantud dokumendi sinna saatmist. Seda on praegu reguleeritud RLS-i § 271 lõike 4 teises lauses ja § 273 lõike 8 teises lauses. Seega tunnistatakse regulatsiooni ümberpaigutamise tõttu ühtlasi kehtetuks **RLS-i § 271 lõike 4 teine lause ja § 273 lõike 8 teine lause**.

Eelnõu § 6 punktidega 3 ja 4 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.

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

Ühtlasi jäetakse lõikest 20 välja teine lause, milles on reguleeritud riigilõivu tagastamata jätmist, kui riigilõiv on tasutud, kuid dokumendi taotleja soovib muuta dokumendi taotluses märgitud väljastuskohta pärast väljaantud dokumendi sinna saatmist. Seda reguleeritakse edaspidi RLS-i §-s 15¹ (eelnõu § 6 p 1).

3.1.8. Viitemuudatus e-residendi digi-ID väljaandmise aluses (§ 1 p 44)

Eelnõu § 1 punktiga 44 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 nimetamata isikule. Kuna see lõige tunnistatakse eelnõu § 1 punktiga 43 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 ja isikusamasuse kontrollimine

3.2.1. Sertifikaatide kehtivuse peatamise ja taastamise lõpetamine (§ 1 p-d 2, 3, 9, 12, 13, 25, 46 ja 50)

Eelnõu § 1 punktidega 13 ja 46 tunnistatakse kehtetuks **ITDS-i § 9⁵ ja § 20⁶ lõige 5**. **Eelnõu § 1 punktidega 2, 3, 9, 12, 25 ja 50** 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 sertifikaatide kehtivuse peatamisele ja taastamisele.

ITDS-i § 9⁵ kohaselt on dokumendi väljaandjal õigus peatada sertifikaatide kehtivus ning taastada peatatud kehtivusega sertifikaatide kehtivus e-identimise ja e-tehingute usaldus-teenuste seaduse §-des 17 ja 18 sätestatud tingimustel. Peatatud kehtivusega sertifikaatidega on aga teoreetiliselt võimalik luua krüptograafiline allkiri ja sertifikaatide kehtivuse taastamisel ei ole võimalik tuvastada, et allkiri on antud ajal, kui sertifikaatide kehtivus oli peatatud. See on vastuolus eIDAS-e määruse artikli 32 nõudega kvalifitseeritud e-allkirja valideerimise kohta, sest puudub võimalus kontrollida, kas sertifikaadid oli allkirja andmise ajal kehtivad. Seega

lõpetatakse võimalus sertifikaatide kehtivust peatada ja taastada nii uue lepingu alusel välja antava dokumendi kui ka varasema lepingu alusel välja antud kehtiva dokumendi puhul.

3.2.2. Digitaalse isikutunnistuse väljaandmise lõpetamine (§ 1 p-d 14 ja 43, § 3 p-d 8–10 ning § 6 p-d 2 ja 4)

- 1) Eelnõu § 1 punktidega 14 ja 43 tunnistatakse kehtetuks ITDS-i § 11² lõiked 5 ja 6 ning § 20¹ lõige 2, milles on reguleeritud digitaalse isikutunnistuse taotluse esitamist ja isikutunnistuse väljaandmist.
- 2) Eelnõu § 3 punktidega 8–10 muudetakse KonS-i § 48 pealkirja ja lõiget 2 ning tunnistatakse kehtetuks lõige 1, milles on reguleeritud digitaalse isikutunnistuse taotluse edastamist ja isikutunnistuse väljastamist.
- 3) Eelnõu § 6 punktiga 2 tunnistatakse kehtetuks RLS-i § 272 lõige 5, milles on reguleeritud digitaalse isikutunnistuse taotluse läbivaatamise riigilõivu, ja punktiga 4 muudetakse lõiget 20, milles on reguleeritud digitaalse isikutunnistuse väljastamise riigilõivu.

Muudatused puudutavad ainult seda digitaalset isikutunnistust, mis antakse välja ITDS-i § 20¹ lõike 2 alusel³⁴. 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 teine dokument, mida on võimalik kasutada vaid e-keskkonnas. Sellel 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 2.

Tabel 2. 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. Tavapäraselt taotlevad digitaalset isikutunnistust korduvalt umbes 50% taotlejatest.

Seega lõpetatakse digitaalse isikutunnistuse väljaandmine, mistõttu:

- tunnistatakse kehtetuks ITDS-i § 11² lõiked 5 ja 6 ning § 20¹ lõige 2, KonS-i § 48 lõige 1 ja RLS-i § 272 lõige 5 ning
- muudetakse KonS-i § 48 pealkirja ja lõiget 2, et välistada digitaalne isikutunnistus, mis antakse välja ITDS-i § 20¹ lõike 2 alusel, ning RLS-i § 272 lõiget 20, et jätta välja viide lõikele 5.

³⁴ 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.

3.2.3. Mobiil-ID väljaandmise volitusnormide kehtetuks tunnistamine (§ 1 p 43)

Eelnõu § punktiga 43 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 28)

Eelnõu § 1 punktiga 28 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. Praktikast on ette tulnud olukordi, kus inimene ei taotle uut dokumenti enne eelmise dokumendi kehtivusaja lõppemist ja kasutab aktiivselt ebaõigete andmetega dokumenti. Näiteks on inimene muutnud nime abiellumisel või muul põhjusel³⁵, 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. Lühendikasutuse ühtlustamine (§ 1 p 1) ning samaliigilise dokumendi esitamise ja surma korral dokumendi tagastamise nõude kaotamine (§ 1 p-d 26 ja 30)

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 26 ja 30 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 praegu 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 märget dokumenti ei tehta. Lõiget 5 muudetakse seega selliselt, et edaspidi muudab 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.

³⁵ Näiteks sages nimevahetus pärast Ukraina-vastase sõja algust, kuna sooviti võtta eestipärasem nimi.

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, muudab 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 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 39 ja 40)

Eelnõu § 1 punktiga 39 loetakse **ITDS-i § 16 tekst lõikeks 1** ja täiendatakse paragrahvi **lõigetega 2 ja 3**.

Lõikes 2 sätestatakse, et 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. Sellega viiakse ITDS kooskõlla praktikaga.

Lõikes 3 sätestatakse, et PPA võib garantii- ja veamenetluses uue dokumendi väljaandmise korral võtta selle kasutajalt uued biomeetrilised andmed, kui:

- olemasoleva, nõuetele mittevastava dokumendi väljaandmiseks võetud biomeetrilisi andmeid ei ole võimalik töödelda või
- dokumendi kasutaja soovib anda biomeetrilised andmed uuesti.

Dokumendi kasutaja ei pea tingimata esitama uut fotot ega andma uusi sõrmejälgi, vaid uus dokument antakse üldjuhul välja samade andmetega nagu eelmine. Vajadusel võib aga PPA võtta dokumendi kasutajalt ka uued biomeetrilised andmed, näiteks kui varem esitatud foto või antud sõrmejäljed ei ole koostalitlusvõimelises formaadis ja neid ei ole seetõttu võimalik enam töödelda. Lisaks võib inimene anda näiteks uued sõrmejäljed omal soovil, st dokument vahetatakse küll välja, kuid juhul, kui see peatselt aegub, annab sõrmejälgede ajakohastamine inimesele võimaluse taotleda uus dokument PPA iseteeninduses ilma isiklikult kohale minemata, sest sõrmejäljed on kehtivad.

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

Eelnõu § 1 punktiga 40 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. PPA menetleja koostab 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. Garantiitaotlus arhiveeritakse PPA-s ja vajadusel vormistatakse dokumendi kasutajale kirjalik kinnitus, 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. Isikusamasuse kontrollimine Eesti teabevärava mobiilirakenduse vahendusel (§ 1 p 41)

Eelnõu § 1 punktiga 41 täiendatakse **ITDS-i § 18¹ lõigetega 1¹ ja 1²**, et luua võimalus kontrollida isikusamasust, võrreldes isikut ja tema dokumendi andmeid, mis on saadud Eesti teabevärava mobiilirakenduse vahendatud kontrollpäringuga ITDAK-ist.

Muudatus on seotud Vabariigi Valitsuse tegevusprogrammi 2023–2027³⁶ eesmärgiga 3.2.4 „Loome e-riigi mobiilirakenduse, mille kaudu riik jõuab informatsiooni ja teenustega personaalselt iga eestimaalaseeni“.

Eesti teabevärava mobiilirakendus hakkab sarnaselt Eesti teabevärava veebilehega³⁷ koondama riiklikke e-teenuseid, olles Eesti teabevärava üks esitluskihte, millega võimaldatakse juurdepääs e-teenustele ja avalikule teabele ning nende tugiteenustele.

Eesti teabeväravat on reguleeritud avaliku teabe seaduse (edaspidi *AvTS*) §-s 32¹. Selle lõike 1 kohaselt on Eesti teabevärv:

veebileht, mille kaudu on kättesaadav teabevaldajate tegevusvaldkonda ja üldkasutatavaid teenuseid puudutav avalikkusele suunatud teave ning mille kaudu võimaldatakse juurdepääs elektroonilisele üldkasutatavale teenusele ja taaskasutatavale teabele.

Paragrahvi ümberkujundamiseks on MKM algatanud seaduseelnõu³⁸, mis on läbinud eelnõude infosüsteemis (EIS) esimese kooskõlastusringi. Seaduseelnõuga laiendatakse Eesti teabevärava mõistet, et see ei oleks piiratud tehnoloogiliselt veebilehega, vaid võimaldaks teabe kuvamist ka mobiilirakenduses. Termin „mobiilirakendus“ on defineeritud *AvTS*-i § 32 lõike 2 alusel kehtestatud määruse³⁹ § 1 punktis 2, mille kohaselt on see rakendustarkvara, mis on arendatud kasutamiseks mobiilseadmes ja ei hõlma mobiilseadet või riistvara kontrollivat tarkvara.

Võrreldes Eesti teabevärava veebilehega luuakse mobiilirakendusse funktsioon, millega saab turvaliselt isikusamasust kontrollida.

³⁶ Vabariigi Valitsuse 18. mai 2023. aasta korralduse nr 131 „Vabariigi Valitsuse tegevusprogrammi 2023–2027“ kinnitamine“ [lisa](#).

³⁷ [Eesti teabevärv](#).

³⁸ Eelnõude infosüsteemi toimiku nr [24-0736](#).

³⁹ Ettevõtlus- ja infotehnoloogiaministri 28. veebruari 2019. aasta määrus nr 20 „[Veebilehe ja mobiilirakenduse ligipääsetavuse nõuded ning ligipääsetavust kirjeldava teabe avaldamise kord](#)“.

Lõikega 1¹ antakse Eesti teabevärava mobiilirakenduse vahendusel isikusamasuse kontrollimisele samaväärne õiguslik tähendus, nagu on füüsilisse dokumenti kantud andmete alusel isikusamasuse kontrollimisel. Isikusamasuse kontrollimise funktsiooni eeldus on PPA ja Riigi Infosüsteemi Ameti (edaspidi *RIA*) vaheline andmevahetusleping, mille alus on omakorda AvTS-i § 32¹ ja selle lõike 5 alusel kehtestatud määrus⁴⁰.

Isikusamasuse kontrollimise funktsioon

Eesti teabevärava mobiilirakenduse vahendusel isikusamasuse kontrollimiseks peab kasutaja ennast esmalt autentima mobiil-ID või Smart-ID-ga, mille tulemusena genereeritakse rakenduses ajutine ruutkood. Ruutkood on unikaalne võti, mille genereerimisel tehakse automaatselt ITDAK-i. Teenuseosutaja, kes soovib Eesti teabevärava mobiilirakenduse vahendusel kliendi isikusamasust kontrollida, avab samuti oma seadmes selle rakenduse ja saab seda kasutades lugeda kliendi seadmest ajutist ruutkoodi. Selle tulemusena kuvatakse talle kliendi dokumendi andmed. Teenuseosutaja kontrollib kliendi isikusamasust, võrreldes füüsilises keskkonnas klienti ning ajutisest ruutkoodist avanevat dokumendifotot ja teisi isikuandmeid.

Klient saab valida, kas ta jagab teenuseosutajaga kõiki dokumendiandmeid või osa neist, näiteks ainult sünniaega ja fotot vanuse kontrolliks. Oluline on, et isikusamasuse tõendamiseks on vaja kindlasti valida ka foto jagamine teenuseosutajaga. Teenuseosutajale kuvatakse ajutisest ruutkoodist andmeid 30 sekundit.

Eesti teabevärava mobiilirakenduse vahendusel isikusamasuse kontrollimiseks on seega vaja, et oleksid täidetud kõik järgmised eeldused:

- 1) kliendil on PPA väljaantud kehtiv dokument;
- 2) teenuseosutaja on võtnud rakenduse kasutusele;
- 3) klient ja teenuseosutaja on rakendusse sisse loginud;
- 4) klient on loonud ajutise ruutkoodi;
- 5) teenuseosutaja loeb ajutist ruutkoodi rakendusega oma seadmes;
- 6) teenuseosutaja kontrollib kliendi isikusamasust, võrreldes ajutisest ruutkoodist avanevaid andmeid kliendiga.

Eesti teabevärava mobiilirakenduse vahendusel isikusamasuse kontrollimine ei ole teenuseosutajatele ega inimestele kohustuslik. Inimesed saavad seda lahendust teenuseosutaja juures kasutada juhul, kui teenuseosutaja seda võimaldab. Teenuseosutajad hindavad selle kasutusele võtmise vajadust ja võimalikkust, lähtudes nõuetest oma äriprotsessidele. Samuti ei piira võimalus kontrollida isikusamasust Eesti teabevärava mobiilirakenduse vahendusel erasektori võimalusi kasutada muid isikusamasuse kontrollimise lahendusi, kui nende tegevusvaldkonda reguleerivatest õigusaktidest ei tulene teisiti. Võimalus kontrollida isikusamasust Eesti teabevärava mobiilirakenduse vahendusel sätestatakse ITDS-is üksnes selleks, et see lisavõimalus oleks riiklikul tasandil selge ja võimalikule kasutajale oleks tagatud kindlus, et see võimalus on sobilik.

Andmed, mis on saadud Eesti teabevärava mobiilirakenduse vahendusel, ei ole eraldi digitaalne dokument ega uus dokumendiliik. Need on varem inimesele väljaantud kehtiva dokumendi andmed ja Eesti teabevärava mobiilirakendus on üksnes turvaline kanal nende kuvamiseks.

⁴⁰ Vabariigi Valitsuse 3. oktoobri 2013. aasta määrus nr 145 „[Eesti teabevärava eesti.ee haldamise, teabe kättesaadavaks tegemise, arendamise ning kasutamise nõuded ja kord](#)“.

Isikusamasuse kontrollimise funktsiooni kasutamise juhud

Eesti teabevärava mobiilirakenduse vahendusel isikusamasuse kontrollimist piiratakse üksnes nii, et see on välistatud ITDS-i alusel dokumendi taotlemise ja väljastamise korral (vt ITDS-i § 18 lg 1² selgitust). Muudel juhtudel otsustab teenuseosutaja ise, kas võtta see võimalus kasutusele, lähtudes sellest, kas tema tegevusvaldkonnas on sätestatud isikusamasuse kontrollimise kohta kohustusi või piiranguid ning kas ta soovib ja on valmis seda võimalust kasutama.

RIA näeb võimalike kasutusjuhtudena näiteks täisealisuse tõendamist kaupluses, kui ostetakse alaealisele keelatud tooteid, või sissepääsul vanusepiiranguga ürituse korral, aga ka näiteks broneeringueelset isikusamasuse tõendamist meditsiini- või majutusasutuses. Tegelikud kasutusjuhud selguvad turutingimustel nõudluse ja pakkumuse tulemusena ning ei pruugi kirjeldatud kasutusjuhte hõlmata.

Isikusamasuse kontrollimise funktsiooni turvalisus

Eesti teabevärava mobiilirakendus on küberturvalisuse seaduse tähenduses võrgu- ja infosüsteem ning peab vastama selle seaduse nõuetele. Seega peab Eesti teabevärava mobiilirakendus vastama rangetele turvanõuetele. Tagatud peab olema isikuandmete kaitstud ja selle kasutamisel seos kasutajaga. Välistatud peab olema nii valeandmete kuvamine kui ka võltsitud mobiilirakenduse kasutamine. Eesti teabevärava mobiilirakenduse vahendusel isikusamasuse kontrollimine logitakse, et rakenduse haldajal oleks võimalik tagada selle kasutamise seaduslikkus. Näiteks sisaldavad logiandmed teavet ajutise ruutkoodi genereerimise algatamise, X-tee päringu tegemise ja vastuse saamise ning ruutkoodi lugemise kohta.

Eesti teabevärava mobiilirakenduse turvalisuse tagab seega muu hulgas see, et RIA rakendab Eesti infoturbestandardit⁴¹ ja järgib küberturvalisuse seaduse nõudeid. Praktikas tähendab see, et RIA-s on olemas infoturbe halduse süsteem ning tegevuskava RIA äriprotsesside kaitseks ja infoturbe-eesmärkide saavutamiseks. Eesti teabevärava mobiilirakenduse arendamisel rakendatakse küberintsidendite ennetuseks infoturbemeetmeid. Näiteks on kohustuslik korraldada läbistustestimist⁴² ja ilmnunud kriitilised vead enne kasutusse andmist parandada. Kuigi kõiki infoturbemeetmeid ei ole võimalik otstarbekuse ega turvalisuse kaalutlustel loetleda, on RIA läbinud kohustuslikud auditid. 2024. aasta aprillis tehti Eesti infoturbestandardi auditis järeldusotsus, mille kohaselt on Eesti teabevärava mobiilirakenduse turvalisus RIA infoturbe halduse süsteemi ja selle infoturbemeetmetega saavutatav.

Euroopa Liidu digiidentiteedikukkur

Uued lahendused, nagu Eesti teabevärava mobiilirakendus, peavad arvestama rahvusvaheliste ja Euroopa Liidu suundadega, toetama olemasolevat Eesti eID ökosüsteemi ja olema võimalusel omavahel koosmõjus. Seetõttu arvestatakse Eesti teabevärava mobiilirakenduse arendamisel Euroopa Liidu eIDAS-e 2.0 määrusest tuleneva kohustusega võtta kasutusele digiidentiteedikukkur: rakenduse isikusamasuse kontrollimise funktsioon põhineb eIDAS-e 2.0 digiidentiteedikukku standardlahendusel. Samas ei rakendata eelnõuga otseselt eIDAS-e 2.0 määrust ega kohustust luua digiidentiteedikukkur. Euroopa Liidu määrused on liikmesriikidele otsekohalduvad ja MKM-i eestvedamisel analüüsitakse, kas ja millisel määral tuleb riigisisest õigust muuta. Eesti teabevärava mobiilirakendus võetakse kasutusele vaid Eesti piires.

⁴¹ Ettevõtlus- ja infotehnoloogiainistri 16. detsembri 2022. aasta määrus nr 101 „Eesti infoturbestandard“.

⁴² Läbistustestimine on sissetungirünnete imiteerimine turvameetmete toimivuse kontrollimiseks. – [AKIT](#).

Lõikega 1² sätestatakse piirang, et Eesti teabevärava mobiilirakenduse vahendusel ei tohi isikusamasust kontrollida ITDS-i alusel dokumendi taotlemise ja väljastamise korral.

Dokumendi väljaandmisele, sealhulgas isiku tuvastamisele ja isikusamasuse kontrollimisele, kohalduvad väga ranged piirangud ning rahvusvahelised standardid ja nõuded. Eesti kodaniku dokumendi esmaväljaandmisel määrab PPA dokumendi taotleja alusidentiteedi, mis on seotud väljaantava dokumendiga ja mida kasutatakse edaspidi isikusamasuse kontrollimisel nii füüsilises kui ka e-keskkonnas. Kui reisidokumendi väljaandmisele kohalduvad Rahvusvahelise Tsiviillennundusorganisatsiooni (ICAO) nõuded, siis digitaalset tuvastamist ja digitaalset allkirjastamist võimaldavatele dokumentidele, nagu isikutunnistus, elamisloakaart ja digitaalne isikutunnistus, sealhulgas mobiil-ID, kohaldub eIDAS-e määrus, milles on seatud ranged piirangud dokumendi väljaandmisele ja identiteedi kontrollimisele⁴³. Dokumendi väljaandmise protsessi muudatustest tuleb teavitada Euroopa Komisjoni ja läbida Euroopa Liidu liikmesriikide vastavushindamine.

Põhimõtet, et isikusamasust ei tohi dokumendi taotlemise ja väljastamise korral kontrollida Eesti teabevärava mobiilirakenduse vahendusel, on võimalik tuletada ka, kui tõlgendada ITDS-i erinevate dokumendi taotlemisel ja väljastamisel isiku tuvastamise ja isikusamasuse kontrollimise kohta. Dokumendi väljaandmisel peab PPA, järgides menetlusreegleid, tõsikindlalt veenduma isiku isikusamasuses, mille alusel luuakse alusidentiteet ja millest lähtutakse edaspidi alati isikusamasuse kontrollimisel. Seetõttu on õigusselguse huvides oluline selline keeld sõnaselgelt ITDS-is sätestada.

Andmekaitsealane mõjuhindang

Isikuandmete kaitse üldmääruse artikli 35 lõike 3 kohaselt peab andmekaitsealase mõjuhindangu tegema järgmistel juhtudel:

- a) füüsiliste isiklike aspektide süstemaatiline ja ulatuslik hindamine, mis põhineb automaatsel isikuandmete töötlemisel, sealhulgas profiilianalüüsil, ja millel põhinevad otsused, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut;
- b) artikli 9 lõikes 1 osutatud andmete eriliikide või artiklis 10 osutatud süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud andmete ulatuslik töötlemine;
- c) avalike alade ulatuslik süstemaatiline jälgimine.

Eesti teabevärava mobiilirakenduse vahendusel isikusamasuse kontrollimisel ei esine ühtegi nendest olukordadest. Seega ei ole andmekaitsealane mõjuhindang kohustuslik. Isikusamasuse kontrollija ei salvesta andmeid, mis on saadud Eesti teabevärava mobiilirakenduse vahendatud kontrollpäringuga, ja päringu kehtivusaeg on piiratud.

3.2.8. Digitaalsete andmete kehtivusaeg (§ 1 p-d 42 ja 58)

Eelnõu § 1 punktidega 42 ja 58 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

⁴³ Kontrollimiseks kasutatakse üht järgmistest identimismeetoditest: a) füüsiline kohalolek, b) kaughindamine, kui eelmisel korral tagati füüsiline kohalolek, c) kvalifitseeritud e-allkiri või kvalifitseeritud e-templi sertifikaat koos kõlas punktidega a ja b või d) muu riiklikult tunnustatud identimismeetod, mis on samaväärne füüsilise kohalolekuga.

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 4 ja 5)

Eelnõu § 1 punktiga 4 muudetakse **ITDS-i § 9¹ lõiget 2**. Praegu saab selle kohaselt 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 5 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 algupärase kujul reisidokumendi märkustelehele ja kanne kinnitatakse pitsatiga. Praktikast kantakse algupärane isikunimi küll endiselt reisidokumendi märkustelehele, 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 6 ja 20)

Eelnõu § 1 punktidega 6 ja 20 täiendatakse **ITDS-i § 9² lõigetega 6¹–6³ ja § 11⁷ lõikega 3**.

Kehtiva õiguse⁴⁴ kohaselt peab dokumendi taotleja, kellele ei ole antud varem välja Eesti kodaniku passi ega isikutunnistust, lisama taotlusele Eesti kodakondsusesse kuulumise tuvastamist võimaldava dokumendi ning oma mõlema vanema nime, kodakondsuse, isikukoodi või sünniaja ja -koha.

ITDS-i § 9² lõikega 6¹ antakse PPA-le õigus nõuda kindlatel 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 kodakondsust tõendav dokument ei ole ehtne või selle alusandmed ei ole õiged. PPA nõuab DNA-ekspertiisi vaid üksikutel juhtudel, kui isadus on omaks võetud aastaid pärast välismaalase sünni registreerimist või vahetult enne dokumendi taotlemist ja PPA-l on alust kahelda esitatud tõendite ehtsuses või andmete õigsuses. Kui PPA-l on võimalik tuvastada dokumendi taotleja põlvnemine muul meetodil, siis DNA-ekspertiisi kui kõige riivavamat meetodit ei kasutata ja Eesti kodakondsus tuvastatakse näiteks lisatõendite või -andmete alusel või dokumendi ekspertiisiga.

Praktikas on saagenud olukorrad, kus Venemaa või Valgevene kodanik soovib tõendada, et ta põlvneb Eesti kodanikust, kuid esitatud tõendites või andmetes on põhjust kahelda. Muudatus puudutab väga väikest rühma välismaalasi, kes esitavad PPA-le dokumendi esmataotluse, tõendades Eesti kodakondsust põlvnemise tuvastamise kaudu, ja kelle suhtes tekib PPA-l põhjendatud kahtlus, kas Eesti kodakondsust tõendav dokument või selle alusandmed on õiged.

⁴⁴ 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](#)“ § 10, § 13 lõige 1 ja § 26 lõige 1.

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 omaksvõtu tunnistusi. Kohtumenetluses on seni suudetud vale-tõendite ja -andmete esitamist tõendada.

Kõikides senistes kohtuasjades on Eesti kodanikke 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 põlvnemise kohta DNA-ekspertiisi tulemus. Kui dokumendi taotleja sellest keeldub, suurendab see selgelt kahtlust, kas tal on õigus Eesti kodakondsusele ja dokumendile. Kui dokumendi taotleja 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. Kui aga dokumendi taotleja keeldub DNA-ekspertiisist, mille tulemusena jätab PPA dokumendi taotluse läbi vaatamata, on tal endiselt võimalik pöörduda kohtusse.

DNA-ekspertiisi tehakse nagu tavalist tasulist ekspertiisi. PPA DNA-ekspertiisi tellimist ei vahenda, vaid dokumendi taotleja läheb ise Eesti Kohtuekspertiisi Instituuti ja tellib DNA-ekspertiisi. Eesti Kohtuekspertiisi Instituut sõlmib DNA-ekspertiisi tellinud dokumendi taotlejaga lepingu ja väljastab eksperdiarvamuse, mille dokumendi taotleja esitab PPA-le.

DNA-ekspertiisi tellinud dokumendi taotleja isikuandmeid töödeldakse isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkti a alusel, mille kohaselt annab andmesubjekt selleks selgesõnalise nõusoleku. Tema selgesõnaline nõusolek väljendub tasulise DNA-ekspertiisi tellimiseks Eesti Kohtuekspertiisi Instituudiga sõlmitud lepingus. Kohtuekspertiisiseaduse § 12 lõike 1 punkti 2 kohaselt ei tehta tasulist ekspertiisi anonüümselt, vaid tellija tagab, et selle tegemisse või tulemusse puutuv isik või tema seaduslik esindaja on ekspertiisi tegemiseks andnud ekspertiisiasutusele nõusoleku.

DNA-ekspertiisi tulemusel saadud eksperdiarvamus salvestatakse ITDAK-i ning selle andmeid töödeldakse ja säilitatakse sama korra kohaselt, mis kehtib muude Eesti kodaniku dokumendi esmataotlemisel esitatud ja ITDAK-i kantud tõendite kohta. Eesti kodaniku dokumendi esmataotlemisel kogutud andmeid säilitatakse tähtajatult.

ITDS-i § 9² lõike 6² kohaselt tellib DNA-ekspertiisi ja katab selle kulud dokumendi taotleja. Kohtuekspertiisiseaduse § 11 lõike 5 alusel kehtestatava korra⁴⁵ kohaselt maksab DNA-ekspertiis ühe isiku DNA analüüsimise eest 70 eurot.

ITDS-i § 9² lõikega 6³ antakse PPA-le õigus edastada Eesti Kohtuekspertiisi Instituudile DNA-ekspertiisiga seotud isiku ees- ja perekonnanime ning isikukoodi või selle puudumise korral sünniaja. Samuti antakse PPA-le õigus saada Eesti Kohtuekspertiisi Instituudilt DNA-ekspertiisi andmeid. DNA-ekspertiisi andmeid ei või kasutada muudes menetlustes.

ITDS-i § 11⁷ lõike 3 kohaselt jäetakse dokumendi taotlus läbi vaatamata, kui dokumendi taotlejale ei ole tehtud PPA nõudmisel DNA-ekspertiisi 90 päeva jooksul. Muudatus puudutab väikest hulka välismaalasi, kes esitavad PPA-le Eesti kodaniku dokumendi esmataotluse ja soovivad tõendada Eesti kodakondsust hilisema isaduse omaksvõtu kaudu. Kui PPA-l tekib põhjendatud kahtlus Eesti kodakondsust tõendava dokumendi või selle alusandmete õigsuses,

⁴⁵ 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 ekspertiiside ja uuringute hinnad](#)“ § 1 lõike 1 punktis 3 kehtestatud hinnale.

annab PPA taotluse kohta puuduste kõrvaldamise määruse, 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 määruse kättetoimetamisest.

3.3.3. Isikuandmete töötlemine teate saatmiseks (§ 1 p 7)

Eelnõu § 1 punktiga 7 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-is sätestatud menetluse või selles väljaantud dokumendi kohta teateid, näiteks dokumendi väljaandmise menetluse oleku või dokumendi kehtivusaja lõppemise kohta, kasutades selleks varasema dokumendi väljaandmise menetluse andmeid.

3.3.4. Dokumendi taotlemine vanglas (§ 1 p-d 15 ja 16–19)

Eelnõu § 1 punktiga 15 muudetakse **ITDS-i § 11³ lõiget 3 ja § 12² lõiget 2**, et asendada ITDS-is termin „vanglatöötaja“ JUM-i ettepanekul terminiga „kinnipidamisasutuse volitatud ametnik või töötaja“. Muudatus on tehniline. Terminit ei muudeta ITDS-i § 40² lõikes 3, sest see on rakendussäte, milles on reguleeritud biomeetriliste andmetega dokumentide kasutuselevõtu erisusi. Biomeetriliste andmetega dokumendid võeti kasutusele 2007. aastal ja dokumendi kasutaja sõrmejäljega passe hakati väljastama 2009. aastal. Seega on see lõige kaotanud aktuaalsuse.

Eelnõu § 1 punktidega 16–19 muudetakse **ITDS-i § 11⁵ lõikeid 4 ja 6**, täiendatakse paragrahvi **lõigetega 4^{1–4}3** 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 reisidokumenti. 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, sealhulgas ennetähtaegset vabastamist. 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 kinnipidamisasutuse volitatud ametnik või töötaja edastab kinnipeetava dokumendi taotluse PPA-le. Samuti kontrollib kinnipidamisasutuse volitatud ametnik või töötaja 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 kinnipidamisasutuse volitatud ametnikul või töötajal võtta dokumendi väljaandmise menetluses ise kinnipeetava sõrmejäljed. Kinnipidamisasutuse volitatud ametnik või töötaja 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 kinnipidamisasutuse volitatud ametnik või töötaja ITDS-i § 15 lõike 6 alusel kehtestatud sõrmejälgede võtmise korda⁴⁶;
 - võetud biomeetrilised andmed kantakse ABIS-esse.
- 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, kui kinnipidamisasutuse volitatud ametnik või töötaja ei saa tehnilistel põhjustel neid andmeid võtta või PPA-le edastada.

Kinnipeetava dokumendi taotlusi ei ole palju: 2023. aastal oli neid augusti lõpu seisuga 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 kinnipidamisasutuse volitatud ametnik või töötaja lisab taotlusele kinnituse kinnipeetava põhjendatud 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. Kuna kinnipeetava vajadust dokumenti taotleda tuleb edaspidi põhjendada igal juhul ja kinnipeetavaga suhtleb otse kinnipidamisasutuse volitatud ametnik või töötaja, oskab dokumendi taotlemise vajadust ja selle põhjendatust hinnata kõige paremini just tema. Seega ei ole otstarbekas koormata dokumendi taotlemise vajaduse kinnitamisega vangla direktorit.

3.3.5. Dokumendi väljastamine (§ 1 p-d 21–24 ja 55) ja väljaandja termin (§ 1 p-d 27 ja 29)

Eelnõu § 1 punktidega 21 ja 22 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 vastuvõtmise 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

⁴⁶ Siseministri 30. novembri 2015. aasta määrus nr 56 „[Elamisloa ja elamisõiguse menetluses ning isikut tõendava dokumendi väljaandmise menetluses sõrmejälgede võtmise kord](#)“.

rakendamise saab võimalikuks ka ID-1 formaadis dokumentide kulleriga kättetoimetamine nii välismaal kui ka Eestis. Seetõttu on regulatsiooni täpsustamine vältimatult vajalik.

Eelnõu § 1 punktiga 23 täiendatakse **ITDS-i § 12¹ lõikega 2⁶**. Uue ID-1 formaadis dokumentide tootmise lepingu rakendamine 15. novembrist 2025 toob dokumendi väljaandmise menetluses kaasa mitmeid uuendusi. Lõikega 2⁶ võetakse uue lepingu rakendamise järel⁴⁷ kasutusele mugav lahendus, mille abil saab dokumendi taotleja, autentides end e-keskkonnas kehtiva eID vahendiga⁴⁸, 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 24 ja 55 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 menetlustoiminguid 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 27 ja 29 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.

3.3.6. Välismaalase passi väljaandmise alus (§ 1 p-d 56 ja 57)

Eelnõu § 1 punktidega 56 ja 57 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 kodakondsusjärgse riigi 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 kodakondsusjärgse riigi 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 välismaalase passi regulatsiooni ja kes ei saa oma kodakondsusjärgse riigi reisidokumenti, on võimalik anda välja ajutine reisidokument.

2024. aasta mai seisuga oli kehtivaid välismaalase passe 52 423. Ajutisi reisidokumente antakse aastas välja umbes 150.

⁴⁷ Muudatus eeldab vähemalt kuuekuulist arendusaega pärast ID-1 formaadis dokumentide tootmise lepingu rakendamist.

⁴⁸ Isikutunnistus, elamisloakaart ja digitaalne isikutunnistus, sealhulgas mobiil-ID.

3.3.7. Isiku daktüloskopeerimine tagasipöördumisdokumendi taotlemise korral (§ 1 p-d 59–61)

Eelnõu § 1 punktidega 59–61 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 32–38, §-ga 2, § 3 punktidega 3 ja 4, §-dega 4, 5, 7 ja 8, § 9 punktidega 11–26 ning §-ga 10 korrastatakse andmekogude regulatsiooni, tuues muu hulgas põhimäärusest seaduse tasandile andmekogudes andmete säilitamise maksimaalse tähtaja ning nende andmete koosseisu, mida töödeldakse ABIS-es, 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 33 ja 35)

Eelnõu § 1 punktiga 33 täpsustatakse ITDS-i § 15² lõikes 3 ITDAK-i andmekoosseisu ja punktiga 35 täiendatakse paragrahvi lõikega 5² andmete säilitamise tähtaja kohta. Praegu on ITDAK-i täpne andmekoosseis sätestatud ITDAK-i põhimääruses⁴⁹. Samuti on ITDAK-i andmete säilitamise tähtjad sätestatud ITDAK-i ja ABIS-e põhimääruses⁵⁰. Dokumendi väljaandmise menetluses võetud biomeetrilised andmed kantakse ITDAK-i kaudu ABIS-esse, kus neid ka säilitatakse (vt seletuskirja p 3.4.2).

Andmekoosseis

Eelnõuga sätestatakse ITDAK-i andmekoosseis, mis on praegu ITDAK-i põhimääruses, ka ITDS-is. 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

⁴⁹ Siseministri 18. detsembri 2015. aasta määrus nr 78 „[Isikut tõendavate dokumentide andmekogu pidamise põhimäärus](#)“.

⁵⁰ Vabariigi Valitsuse 23. detsembri 2021. aasta määrus nr 125 „[Automaatse biomeetrilise isikutuvastuse süsteemi andmekogu põhimäärus](#)“.

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.

1) **Isikuandmed** (p-d 1–3 ja 7)

ITDAK-i kantakse dokumendi taotleja ja kasutaja kohta:

- üldandmed: ees- ja perekonnanimi, isikukood või selle puudumise korral sünniaeg, sugu, kodakondsus, kontaktandmed (aadress, e-posti aadress ja telefoninumber) ning emakeel;
- sünnikoht;
- rahvus;
- kasutaja sünnitunnistuse andmed ja Eesti kodakondsust tõendava dokumendi andmed;
- ema ja isa ees- ja perekonnanimi, isikukood või selle puudumise korral sünniaeg, sünnikoht ning kodakondsus.

PPA üks põhiülesanne on PPVS-i § 1 lõike 2 järgi kodakondsuse ja migratsiooni valdkonna asjade korraldamine. See hõlmab ka ITDS-i § 15 lõike 4 alusel dokumentide väljaandmist. Dokumendi väljaandmisel on oluline veenduda, et isik on see, kes ta väidab end olevat ja et riikliku staatust tõendav dokument antakse välja selleks õigustatud isikule. Isikuandmeid töödeldakse dokumendi väljaandmise menetluses isiku tuvastamiseks või isikusamasuse kontrollimiseks, isiku õigusliku staatuse kontrolliks ja andmete dokumenti kandmiseks.

Sünnitunnistuse, Eesti kodakondsust tõendava dokumendi ja vanemate andmed kantakse ITDAK-i vaid juhul, kui isik taotleb Eesti kodaniku dokumenti esimest korda ja see on vajalik tema Eesti kodakondsuse tõendamiseks.

E-residendi digi-ID taotlemise korral kantakse ITDAK-i lisaks eelloetletud andmetele taotleja:

- varasemad ja muud nimed, sealhulgas isanimi;
- varasemad kodakondsused;
- välisriigi isikukood ning
- sotsiaalmeediakontode andmed.

Need andmed kantakse ITDAK-i juhul, kui e-residendi digi-ID taotleja on need esitanud. Andmete töötlemise vajadust on põhjendatud siseministri 22. veebruari 2021. aasta määruse nr 11 „Siseministri määruste muutmine seoses isikut tõendava dokumendi menetluses kogutavate andmete täpsustamisega“ eelnõu seletuskirjas⁵¹.

2) **Biomeetrilised andmed** (p 4)

ITDS-i § 9² lõikes 2 on sätestatud, mis andmed on ITDS-i tähenduses biomeetrilised andmed. Dokumendi väljaandmise menetluses töödeldakse näokujutist või fotot, sõrmelälekujutisi ja allkirja või allkirjakujutist.

Kohustus töödelda dokumendi väljaandmisel biomeetrilisi andmeid tuleneb Euroopa Liidu õigusest⁵². ITDS-i § 11⁶ lõike 1 kohaselt on dokumendi taotleja kohustatud võimaldama

⁵¹ Eelnõude infosüsteemi toimiku nr [21-0091](#).

⁵² Euroopa Parlamendi ja nõukogu 28. mai 2009. aasta määrus (EÜ) nr 444/2009, millega muudetakse nõukogu määrust (EÜ) nr 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria

enda sõrmejälgedele ja näokujutise võtmist ning nende andmete töötlemist. Sõrmejäljed ja näokujutis või foto kantakse ja neid säilitatakse ABIS-es⁵³. Allkirjakujutist, mis kantakse dokumendile, säilitatakse ITDAK-is.

Juhul, kui taotlejalt ei ole võimalik sõrmejälgi võtta, näiteks kui sõrmed puuduvad, kantakse ITDAK-i andmed sõrmejälgedele võtmise võimatuse kohta (vt täpsemalt alapunkt 6).

Sõrmejälgedele võtmise kohustust ja selle mõju on käsitletud siseministri 12. augusti 2021. aasta määruse nr 20 „Siseministri määruste muutmine seoses isikut tõendava dokumendi menetluses kogutavate andmete täpsustamisega“ eelnõu seletuskirjas⁵⁴.

3) Taotlemise eesmärk ja plaanitava tegevuse kirjeldus ning taotlemise põhjendus (p 15)

- a) Ajutine reisidokument. ITDS-i § 29 lõike 1 kohaselt võib Eestis viibivale välismaalasele anda ajutise reisidokumendi Eestist lahkumiseks ja Eestisse tagasipöördumiseks. Ajutine reisidokument antakse väga piiratud alustel ja ainult põhjendatud vajaduse korral, kui välismaalasel puudub kehtiv reisidokument või välisriik on talle andnud tagasipöördumistunnistuse ja tal ei ole õigust saada välismaalase passi. Üldjuhul dokumenteerib oma kodanikke ja annab neile reisidokumente kodakondsusjärgne riik ise. Kuna ajutise reisidokumendi andmine on pigem erandlik, kantakse selle taotlemise korral ITDAK-i taotlemise põhjendus.
- b) Eesti kodaniku lisapass. Taotlemise põhjendus kantakse ITDAK-i ka Eesti kodaniku lisapassi taotlemise korral. Eesti kodanikul on õigus omada samal ajal kahte Eesti kodaniku passi. Lisapassi taotlemise vajadust peab aga põhjendama, sest üldjuhul tunnistatakse uue samaliigilise dokumendi taotlemise korral varasem dokument kehtetuks. Lisapassi vajadus võib tuleneda näiteks viisa taotlemisest, mille korral tuleb pass anda Eesti välisesindusele, kuid samal ajal võib inimesel olla passi vaja ka reisimiseks.
- c) E-residendi digi-ID. E-residendi digi-ID taotlemise korral kantakse ITDAK-i nii taotlemise eesmärk, plaanitava tegevuse kirjeldus kui ka taotlemise põhjendus. ITDS-i § 20⁵ lõike 2 kohaselt on e-residendile digi-ID väljaandmise eesmärk soodustada Eesti majanduse, teaduse, hariduse või kultuuri arengut. Seega peab selle taotleja suutma kirjeldada ja põhjendada, mis eesmärgil ja mis tegevuseks ta e-residendi digi-ID-d taotleb. E-residentsuse kontseptsiooni ja eesmärki on selgitatud isikut tõendavate dokumentide seaduse ja riigilõivuseaduse muutmise seaduse eelnõu⁵⁵ seletuskirjas ja selle lisas 1 „E-residendi digi-ID kontseptsioon“.

3) Eluloolised andmed

- a) Hariduse andmed (p 5). Dokumendi taotluses küsitakse taotleja ja kasutaja hariduse andmeid. Nende esitamine on vabatahtlik⁵⁶ ja neid kogutakse statistilistel eesmärkidel rahvastikuregistri andmete uuendamiseks.

standardite kohta. – [ELT L 142, 6.6.2009, lk 1–4](#); Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta määrus (EL) 2019/1157 liidu kodanike isikutunnistuste ning vaba liikumise õigust kasutavatele liidu kodanikele ja nende pereliikmetele väljaantavate elamislubade turvalisuse suurendamise kohta. – [ELT L 188, 12.7.2019, lk 67–78](#).

⁵³ ABIS-e õiguslik alus loodi isikut tõendavate dokumentide seaduse ja teiste seaduste muutmise seadusega ([RT I, 08.07.2021, 1](#)). Selle põhjendused on eelnõu [366 SE](#) seletuskirjas.

⁵⁴ Eelnõude infosüsteemi toimiku nr [21-0520](#).

⁵⁵ [699 SE](#).

⁵⁶ Siseministri 18. detsembri 2015. aasta määruse nr 77 „[Isikutunnistuse, elamisloakaardi, digitaalse isikutunnistuse, Eesti kodaniku passi, meremehe teenistusraamatu, välismaalase passi, ajutise reisidokumendi, pagulase](#)

- b) Koduteeninduse avalduse andmed (p 6). ITDS-i § 11⁵ lõike 1 kohaselt võib PPA võtta dokumendi taotluse vastu, tuvastada taotleja isiku või kontrollida tema isikusamasust ja võtta talt biomeetrilised andmed tema elu- või viibimiskohas Eestis, kui taotleja tervise- seisund püsivalt ei võimalda tal isiklikult PPA-sse pöörduda. Sellisel juhul peab taotleja esitama avalduse, mille andmed kantakse ITDAK-i.
- c) Ajutine reisidokument (p 11). ITDS-i § 29 lõike 1 kohaselt võib Eestis viibivale välismaalasele anda ajutise reisidokumendi Eestist lahkumiseks ja Eestisse tagasipöördumiseks. Ajutine reisidokument antakse väga piiratud alustel ja ainult põhjendatud vajaduse korral, kui välismaalasel puudub kehtiv reisidokument või välisriik on talle andnud tagasipöördumistunnistuse ja tal ei ole õigust saada välismaalase passi. Üldjuhul dokumenteerib oma kodanikke ja annab neile reisidokumente kodakondsusjärgne riik ise. Kuna ajutise reisidokumendi andmine on pigem erandlik, peab selle taotleja põhjendama, miks tal on seda vaja, ja esitama lisaandmed: Eestist lahkumise põhjuse ja riigi, kuhu ta lahkuib.⁵⁷
- d) Staatuse andmed (p 9). Välismaalasele taotlejale dokumendi väljaandmise alus on tema õiguslik staatus. PPA-l on kohustus veenduda, et dokument antakse välja vaid sellele, kellel on selleks õigus. Seetõttu kantakse ITDAK-i andmed taotleja elamisloa või elamisõiguse kohta, või kui taotleja viibib Eestis riigikaitseaduse alusel, siis muu Eestis viibimise loa või staatuse kohta.
- e) E-residendi digi-ID taotlemise lisaandmed (p-d 10 ja 12–21). E-residendi digi-ID taotlemise korral kantakse ITDAK-i taotleja kohta lisaks isikuandmetele:
- e-residendi staatuse andmed;
 - temaga seotud ettevõtja ja ettevõtluse andmed;
 - elulookirjeldus;
 - talle mõistetud või määratud karistuse andmed;
 - andmed selle kohta, kas teda kahtlustatakse või süüdistatakse või on kahtlustatud või süüdistatud majandus-, küber- või terrorikuriteos;
 - talle viisa andmisest keeldumise ja sissesõidukeelu kohaldamise andmed;
 - ajateenistuses, relvajõududes, kaadrisõjaväelasena või luure- või julgeolekuteenistuses teenimise ja töötamise andmed, väljaspool Eestit sõjaväelises operatsioonis osalemise andmed ning riiklikus või mitteriiklikus relvastatud organisatsioonis või üksuses teenimise andmed;
 - ühiskondlikusse organisatsiooni kuulumise andmed;
 - terroriorganisatsiooni kuulumise andmed.

Võrreldes ITDAK-i põhimäärusega ei nimetata eraldi rahapesukuriteo kahtlust ja süüdistust. See ei tähenda, et selle kohta andmeid enam ei küsita, vaid arvestades, et karistusseadustikus on rahapesualased süüteod 21. peatükis „Majandusalased süüteod“, on rahapesukuritegu hõlmatud terminiga „majanduskuritegu“⁵⁸.

[reisidokumendi või meresõidutunnistuse väljaandmise taotlemisel esitatavate tõendite ja andmete loetelu, väljastamise kord ning väljaandmise tähtsused](#) § 24 lg 6.

⁵⁷ Sealsamas, § 31.

⁵⁸ Ka [Euroopa Liidu terminoloogia andmebaasis](#) on rahapesukuritegu käsitatud majanduskuriteo liigina.

Eelloetletud andmete töötlemise vajadust on põhjendatud siseministri 22. veebruari 2021. aasta määruse nr 11 „Siseministri määruste muutmine seoses isikut tõendava dokumendi menetluses kogutavate andmete täpsustamisega“ eelnõu seletuskirjas⁵⁹.

4) Esindaja andmed (p 8)

ITDS-i § 11², § 11⁴ lõike 1 ja § 12¹ lõike 2¹ kohaselt võib dokumenti taotleda ja selle väljastada ka dokumendi taotleja ja kasutaja seadusliku või volitatud esindaja kaudu. Sellisel juhul on oluline veenduda esindaja isikusamasuses ja tema esindusõiguses. ITDAK-is töödeldakse esindaja:

- üldandmeid: ees- ja perekonnanimi ning isikukood;
- esindusõiguse andmeid.

5) Dokumendi andmed (p 24)

Dokumendi väljaandmise menetluses kantakse ITDAK-i ka välismaalase:

- reisidokumendi andmed: reisidokumendi väljaandnud riik ja asutus, liik, number, väljaandmise aeg ja kehtivusaja lõppemise aeg;
- andmed Eesti elamisloa või elamisõiguse kohta.

Nende andmete töötlemine on vajalik, et tuvastada välismaalase isik või kontrollida tema isikusamasust ja veenduda, et tal on õigus konkreetset dokumenti omada.

6) Terviseseisundi andmed (p 6)

ITDAK-is töödeldakse dokumendi taotleja ja kasutaja tervisetõendi ja puuet tõendava dokumendi andmeid.

- ITDS-i § 11⁵ lõike 1 kohaselt võib PPA võtta isikult dokumendi taotluse vastu, tuvastada tema isiku või kontrollida tema isikusamasust ja võtta temalt biomeetrilised andmed tema elu- või viibimiskohas Eestis, kui isiku terviseseisund püsivalt ei võimalda tal dokumendi taotluse esitamiseks isiklikult PPA-sse pöörduda ja isiklik pöördumine on nõutav.
- ITDS-i § 11⁶ lõike 5 kohaselt ei võeta sõrmejälgi isikult, kellel puuduvad kõik sõrmed või kelle püsiv terviseseisund ei võimalda seda teha. Sama paragrahvi lõike 6 kohaselt ei võeta sõrmejälgi ka isikult, kellelt ei ole ajutiselt võimalik tema terviseseisundi tõttu sõrmejälgi võtta. Kui isikult ei ole tema terviseseisundi tõttu ajutiselt võimalik sõrmejälgi võtta ega seetõttu sõrmejäljekujutisi dokumenti kanda, ei tohi ITDS-i § 11⁶ lõike 7 kohaselt talle väljaantava dokumendi kehtivusaeg ületada ühte aastat.
- ITDS-i § 12² lõike 1 kohaselt võib dokumendi väljastaja anda dokumendi kasutaja kirjalikul nõusolekul dokumendi väljastamiseks üle valla- või linnavalitsuse või hoolekandeametuse juhi volitatud töötajale, kui dokumendi kasutaja viibib Eestis, aga tema terviseseisund püsivalt ei võimalda tal dokumendi kättesaamiseks isiklikult dokumendi väljastaja asukohta ilmuda. Sama paragrahvi lõike 3 kohaselt võib Eesti kodanik või tema seaduslik esindaja kirjalikult taotleda Eesti välisesinduselt dokumendi väljastamist oma viibimis- või elukohas, kui ta viibib välisriigis kinnipidamis- või hoolekandeametuses või kui tema terviseseisund püsivalt ei võimalda tal dokumendi kättesaamiseks isiklikult Eesti välisesindusse pöörduda.

⁵⁹ Eelnõude infosüsteemi toimiku nr [21-0091](#).

Kõigil kirjeldatud juhtudel peab isik ise tõendama, et isiklik pöördumine ei ole tervise- seisundi tõttu võimalik. Praktikaks esitatakse selleks PPA-le perearsti tervisetõend. Seetõttu on vaja töödelda ka selle andmeid. Puude tõendamine on vajalik riigilõivu soodustuse saamiseks.

Andmete säilitamise tähtaeg

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 menetleda dokumendi taotlusi, vaid tagada ka avalik kord ja riigi julgeolek, võimaldades tuvastada riikliku identiteedi saanuid. 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 tähtajatult** ITDAK-i kandmisest arvates. Tähtajatult 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 õiguse Eesti kodakondsusele ka mitmenda põlve järeltulijale, on vaja neid andmeid säilitada tähtajatult. Kui neid andmeid säilitada lühemalt, ei ole võimalik ITDAK-i pidajal täita selle pidamise põhieesmärki tagada avalik kord ja riigi julgeolek. Teisi ITDS-i alusel ITDAK-i kantud andmeid säilitatakse **kuni 75 aastat** ja nendele võib kehtestada lühema säilitustähtaja ITDAK-i põhimääruses.

Isikuandmete säilitamist käsitatakse eraelu puutumatusena. Konkreetse säilitustähtaja sätestamine seaduse tasandil aitab kaasa läbipaistvale andmetöötlemisele.

3.4.2. ABIS-e andmete säilitamise tähtajad (§ 1 p 38, § 2 p 9, § 3 p 4, § 4 p 3, § 7 p 3, § 9 p-d 16, 25 ja 26 ning § 10 p 3)

- 1) **ITDS-i § 15⁴ lõikes 6¹** sätestatakse, et **ITDS-i** alusel ITDAK-i kaudu ABIS-esse kantud andmeid säilitatakse **kuni 75 aastat** (eelnõu § 1 p 38). 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. ITDAK-i andmeid on vaja kasutada läbi kogu inimese elu. Teatud juhtudel on vaja inimese andmeid ka pärast tema surma, näiteks põlvnemis- ja kodakondsusküsimustes või identiteedikonflikti lahendamisel. Kuna inimeste keskmine eluiga aja jooksul pikeneb, ei ole ABIS-e põhimääruses sätestatud kuni 65-aastane säilitustähtaeg enam piisav ja ABIS-e arhiivandmete säilitamist on vaja pikendada 50 aastalt 60-le, s.o dokumendimenetlusega seotud ja ABIS-esse kantud andmete säilitamise kogutähtaeg on 75 aastat. ABIS-e põhimäärust on kavas pärast eelnõu jõustumist muuta.
- 2) **KodS-i § 2⁴ lõikes 7¹** sätestatakse, et **KodS-i** alusel ABIS-esse kantud andmeid säilitatakse **tähtajatult** (eelnõu § 2 p 9). 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 tähtajatult. KodS-i alusel ABIS-esse kantud andmeid peab säilitama tähtajatult, 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 PS-i §-s 8 on sätestatud kodakondsuse alusena põhimõtte, 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 tähtajatult. Lisaks on Rahvusarhiiv kuulutanud Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu toimikud arhiiviväärtuslikuks ning neid säilitatakse riigiarhiivis.

- 3) **KonS-i § 12¹ lõikes 7¹** sätestatakse, et **KonS-i** alusel ABIS-esse kantud andmeid säilitatakse **neli kuud** pärast dokumendi taotluse edastamist PPA-le (eelnoü § 3 p 4). 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 § 109² lõikes 5¹, VangS-i § 5⁵ lõikes 5¹ ja VTMS-i § 31⁶ lõikes 5¹** sätestatakse, et **KrMS-i, VangS-i ja VTMS-i** alusel ABIS-esse kantud andmeid säilitatakse **kuni 75 aastat** ABIS-esse kandmisest arvates (eelnoü § 4 p 3, § 7 p 3 ja § 10 p 3). Lühema säilitustähtaja võib kehtestada ABIS-e põhimääruses. Kõnealuseid andmeid töödeldi varem riiklikus sõrmejälgede registris. Riiklik sõrmejälgede register ja riiklik DNA-register ühendati riiklikuks süüteomenetluse biomeetriaregistris (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 põhimääruse⁶⁰ §-s 16 sätestatud andmete säilitamise regulatsiooniga.
- 5) **VSS-i § 33 lõigetes 8¹ ja 8² ning § 33¹⁵ lõigetes 7¹ ja 7²** sätestatakse, et **VSS-i** alusel alalise sissesõidukeelu kohaldamise menetluses **sissesõidukeeldude riikliku registri** kaudu ABIS-esse kantud andmeid säilitatakse järgmiselt (eelnoü § 9 p-d 16, 25 ja 26):
 - alalise sissesõidukeelu andmed – **75 aastat** välismaalase sünnist arvates;
 - tähtjalise sissesõidukeelu andmed – aktiivselt **kümme aastat** tähtjalise sissesõidukeelu tähtaja lõppemisest arvates ja arhiveerituna **40 aastat**, kui registri põhimääruses ei ole nähtud ette lühemat tähtaega.Alalise sissesõidukeelu andmete säilitamise tähtaega lühendatakse tähtajatust 75 aastani, sest sissesõidukeeld kehtestatakse välismaalasele ja üle 75 aasta ei ole vaja selle andmeid säilitada, arvestades, et välismaalasele kehtestatud sissesõidukeeld ei mõjuta tema järeltulija võimalusi Eestisse saabuda. Võttes arvesse inimese keskmist eluiga ja asjaolu, et VSS-i § 30 punkti 1 kohaselt ei saa kohaldada sissesõidukeeldu alla 13-aastasele, oleks alalise sissesõidukeelu andmete tähtajatu säilitamine põhjendamatu ja koormaks digivõrku.

VSS-i alusel **Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu** kaudu ABIS-esse kantud Eestis viibimise ja Eestist lahkumise kohustuse täitmisega seotud andmeid säilitatakse aktiivselt **kümme aastat** välismaalase lahkumiskohustuse täitmisest

⁶⁰ Vabariigi Valitsuse 28. septembri 2023. aasta määrus nr 87 „[Riikliku süüteomenetluse biomeetriaregistri põhimäärus](#)“.

arvates, pärast mida need arhiveeritakse. Arhiveeritud andmeid säilitatakse **40 aastat**. Andmetele võib näha ette lühema säilitustähtaja ABIS-e põhimääruses (eelnõu § 9 p 26).

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

Praegu on Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu täpset andmekoosseisu ja andmete säilitamist reguleeritud andmekogu põhimääruses⁶¹. Isikuandmete säilitamist käsitatakse eraelu puutumatusena. Konkreetse säilitustähtaja sätestamine seaduse tasandil aitab kaasa läbipaistvale andmetöötlemisele. 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.

Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu esialgne andmekoosseis oli kehtestatud siseministri 3. juuli 2009. aasta määrusega nr 23 „Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu pidamise põhimäärus“, mille eelnõu seletuskirjas on põhjendatud ka andmete töötlemise vajalikkust⁶². 2015. aastal kehtestati uus terviktekst, sealhulgas muudeti mõnevõrra andmekogu andmekoosseisu, mida on põhjendatud selle eelnõu seletuskirjas⁶³.

3.4.4. Sissesõidukeeldude riikliku registri ning Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu andmekoosseis ja andmete säilitamise tähtajad (§ 9 p-d 13, 15, 19, 21 ja 22)

Eelnõu § 9 punktidega 13 ja 15 muudetakse **VSS-i § 33 lõikeid 3 ja 8**. Punktidega 19, 21 ja 22 muudetakse **VSS-i § 33¹⁴ lõikeid 3, 6 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).

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.
- 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.

⁶¹ Siseministri 18. detsembri 2015. aasta määrus nr 75 „[Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu põhimäärus](#)“.

⁶² Eelnõude infosüsteemi toimiku nr [2-1-2/4399](#).

⁶³ Eelnõude infosüsteemi toimiku nr [15-1540/01](#).

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 piirieskirjades⁶⁴ 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 andmeid, mis on vajalikud, et luua määruse (EL) 2018/1861 alusel sissesõidukeeldu käsitlev hoiatusteade ja seda ajakohastada. Sissesõidukeeldude riikliku registri andmekoosseis viiakse eelnõuga registri põhimäärusest⁶⁵ VSS-i. Andmekoosseisu ja andmete töötlemist on põhjendatud põhimääruse eelnõu seletuskirjas⁶⁶.

VSS-i § 27¹ lõike 1 kohaselt võib sissesõidukeeld olla alaline või tähtajaline. Andmeid, mis kantakse sissesõidukeeldude riiklikusse registrisse alalise sissesõidukeelu kohaldamise menetluses, säilitatakse 75 aastat välismaalase sünnist arvates. Tähtajalise sissesõidukeelu andmeid säilitatakse aktiivselt kümme aastat tähtajalise sissesõidukeelu tähtaja lõppemisest arvates, pärast mida need arhiveeritakse. Arhiveeritud andmeid säilitatakse 40 aastat. Andmete säilitamise tähtaegade täpsem selgitus on seletuskirja punkti 3.4.2 alapunktis 5.

Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu

Andmed, mida töödeldakse Eestis seadusliku aluseta viibiva ja viibinud välismaalase Eestis viibimise ja Eestist lahkumise kohustuse täitmisega 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 lahkumisettekirjutus, millega kohustatakse teda Euroopa Liidust lahkuma. Määruse (EL) 2018/1860 artiklis 4 on sätestatud, mis andmete põhjal tagasisaatmist käsitlev hoiatusteade luuakse. Kuigi tagasisaatmist käsitleva hoiatusteate 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 täitmisega seotud menetluses.

Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu andmeid säilitatakse aktiivselt kümme aastat välismaalase lahkumiskohustuse täitmisest arvates, pärast mida need arhiveeritakse. Arhiveeritud andmeid säilitatakse 40 aastat. Andmete säilitamise tähtaja täpsem selgitus on seletuskirja punkti 3.4.2 alapunktis 5.

⁶⁴ 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](#).

⁶⁵ Siseministri 7. detsembri 2022. aasta määrus nr 40 „[Schengeni riikliku registri põhimäärus](#)“.

⁶⁶ Eelnõude infosüsteemi toimiku nr [22-0871/01](#).

Eelnõuga viiakse Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu andmekoosseis ja andmete säilitamise tähtaeg andmekogu põhimäärusest⁶⁷ VSS-i. Andmekoosseisu ja andmete töötlemist on põhjendatud põhimääruse eelnõu seletuskirjas⁶⁸.

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 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 asjaomasesse 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 õiguselguseks reguleerida biomeetrilist võrdlusuuringut selliste Euroopa Liidu andmekogudega, millesse tehtud päringu tulemus ei ole lõplik, vaid võimalik tabamus.

⁶⁷ Siseministri 1. juuli 2020. aasta määrus nr 25 „[Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu põhimäärus](#)“.

⁶⁸ Eelnõude infosüsteemi toimiku nr [18-0498](#).

Schengeni infosüsteemi kasutamist piirikontrolli valdkonnas on reguleeritud määruses (EL) 2018/1861. Selle artikli 33 lõike 2 kohaselt tuleb teha isiku tuvastamiseks daktüloskoopiliste andmete ehk sõrmejälgede 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 välismaalaselt 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 õigusselguseks. 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-t, 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 õigusselguse huvides sätestada, et piiriületusel võetud biomeetrilisi andmeid võrreldakse ABIS-e võrdlusmootorit kasutades. Seega **ei ole muudatusel olulist mõju**, kuna PPA peab rakendama Schengeni piiri-eeskirju ja kontrollib ka praegu välispiiri ületajaid. Samuti võib piirikontrollis võetud sõrme-

jälgi 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 kontrolli⁶⁹ 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 põhimääruste volitusnormide täpsustamine (§ 1 p-d 34, 36 ja 37, § 2 p-d 4, 5, 7 ja 8, § 3 p-d 2 ja 3, § 4 p-d 1 ja 2, § 5 p 5, § 7 p-d 1 ja 2, § 8, § 9 p-d 14, 15, 20, 21, 23 ja 24 ning § 10 p-d 1 ja 2)

Eelnõu § 1 punktides 34 ja 37, § 2 punktides 5 ja 8, § 3 punktis 3, § 4 punktis 2, § 5 punktis 5, § 7 punktis 2, § 8 punktis 2, § 9 punktides 15, 21 ja 24 ning § 10 punktis 2 täpsustatakse järgmiste andmekogude põhimääruste volitusnorme:

- ITDAK (**ITDS-i § 15² lg 5**);
- Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu (**KodS-i § 2¹ lg 5**);
- sissesõidukeeldude riiklik register (**VSS-i § 33 lg 8**);
- Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu (**VSS-i § 33¹⁴ lg 7**);
- ABIS (**KodS-i § 2⁴ lg 7, KonS-i § 12¹ lg 7, KrMS-i § 109² lg 5, PPVS-i § 25⁷ lg 3¹, VangS-i § 5⁵ lg 5, VRKS-i § 13⁷ lg 7, VSS-i § 33¹⁵ lg 7 ja VTMS-i § 31⁶ lg 5**).

Andmekogu põhimääruses võib muu hulgas kehtestada:

- andmeandjad ja nendelt saadavad andmed;
- täpsema andmekoosseisu;
- andmekogudevahelise andmevahetuse;
- vastutava töötleja ülesanded;
- volitatud töötleja ja tema ülesanded;
- andmetele juurdepääsu ja andmete väljastamise korra ning
- muud korralduslikud küsimused.

Täpsustus on vajalik, et oleks seaduse tasandil selge, mida võib andmekogu põhimääruses sätestada.

Kuna kohustus määrata andmekogu volitatud töötleja põhimääruses on edaspidi volitusnormis, jäetakse **eelnõu § 1 punktiga 36, § 2 punktidega 4 ja 7, § 3 punktiga 2, § 4 punktiga 1, § 7 punktiga 1, § 8 punktiga 1, § 9 punktidega 14, 20 ja 23 ning § 10 punktiga 1** välja samasuline regulatsioon teistes sätetes.

3.4.7. Andmekogude regulatsiooni tehnilised muudatused (§ 1 p 32, § 2 p-d 1 ja 2, § 3 p 1, § 5 p-d 2–4 ning § 9 p-d 11, 12, 17 ja 18)

Eelnõu § 1 punktiga 32 täpsustatakse **ITDS-i § 15² lõikes 1**, et lühendit „andmekogu“ kasutatakse ITDAK-i tähenduses vaid selles paragrahvis.

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

- 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.

⁶⁹ Schengeni piirieskirjade artikli 2 punkti 13 kohaselt on see lisakontroll, mida võib teha spetsiaalselt selleks ettenähtud kohas eemal kohast, kus kontrollitakse kõiki isikuid.

Eelnõu § 3 punktiga 1 muudetakse **KoS-i § 12 lõigetes 1, 3¹, 4 ja 5 ning §-s 75¹** konsulaar-ametniku ametitoimingute andmekogu nimetus „konsulaarametniku ametitoimingute ja diplomaatiliste passide andmekoguks“, sest andmekogusse on lisandunud diplomaatiliste passide menetlemise moodul. Sama muudatus⁷⁰ tehti 2019. aastal ka välisministri 7. augusti 2017. aasta määruses nr 6 „Konsulaarametniku ametitoimingute ja diplomaatiliste passide andmekogu pidamise kord“.

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 § 5 punktiga 1 võetakse ABIS-e lühend kasutusele PPVS-i § 19² lõikes 2.

Eelnõu § 9 punktidega 11, 12 ja 18 ühtlustatakse lühendikasutust.

- 1) **Punktiga 11** muudetakse **VSS-i § 33 lõiget 1** ja antakse sissesõidukeeldude riikliku registri lühend, mida edaspidi paragrahvis kasutatakse.
- 2) **Punktiga 12** muudetakse **VSS-i § 33 lõiget 2** ja kasutatakse selles sissesõidukeeldude riikliku registri täisnimetuse asemel lühendit.
- 3) **Punktiga 18** 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 17 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. KoS-i tehnilised muudatused (§ 3 p-d 5–7 ja 11)

Eelnõu § 3 punktidega 5–7 ja 11 muudetakse **KoS-i § 32 lõiget 1, § 37 lõiget 1, §-e 46 ja 70** ning tunnistatakse kehtetuks **§ 32 lõige 2**. Muudatused on tehnilised.

- 1) **KoS-i § 32 lõike 1 ja § 37 lõike 1** muutmise ning **§ 32 lõike 2** kehtetuks tunnistamisega vabastatakse aukonsul tõlketeenuse osutamise ja elu- või viibimiskohta registreerimise ülesandest. Aukonsul ei ole konsulaarametnik. Seetõttu tuleks aukonsulile anda seadusega konsulaarülesandeid võimalikult vähe, suunates inimesi kasutama teisi võimalusi. Eesti asutuste väljaantud dokumendid, mida kasutatakse välisriigis, väljastatakse valdavalt asukohariigi või inglise keeles, millest saab enamikus riikides teha vajadusel tõlke asukohariigi keelde. Samuti puudub võimalus kontrollida aukonsuli tõlketeenuse osutamise pädevust. Praktikast ei ole aukonsulid tõlketeenust ka pikema aja jooksul osutanud. Samuti ei registreeri aukonsulid elu- või viibimiskohta. Vajadusel võivad aukonsulid võtta vastu välisriigis püsiva elukoha registreerimise taotlusi, kuid sel juhul edastavad nad selle elukoha registreerimiseks konsulaarametnikule.
- 2) **KoS-i § 46** sõnastus viiakse vastavusse viisaeeskirjaga⁷¹, mida on muudetud 1. veebruaril 2020 jõustunud Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/1155⁷². Muudetud artikli 8 kohaselt vastutab esindav Euroopa Liidu liikmesriik viisamenetluse eest algusest lõpuni, ilma et esindatav liikmesriik oleks kaasatud. Kahepoolseid viisaküsimustes vastastikuse esindamise kokkuleppeid on VÄM vajaduse järgi juba muutnud.

⁷⁰ [RT I, 18.06.2019, 5](#).

⁷¹ Euroopa Parlamendi ja nõukogu 13. juuli 2009. aasta määrus (EÜ) nr 810/2009, millega kehtestatakse ühenduse viisaeeskiri (viisaeeskiri). – [ELT L 243, 15.9.2009, lk 1–58](#).

⁷² Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta määrus (EL) 2019/1155, millega muudeti määrust (EÜ) nr 810/2009, millega kehtestatakse ühenduse viisaeeskiri (viisaeeskiri). – [ELT L 188, 12.7.2019, lk 25–54](#).

- 3) KonS-i § 70 täiendatakse sõnadega „põhjustatud vajadus“. Kehtiva paragrahvi kohaselt edastab konsulaarametnik isiku või ametiasutuse kirjalikul taotlusel ametliku dokumendi, näiteks sünnitunnistuse, Eesti või välisriigi ametiasutusele, kui välislepinguga või seaduse alusel ei ole ette nähtud teistsugust korda. Põhjustatud vajaduse tingimus on oluline, et vältida diplomaatilise posti tasuta kasutamist juhul, kui on ka muid turvalisi postiteenuseid. Põhjustatud vajaduseks saab lugeda olukorda, kus isikul või ametiasutusel on vältimatu vajadus esitada selliseid dokumente teisele riigile, kuid puudub näiteks turvalise postiteenuse võimalus. Vajaduse põhjustatuse üle otsustab VÄM kui teenuseosutaja.

3.6. 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 hindamistel juhtinud Euroopa Liidu liikmesriikide tähelepanu sellele, et tagasisaatmisdirektiivi reguleerimisalas 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.

3.7. Välismaalase kinnipidamine (§ 9 p-d 3–10)

Eelnõu § 9 punktidega 3–10 muudetakse **VSS-i § 15 pealkirja, lõikeid 1, 3 ja 4 ning § 15⁴ lõiget 3**, täiendatakse **VSS-i § 15 lõigetega 4¹ ja 4²** ja **§ 15⁴ lõikega 4¹** ning tunnistatakse kehtetuks **VSS-i § 15⁴ lõige 5**.

Muudatused on ajendatud Riigikohtu halduskolleegiumi 12. aprilli 2024. aasta otsustest nr 3-23-2232 ja 3-23-2204⁷³, milles on kohus leidnud, et välismaalase kinnipidamine peab hetkest, kui asutus on enda hinnangul teinud kindlaks välismaalase ebaseadusliku Eestis viibimise, vastama tagasisaatmisdirektiivi artikli 15 nõuetele. Artikli lõike 1 kohaselt võib ebaseaduslikult riigis viibivat välismaalast pidada tagasisaatmise ettevalmistamiseks ja/või väljasaatmise täideviimiseks kinni juhul, kui esineb tema põgenemise oht või ta ei tee koostööd, sealhulgas takistab oma tagasisaatmist või tema reisidokumendi hankimine kolmandast riigist viibib. Ebaseaduslikult riigis viibiva välismaalase põgenemise oht esineb, kui on täidetud vähemalt üks VSS-i §-s 6⁸ sätestatud tingimus:

- 1) välismaalane ei ole Eestist või teisest Schengeni konventsiooni või Euroopa Liidu liikmesriigist lahkunud pärast lahkumisettekirjutusega määratud lahkumiskohustuse vabatahtliku täitmise tähtaega;
- 2) välismaalane on esitanud valeandmeid või võltsitud dokumendi Eestis viibimise seadusliku aluse või selle pikendamise, Eesti kodakondsuse, rahvusvahelise kaitse või dokumendi taotlemisel;
- 3) on põhjustatud kahtlus välismaalase isikusamasuses või tema kodakondsuses;
- 4) välismaalane on korduvalt toime pannud tahtlikke kuritegusid või toime pannud kuriteo, mille eest on talle mõistetud vangistus;
- 5) välismaalane ei ole järginud tema suhtes lahkumisettekirjutuse täitmise tagamiseks kohaldatud järelevalvemeetmeid;
- 6) välismaalane on PPA-le või KAPO-le teada andnud või haldusorgan järeldab tema hoiakutest ja käitumisest, et ta ei soovi lahkumiskohustust täita;
- 7) välismaalane on sisenenud Eestisse tema suhtes kohaldatud sissesõidukeelu kehtivusaja jooksul;

⁷³ RKHKo, 12.04.2024, 3-23-2232, p 22; RKHKo, 12.04.2024, 3-23-2204, p 21.

- 8) välismaalane on kinni peetud Eesti välispiiri ebaseadusliku ületamise tõttu ja ta ei ole saanud luba või õigust Eestis viibida;
- 9) välismaalane on loata lahkunud määratud elukohast või teisest Schengeni konventsiooni või Euroopa Liidu liikmesriigist;
- 10) välismaalase lahkumiskohustus on kohtulahendiga pööratud sundtäitmisele.

Euroopa Kohus on selgitanud, et tagasisaatmisdirektiivis on käsitletud üksnes ebaseaduslikult riigis viibiva välismaalase tagasisaatmist. Selle eesmärk ei ole ühtlustada kogu välismaalase viibimise riigisisest õigust. Euroopa Liidu liikmesriikidel on jätkuvalt võimalik riigisiseses õiguses reguleerida kolmanda riigi kodaniku kinnipidamist selleks, et teha kindlaks, kas ta viibib riigis seaduslikult või mitte. Kui selline kinnipidamise võimalus riigisiseses õiguses puuduks, võiks ebaseaduslikult riigis viibimises kahtlustatav välismaalane põgeneda enne, kui tema õiguslik seisund on kindlaks tehtud.⁷⁴

Sellest lähtudes muudetakse VSS-i §-des 15 ja 15⁴ välismaalase kinnipidamise alused õigus-selgemaks. Kehtiv VSS-i § 15 lõige 1 lubab PPA-l või KAPO-l pidada välismaalast kuni 48 tundi kinni, et kontrollida tema Eestisse saabumise ja Eestis viibimise asjaolusid ning selgitada välja tema kinnipidamise vajalikkus tagasisaatmisdirektiivi alusel. Kuivõrd Riigi-kohtu hinnangul tuleb tagasisaatmisdirektiivi nõudeid järgida hetkest, kui välismaalase riigis viibimise ebaseaduslikkus on kindlaks tehtud, sätestatakse välismaalase kinnipidamise alused välismaalase õigusliku seisundi järgi edaspidi eri sätetes.

VSS-i § 15 lõikest 1 jäetakse välja kinnipidamise vajalikkuse väljaselgitamise osa. Ka edaspidi võib PPA või KAPO pidada ebaseaduslikus viibimises kahtlustatavat välismaalast kuni 48 tundi kinni, et kontrollida tema Eestisse saabumise ja Eestis viibimise seaduslikke aluseid, kuid kinnipidamise vajalikkust reguleeritakse eraldi. Kui kontrollist selgub, et välismaalase suhtes tuleb läbi viia muu menetlus, näiteks ta on tagaotsitav või ta on teises Euroopa Liidu liikmesriigis taotlenud rahvusvahelist kaitset, algatatakse menetlustoimingud ja välismaalane peetakse vajadusel kinni näiteks KrMS-i või VRKS-i alusel. Seetõttu täiendatakse **VSS-i § 15 lõiget 3** ning nähakse PPA-le ja KAPO-le ette kohustus vabastada välismaalane kinnipidamisaluse äralangemise korral vaid juhul, kui ei esine muud seadusjärgset alust tema kinnipidamiseks.

Eelnõukohase **VSS-i § 15 lõike 4** kohaselt võib PPA või KAPO taotleda halduskohtult luba pidada ebaseaduslikult riigis viibimises kahtlustatavat välismaalast kinni kauem kuni kolm päeva, kui vajalikud menetlustoimingud nõuavad rohkem aega. See võib osutada vajalikuks eeskätt olukordades, kus välismaalasel puudub tagasipöördumiseks vajalik dokument, kuid ta väidab, et teine Euroopa Liidu liikmesriik on talle väljastanud kehtiva elamisloa, või menetlus-toiminguks tuleb kaasata tõlk.

Välismaalase suhtes, kelle riigis viibimise ebaseaduslikkus on juba kindlaks tehtud, tuleb kohaldada tagasisaatmisdirektiivi kinnipidamisaluseid ja -põhimõtteid. Seetõttu täiendatakse **VSS-i § 15 lõikega 4¹**, mis võimaldab PPA-l või KAPO-l pidada ebaseaduslikult riigis viibivat välismaalast kuni 48 tundi kinni, et viia läbi Eestist lahkuma kohustamise menetlus või pöörata tagasisaatmine sunniviisiliselt täitmisele, kui:

- esineb välismaalase põgenemise oht;
- välismaalane ei täida kaasaaitamiskohustust või
- välismaalasel puuduvad tagasipöördumiseks vajalikud dokumendid või nende hankimine vastuvõtvast või transiidiriigist viibib.

⁷⁴ Vt täpsemalt Euroopa Kohtu 6. detsembri 2011. aasta otsus kohtuasjas C-329/11, Alexandre Achughbabian vs. Préfet du Val-de-Marne, [ECLI:EU:C:2011:807](https://eur-lex.europa.eu/eli/cejoc/2011/807), p-d 29 ja 30.

Selline kinnipidamine peab olema vajalik ja proportsionaalne ning arvestama välismaalasega seotud olulisi asjaolusid, nagu tervise seisund ja haavatavus. Kui ebaseaduslikult riigis viibiva välismaalase tagasisaatmine ei ole 48 tunni jooksul võimalik, tuleb PPA-l või KAPO-l **VSS-i § 15 lõike 4²** kohaselt taotleda halduskohtult luba pidada välismaalast kinni kuni kaks kuud.

Samasisulised muudatused tehakse **VSS-i § 15 pealkirjas** ja **§-s 15⁴**, milles on reguleeritud välismaalase kinnipidamist massilisest sisserändest põhjustatud hädaolukorras.

3.8. Seaduse jõustumine (§ 11)

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

- Eelnõu **§ 1 punktid 14 ja 43, § 3 punktid 8–10 ning § 6** on seotud riigilõivuseaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduses⁷⁵ sätestatud uue riigilõivumääraga ning jõustuvad selle seadusega samal ajal: 2025. aasta 1. jaanuaril.
- Muudatused, mille rakendamiseks on vaja teha infotehnoloogilisi arendustöid, jõustuvad pärast nende valmimist.
 - Eelnõu **§ 1 punktid 2–4, 9, 12, 13, 25, 46 ja 50**, millega lõpetatakse sertifikaatide kehtivuse peatamine ja taastamine ning suurendatakse perekonnanime tähemärkide arvu dokumendil, jõustuvad 2025. aasta 15. novembril.
 - Eelnõu **§ 1 punkt 23**, millega võimaldatakse dokumendi taotlejal aktiveerida ID-1 formaadis dokument ja sertifikaadid elektrooniliselt, jõustub 2026. aasta 1. juunil.

4. Eelnõu terminoloogia

- 1) 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.
- 2) Lisaks asendatakse ITDS-is termin „vanglatöötaja“ JUM-i ettepanekul terminiga „**kinnipidamisasutuse volitatud ametnik või töötaja**“ ja ühtlustatakse lühendikasutust.
- 3) Andmekogude andmekoosseisu sätetes kasutatakse terminit „**isiku üldandmed**“. Isiku üldandmed on nimi, isikukood või selle puudumise korral sünniaeg, sugu, kodakondsus, kontaktandmed, sealhulgas aadress, ja emakeel.
- 4) KonS-is nimetatakse konsulaarametniku ametitoimingute andmekogu ümber **konsulaarametniku ametitoimingute ja diplomaatiliste passide andmekoguks**, sest andmekogusse on lisandunud diplomaatiliste passide menetlemise moodul.

5. Eelnõu vastavus Euroopa Liidu õigusele

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

Eelnõu § 3 punktiga 7 viiakse KonS vastavusse viisaeeskirjaga, mille muudetud artikli 8 kohaselt vastutab esindav Euroopa Liidu liikmesriik viisamenetluse eest algusest lõpuni, ilma

⁷⁵ [RT I, 29.06.2024, 3.](#)

et esindatav liikmesriik oleks kaasatud. Kahepoolseid viisaküsimustes vastastikuse esindamise kokkuleppeid on VÄM vajaduse järgi juba muutnud.

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 lahkumisetekirjutus 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 personaalseid 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. 1. jaanuari 2024. aasta seisuga on kehtiv e-residendi digi-ID 60 629 inimesel.

Tabel 3. E-residendi digi-ID taotlejate prognoositud arv aastatel 2024–2028

	2024	2025	2026	2027	2028
E-residendi digi-ID taotlejate prognoositud arv	16 600	15 200	16 300	17 000	18 700

Allikas: PPA

Võrreldes teiste PPA väljaantavate dokumentide⁷⁶ taotlejatega, st Eesti elanikega, keda on 2023. aasta seisuga 1 365 884⁷⁷, on sihtrühm **väike**.

Mõju ulatus ja esinemise sagedus on **väikesed**, kuna muudatustega ei kaasne e-residendile lisategevusi ega kohanemiskulusi. 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 üle⁷⁸. 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. E-residentsuse riskiriigi kodaniku e-residendi digi-ID taotluse tagastamine läbi vaatamata

Eelnõuga luuakse õiguslik alus **tagastada** seletuskirja tabelis 1 nimetatud **e-residentsuse 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 e-residentsuse riskiriigi kodanik võimaluse kasutada Eesti 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

⁷⁶ Ajutine reisidokument, digitaalne isikutunnistus, Eesti kodaniku pass, elamisloakaart, isikutunnistus, meremehe teenistusraamat, meresõidutunnistus, pagulase reisidokument ja välismaalase pass.

⁷⁷ Statistikaamet 2024. [Rahvaarv](#).

⁷⁸ RahaPTS-i § 53 lõike 4 kohaselt on RAB-i teenistus- ja töökohtade koosseis ning isikkoosseis asutusesiseseks kasutamiseks mõeldud teave AvTS-i tähenduses.

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: e-residentsuse riskiriigi kodanikud, kes soovivad taotleda e-residendi digi-ID-d. 1. jaanuari 2024. aasta seisuga on e-residentsuse riskiriigi kodanikest e-residente 6886. Arvestades kavandatavaid erisusi, puudutab muudatus 28 e-residentsuse riskiriigi kodanikke. 1. jaanuari 2024. aasta seisuga oli kehtiv e-residendi digi-ID 60 629 inimesel. Kuna enamikul e-residentsuse riskiriigi kodanikel ei ole huvi Eestis ettevõtlusega tegeleda ega Eesti e-teenuseid kasutada, ei ole neil ka huvi e-residendi digi-ID-d taotleda. Seega on sihtrühm võrreldes e-residentide koguarvuga **väike**.

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 kohanemiskursi ei teki.

Mõju esinemise sagedus on **väike**, sest sihtrühma kokkupuude muudatusega on ebaregulaarne ja juhuslik. E-residentsuse 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 e-residentsuse riskiriigi kodanikul edaspidi võimalik saada 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 e-residentsuse riskiriigi kodanikule võimalus taotleda e-residendi digi-ID-d, kui tal on Eestis tõestatav majandustegevus. Lisaks saab praegu e-residentsuse 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 muutu. Kuigi PPA töömaht võib väheneda nende e-residendi digi-ID taotlejate võrra, kes on e-residentsuse riskiriigi kodanikud ja kellele ei kohaldu kavandatavad erisused, tuleb erisuste väljaselgitamiseks PPA ametnikel teha varasemaga võrreldes lisatööd.

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.⁷⁹ 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. E-residentsuse riskiriigi kodanikele e-residentsuse võimaldamine on vastuolus e-residentsuse eesmärgiga ning kahjustab Eesti julgeolekut ja mainet, sealhulgas välissuhteid.

E-residentsuse 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 põhjal⁸⁰ annab Eesti e-residentsus võimaluse siseneda Euroopa Liitu ja teha rahvusvahelist äri, kuna lihtsustab viibimiseluse saamist Eestis ja Euroopa Liidus. PPA statistika kohaselt oli 9,3%-l Iraani kodanikest e-residentidel elamisloa.

Tabel 4. Iraani kodanike e-residendi digi-ID taotluste arv aastatel 2014–2023

2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Kokku
1	24	59	82	213	189	129	161	130	170	1158

Allikas: PPA

Muudatus aitab maandada ja ennetada riigi julgeolekut ja siseturvalisust ohustavaid riske ning nendega kaasnevaid ühiskondlikke tagajärgi, mis tulenevad e-residentsuse riskiriigi kodanike kogukondade suurenemisest. Need riskid on vaenulik mõjutustegevus, terrorism, radikaliseerumine, raske ja organiseeritud kuritegevus, eriti majanduskuritegevus, korrupsioon, 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 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.

⁷⁹ Statistikaamet 2024. [Rahvaarv](#).

⁸⁰ [Iraani avalikud allikad Eesti e-residentsuse kohta](#).

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

6.1.2.4. Mõju majandusele

Sihtrühm: Eesti elanikud. 2024. aasta alguse seisuga elas Eestis 1 366 491 inimest.⁸¹ Sihtrühm on seega **suur**.

E-residentsuse riskiriigi kodanikest e-residentide ettevõtted ning nende käive ja töötajumaksud

01.01.2024 oli kehtiva e-residenti digi-ID-ga e-residentsuse riskiriigi kodanikel seos 2869 ettevõttega. See on 12,8% kõikidest e-residenti ettevõtetest, millest omakorda oli maksumaksjaid umbes 27%.

Tabel 5. E-residentsuse riskiriigi kodanike ettevõtete arv

	Riik	Ettevõtete arv
1	Afganistani Islamivabariik	10
2	Alžeeria Demokraatlik Rahvavabariik	54
3	Burkina Faso	3
4	Egiptuse Araabia Vabariik	154
5	Iraagi Vabariik	6
6	Iraani Islamivabariik	166
7	Jeemeni Vabariik	12
8	Jordaania Hašimiidi Kuningriik	27
9	Kongo Demokraatlik Vabariik	7
10	Liibanoni Vabariik	62
11	Liibüa Riik	15
12	Lõuna-Sudaani Vabariik	0
13	Mali Vabariik	3
14	Maroko Kuningriik	92
15	Mosambiigi Vabariik	1
16	Nigeeria Liitvabariik	71
17	Nigeri Vabariik	0
18	Pakistani Islamivabariik	134
19	Palestiina Omavalitsus	11
20	Korea Rahvademokraatlik Vabariik	0
21	Saudi Araabia Kuningriik	3
22	Somaalia Liitvabariik	0
23	Sudaan	11
24	Süüria Araabia Vabariik	32
25	Tuneesia Vabariik	120
26	Usbekistan	46
27	Valgene Vabariik	350
28	Venemaa Föderatsioon	1479
	KOKKU	2869

Allikas: PPA

⁸¹ Statistikaamet 2024. [Rahvaarv](#).

2022. aasta III kvartalist kuni 2023. aasta I kvartalini deklareeris käivet või maksis tööjõumakse 870 e-residentsuse riskiriigi kodaniku ettevõtet. Neist 781 tasus riiklikke makse ja 463 maksis tööjõumakse.

Mõju kirjeldus ja järelendus mõju olulisuse kohta

Muudatuse tulemusena võib väheneda e-residentsuse programmi võimalik tulu riigile, kuid arvestades, et e-residentsuse riskiriigi kodanikke on vähe, on võimalik saamata jääv tulu marginaalne ega kaalu üles muudatuse rakendamata jätmise võimalikku kahju Eesti julgeolekule. E-residentsuse programmi otsene majanduslik kogumõju Eestile tööjõu- ja dividendimaksudes ning riigilõivudes on 1. jaanuari 2024. aasta seisuga 213 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 e-residentsuse riskiriikide kodanike puhul. Moneyvali hindamise tulemusena võib hinnatav riik sattuda riskiriikide halli või musta nimekirja⁸². 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 e-residentsuse 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 e-residentsuse riskiriigi kodanike ettevõtetest Eestile laekuv tulu. Kui e-residentsuse 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. Isikusamasuse kontrollimine Eesti teabevärava mobiilirakenduse vahendusel

Eelnõuga luuakse võimalus kontrollida füüsilises keskkonnas isikusamasust Eesti teabevärava mobiilirakenduse vahendusel.

⁸² Mustas nimekirjas on kõrge riskiga riigid, kus on tõsiseid strateegilisi puudujääke võitluses rahapesu, terrorismi rahastamise ja massihävitusrelvade 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 töökonna tugevdatud järelevalve all. Rahapesuvastane töökond (FATF) töötab välja rahapesu ja terrorismi rahastamise vastase võitluse standardeid ning meetodeid ja edendab sellealast poliitikat.

6.2.1. Sotsiaalne, sealhulgas demograafiline mõju

Sihtrühm: Eesti elanikud. Eestis elab 2024. aasta alguse seisuga 1 366 491 inimest.⁸³ Kuna muudatus võib mõjutada kõiki Eesti elanikke, on sihtrühm **suur**.

Mõju ulatus ja esinemise sagedus on **väikesed**. Inimesed on harjunud igapäevaelus kasutama erinevaid mobiilirakendusi ja seega ei valmista oma isikusamasuse tõendamine Eesti teabevärava mobiilirakenduse vahendusel neile raskusi. Rakenduse saab alla laadida Google Play poest või App Store'ist ning esimesel kasutuskorral kuvatakse inimesele põhjalik selgitus selle aktiveerimiseks ja seadistamiseks. Sisselogimine on sarnane juba praegu laialdaselt kasutusel olevate mobiilirakenduste ja e-teenustega ning seda saab teha Smart-ID, mobiil-ID või kasutaja seadistatud turvakoodi või biomeetriliste andmetega.

Muudatusega ei kehtestata kohustust: Eesti teabevärava mobiilirakenduse kasutamine on inimese vaba valik. Endiselt jääb alles võimalus esitada oma isikusamasuse tõendamiseks isikutunnistus või muu dokument. Seeläbi ei too muudatus sihtrühmale kaasa uusi kohustusi ega kohanemiskulusi. Lisaks, kuna praegu ei ole võimalik kirjeldada konkreetset kasutust ja ei ole teada, kes teenuseosutajatest võtavad Eesti teabevärava mobiilirakenduse kasutusele, on väga keeruline hinnata, kui palju hakkavad inimesed rakenduse isikusamasuse tõendamise funktsiooni kasutama.

Ebasoovitava mõju kaasnemise risk on **väike**. Muudatus on positiivne, luues alternatiivse ja mugava isikusamasuse tõendamise võimaluse. Selle kasutusele võtmisega kaasnevad võimalikud riskid ja turvalisusküsimused on maandatud kaasaegsete infotehnoloogiliste lahendustega. Andmekaitseriske on koostöös Andmekaitse Inspeksiooniga hinnatud⁸⁴ ning PPA ja RIA andmevahetuslepinguga sätestatakse konkreetset andmetöötlustingimused. Lisaks on RIA koostöös MKM-iga hinnanud tehnoloogilisi riske, mille kohta valmib 2024. aasta sügisel riskihinnang, mis avalikustatakse RIA kodulehel.

Seega on muudatusel sihtrühmale **väheoluline mõju**.

6.2.2. Mõju majandusele

Sihtrühm: ettevõtjad, kes kasutavad võimalust kontrollida isikusamasust Eesti teabevärava mobiilirakenduse vahendusel. Majanduslikult aktiivseid ettevõtteid on 2023. aasta seisuga 153 883.⁸⁵ Ilmselt ei osuta kõik majanduslikult aktiivsed ettevõtted teenuseid ja muudatus ei puuduta kogu Eesti ettevõtluskeskkonda. Lisaks on Eesti teabevärava mobiilirakenduse vahendusel isikusamasuse kontrollimine ettevõtjale vabatahtlik ja ilmselt kõik ettevõtjad seda võimalust ei kasuta. Seetõttu võib pidada sihtrühma **keskmiseks**.

Mõju ulatus ja esinemise sagedus võivad olla suured. Ettevõtjad, kes võtavad Eesti teabevärava mobiilirakenduse kasutusele, kasutavad seda ilmselt aktiivselt. Olulisi kohanemiskulusi ei teki, sest Eestis on harjutud erinevaid e-teenuseid ja mobiilirakendusi kasutama. Samas on Eesti teabevärava mobiilirakenduse kasutusele võtmine ettevõtjatele vabatahtlik ja ei saa prognoosida, kui paljud neist seda teevad. Eesti teabevärava mobiilirakenduse vahendusel isikusamasuse kontrollimiseks on ettevõtjal vaja rakendus alla laadida ja sellesse sisse logida (vt lähemalt seletuskirja p 6.2.1).

⁸³ Statistikaamet 2024. [Rahvaarv](#).

⁸⁴ [Riikliku mobiilirakenduse andmetöötluse õigusanalüüs PPA teenuste näitel](#) 2024.

⁸⁵ Statistikaamet 2023. [Majandusüksused](#).

Ebasoovitava mõju kaasnemise risk on **väike**. Eesti teabevärava mobiilirakenduse kasutusele võtmine võib tuua ettevõtjatele kaasa muudatusi tööprotsessides, lisaseadmete hankimist või olemasolevate lahenduste arendamist. Samas on need muudatuse rakendamiseks ühekordsed ning edaspidi ei kaasne igapäevaseid suuri muudatusi ja kulusid.

Seega on muudatusel sihtrühmale **väheoluline mõju**.

6.2.3. Mõju riigiasutuste töökorraldusele

Sihtrühm: RIA, PPA ja SMIT-i identiteedi ja biomeetria valdkonna ning RIA personaalriigi valdkonna teenistujad. Neid on ligikaudu 30. Seega on sihtrühm **väike**.

Mõju ulatus ja esinemise sagedus on **keskmine**. Muudatus toob sihtrühmale kaasa arendusvajaduse. RIA-s on vajalik protsess juba välja töötatud ja suurem osa arendustööst tehtud. PPA-l ja SMIT-il tekivad andmekogude toimeleogika, baastaristu ja X-tee teenuste arendamisel analüüsi- ja arenduskulud, mis on vajalikud ABIS-e ja ITDAK-i tehniliste rakenduste, sealhulgas serverite ja andmesidevõrgu võimsuse ja mahu suurendamiseks. Samuti peavad PPA ja RIA sõlmima andmevahetuseks andmevahetuslepingu.

Ebasoovitava mõju kaasnemise risk on **väike**. Kaasneb analüüsi- ja arendusvajadus, et luua Eesti teabevärava mobiilirakenduses isikusamasuse kontrollimise funktsioon. Andmekaitse- ja tehnoloogilised riskid on hinnatud ning neid maandatakse kaasaegsete infotehnoloogiliste meetmetega. Lisaks sätestatakse PPA ja RIA andmevahetuslepingus konkreetsed andmetöötlustingimused.

Seega on muudatusel sihtrühmale **väheoluline mõju**.

6.3. Dokumendiliigid ja dokumendi kasutaja kohustused

Eelnõuga **ajakohastatakse dokumendiliikide ja dokumendi kasutaja kohustuste regulatsiooni**:

- 1) kaotatakse kohustus esitada dokumendi kättesaamisel samaliigiline kehtiv dokument;
- 2) kaotatakse nõue tagastada isiku surma või surnuks tunnistamise korral dokument selle väljaandjale;
- 3) karmistatakse nõuet taotleda andmete, näiteks nime muutumise korral uus kohustuslik dokument: edaspidi peab seda tegema ühe kuu jooksul, pärast mida tunnistatakse valede andmetega dokument kehtetuks;
- 4) lõpetatakse Eesti kodanikule ja elanikule digitaalse isikutunnistuse väljaandmine;
- 5) lõpetatakse sertifikaatide kehtivuse peatamise ja taastamise võimalus.

6.3.1. Sotsiaalne, sealhulgas demograafiline mõju

Sihtrühm: dokumendi taotlejad. Need võivad olla kõik Eesti elanikud. Eestis elab 2024. aasta alguse seisuga 1 366 491 inimest.⁸⁶ Kuna sihtrühm võib olla kogu Eesti elanikkond, on see **suur**.

PPA prognoos aastatel 2024–2028 dokumendi taotlejate arvu kohta on toodud tabelis 7.

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

⁸⁶ Statistikaamet 2024. [Rahvaarv](#).

muutumisest on ITDS-i § 14 lõikes 1 ka praegu, kuid kui inimene ei taotle uute andmetega dokumenti, kehtib valed andmetega dokument kuni kehtivusaja lõpuni. Muudatuse tulemusel teavitab PPA edaspidi inimest kohustusest taotleda uus dokument ja kui inimene seda kohustust tähtajal ei täida, tunnistab valed andmetega dokumendi automaatselt kehtetuks. PPA teavitab inimest korduvalt, enne kui tunnistab dokumendi kehtetuks. Surma või surnuks tunnistamise korral dokumendi tagastamise nõude kaotamine vähendab mõnevõrra inimeste halduskoormust.

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

Turvalisuse kaalutlustel lõpetatakse sertifikaatide kehtivuse peatamise ja taastamise võimalus, kuid endiselt jääb alles võimalus tunnistada need kehtetuks näiteks juhul, kui isikutunnistus või elamisloakaart on läinud kaduma. Dokumendi kadumisest või varastamisest teavitamine, et tunnistada sertifikaadid kehtetuks, peab olema kasutaja jaoks kiire ja mugav. Kui dokument leitakse üles, ei taastata selle ega sertifikaatide kehtivust. See tähendab, et sellisel juhul peab edaspidi dokumendi kasutaja taotlema uue dokumendi ja maksma riigilõivu. Ajavahemikul 01.01.–31.10.2023 peatati sertifikaatide 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, näiteks tööülesannete täitmisel. See puudutab ennekõike inimesi, kelle tööülesanded eeldavad sagedasti e-teenustesse sisselogimist ja digiallkirjastamist. Praegu saavad nad selleks kasutada digitaalset isikutunnistust, mida nad ei võta tihti tööpäeva lõpus arvestist välja. Edaspidi selleks näiteks isikutunnistust kasutades peavad nad selle kaasa võtma, sest isikutunnistust võib minna vaja ka väljaspool tööruume, ja kui see unustada tööle arvestisse, ei ole alternatiivi. Samas on digitaalse isikutunnistuse töökoha arvestisse unustamine või jätmine turvarisk, mis võimaldab dokumenti ära kasutada ja inimese nimel tehinguid teha. Seega toob digitaalse isikutunnistuse väljaandmise lõpetamine ühelt poolt selle kasutajale kaasa mõningal määral ebamugavusi, kuid teiselt poolt suurendab ühe dokumendi kasutamine inimese jaoks turvalisust. Edaspidi saavad inimesed digitaalse isikutunnistuse asemel kasutada isikutunnistust või mobiil-ID-d.

Seega on muudatusel sihtrühmale **väheoluline mõju**.

6.3.2. Mõju riigiasutuste töökorraldusele

Sihtrühm: PPA ametnikud, kes menetlevad dokumendi 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. Kuna digitaalse isikutunnistuse väljaandmine lõpetatakse, ei ole PPA-l edaspidi vaja hankida selle isikustamiseks spetsiifilist riistvara.

Ebasoovitava mõju kaasnemise risk on väike. PPA ametnike töökorraldus ei muutu oluliselt ja töömaht pigem väheneb. Vähenevad dokumendiliikide arv ning sertifikaatide kehtivuse peatamise ja uuendamise seotud ülesanded. Samas tuleb menetleda rohkem uute dokumentide taotlusi.

Seega on muudatusel sihtrühmale **väheoluline mõju**.

Tabel 6. Väljastatud dokumentide arv aastatel 2019–2023

	2019	2020	2021	2022	2023
Eesti kodaniku pass	188 121	103 347	119 870	106 036	86 552
Välismaalase pass	15 811	15 814	7955	3235	2430
Digitaalne isikutunnistus	5103	4762	5019	4136	4184
Eesti kodaniku isikutunnistus	281 495	185 284	204 120	263 397	277 774
Euroopa Liidu kodaniku isikutunnistus	6616	6001	6253	5728	5665
Elamisloakaart	52 627	48 213	44 351	78 363	89 880

Allikas: PPA

Tabel 7. Dokumendi taotluste prognoositud arv aastatel 2024–2028⁸⁷

	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	267 000	284 000
Euroopa Liidu kodaniku isikutunnistus	7000	7000	7100	7000	7000
Elamisloakaart	71 000	67 000	61 000	57 000	58 000

Allikas: PPA

6.4. 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 põhimõte on, et iga riik dokumenteerib oma kodanikud ise. Selle põhimõtte ja Eesti identiteedihalduspoliitika turvalisuse tagamiseks:

- 1) antakse PPA-le piiratud õigus nõuda DNA-ekspertiisi välismaalasel, kes taotleb esimest korda Eesti kodaniku dokumenti;
- 2) täpsustatakse välismaalase passi saajate sihtrühma;
- 3) võimaldatakse 15–17-aastase isiku dokumendi väljastamist tema seaduslikule esindajale;
- 4) antakse kinnipidamisasutuse volitatud ametnikule või töötajale õigus võtta sõrmejäljed dokumendi väljaandmise menetluses;
- 5) luuakse dokumendi taotlejale võimalus aktiveerida oma dokument ja sertifikaadid ise.

6.4.1. Sotsiaalne, sealhulgas demograafiline mõju

Sihtrühm: dokumendi taotlejad. Need võivad olla kõik Eesti elanikud. Eestis elab 2023. aasta alguse seisuga 1 365 884 inimest.⁸⁸ Kuna muudatused võivad mõjutada kõiki Eesti elanikke, on sihtrühm **suur**.

⁸⁷ Prognoos põhineb varasemate dokumentide taotlemise andmetel.

⁸⁸ Statistikaamet 2024. [Rahvaarv](#).

Mõju ulatus on **väike** ja esinemise sagedus **keskmine**. Enamik muudatustest on positiivsed ja ei too sihtrühmale kaasa uusi kohustusi ega vajadust kohaneda, vaid avardavad või lihtsustavad isikusamasuse kontrollimist ja võivad vähendada inimeste halduskoormust.

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 kümmekond 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 kodakondsus ja välistada selle omandamine pettuse teel. Muudatus ei puuduta dokumendi taotlejaid, kelle esitatud tõendites või andmetes ei ole alust kahelda.

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, arvestades, et nende halduskoormus dokumendi taotlemisel väheneb.

Seega on muudatustel sihtrühmale **väheoluline mõju**.

6.4.2. Mõju riigiasutuste töökorraldusele

Sihtrühm

- 1) PPA ametnikud, kes menetlevad dokumendi taotlusi. Neid on umbes 160. PPA-s töötab umbes 5000 inimest.
- 2) Eesti välisesinduste töötajad, kes väljastavad dokumente. Neid on 73. Eesti välisesindustes töötab kokku 358 inimest.
- 3) Eesti Kohtuekspertiisi Instituudi DNA-eksperdid. Neid on 13. Eesti Kohtuekspertiisi Instituudis töötab 138 inimest.
- 4) Kinnipidamisasutuse volitatud ametnikud ja töötajad, kes võtavad kinnipeetavate sõrmejälgi. Neid on umbes 12. Vanglateenistuses 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 pääsلاس. 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 Kohtueksperitiisi 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**.

6.5. Lahkumisettekirjutus

Eelnõu § 9 punktidega 1 ja 2 täpsustatakse juba Eesti õigusesse üle võetud tagasisaatmisdirektiivist tulenevat regulatsiooni selliselt, et oleks üheselt arusaadav, et viibimiseluseta 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**⁸⁹, mille rakendamise mõju on hinnatud selle eelnõu seletuskirjas⁹⁰.

Eelnõuga kavandatud täpsustus **ei too kaasa lisamõju**. Lahkumisettekirjutuses märgitakse ka praegu ära, millisesse riiki peab viibimiseluseta 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.

6.6. Välismaalase kinnipidamine

Õigusselguse eesmärgil muudetakse eelnõu § 9 punktidega 3–10 välismaalase kinnipidamise aluseid.

6.6.1. Mõju riigi julgeolekule

Sihtrühm: kinnipeetud välismaalased, keda kahtlustatakse ebaseaduslikus Eestis viibimises või kelle väljasõidukohustus on kindlaks tehtud. Aastas kohustatakse lahkumisettekirjutusega lahkuma ca 1200 Eestis viibimise aluseta välismaalast. Üldjuhul täidavad need välismaalased lahkumiskohustuse vabatahtlikult. Väljasaadetavaid, kelle lahkumiskohustus tuleb pöörata täitmisele kinnipidamise teel, on aastas ca 100. Seega on sihtrühm **väike**.

Mõju ulatus ja esinemise sagedus. Eristades VSS-i §-s 15 selgelt välismaalase kinnipidamise aluseid, luuakse parem õigusselgus olukorras, kui välismaalast on vaja pidada kinni selleks, et teha kindlaks tema väljasõidukohustus ja/või viia läbi Eestist lahkuma kohustamise menetlus. Seetõttu võib muudatuste mõju pidada riigi julgeolekule **väikeseks**: kohanemisvajadust ei ole. Küll aga võimaldavad muudatused selgemini piiritleda, millised riigisisised õigusnormid on seotud Euroopa Liidu õigusega. Mõju on väheoluline ja see esineb **harva**, kuna muudatused

⁸⁹ [RT I, 29.11.2010, 2.](#)

⁹⁰ [793 SE](#) seletuskiri.

puudutavad vaid neid välismaalasi, kelle kinnipidamine on vajalik, et teha kindlaks väljasõidu-kohustus või viia läbi Eestist lahkuma kohustamise menetlus. Enamasti välismaalane väga tihti sellisesse olukorda ei satu.

Ebasoovitava mõju kaasnemise riski ei ole. Eelnõuga ei muudeta välismaalase kinnipidamise põhimõtteid, vaid eristatakse selgelt selle eesmärgi. Tänu sellele paraneb õigusselgus.

Seega on muudatustel sihtrühmale **väheoluline mõju**.

6.6.2. Mõju riigiasutuste töökorraldusele

Sihtrühm: PPA ja KAPO ametnikud. Eelnõu puudutab alla 5% ehk umbes 150 PPA teenistajat. PPA-s töötab kokku umbes 5000 teenistajat. Sihtrühma võib pidada **väikeseks**.

Mõju ulatus. Enamik välismaalasi, kes ei vasta Eestisse saabumise või Eestis viibimise tingimustele, saadetakse juba piiripunktist tagasi riiki, kust nad on Eestisse saabunud. 2023. aastal ei lubatud Eestisse siseneda 260 välismaalasel. Ebaseaduslikult välispiiri ületajate arv on aastate jooksul olnud väike: eelmisel aastal peeti kinni 46 ebaseaduslikult välispiiri ületanud. Tihti esitavad ebaseaduslikult Eestisse saabunud välismaalased kinnipidamisel rahvusvahelise kaitse taotluse või selgub väljasõidukohustuse väljaselgitamisel vajadus pidada välismaalane kinni muul alusel, näiteks Dublini määruse⁹¹ alusel vastutavale riigile üleandmiseks. Seetõttu on muudatustel positiivne mõju, sest pärast välismaalase Eestis viibimise aluse kindlakstegemist saab suunata ta kohe õigesse menetlusse: rahvusvahelise kaitse, tagasisaatmis- või kriminaalmenetlusse. Olukorras, kus välismaalane ei vasta Eestisse saabumise või Eestis viibimise tingimustele ja ta pole esitanud rahvusvahelise kaitse taotlust, tuleb tema kinnipidamisel kohaldada tagasisaatmisdirektiivi. Kuivõrd ka praegu on lubatud välismaalase kinnipidamine nii tema väljasõidukohustuse kindlakstegemiseks kui ka lahkumiskohustuse ettevalmistamiseks ja täitmiseks, on mõju **väike**.

Mõju esinemise sagedus on väike, kuna PPA ja KAPO põhiülesanded ei muutu ja töökorralduse võimalike muudatuste mõju on ühekordne.

Ebasoovitava mõju kaasnemise risk. Kui välismaalase kinnipidamise alus muutub, tuleb PPA-l või KAPO-l vormistada ümber ka välismaalase kinnipidamise protokoll. Seetõttu võib kinnipidamisaluste täpsustamine veidi suurendada PPA ja KAPO töökoormust. Kuivõrd praktikas peetakse kinni vähe välismaalasi, võib ebasoovitava mõju kaasnemise riski pidada **väikeseks**.

Mõju on positiivne, sest muudatused tagavad kinnipidamisaluste kohaldamisel parema õigusselguse ja -kindluse, arvestades menetluse eesmärgi.

Seega on muudatustel sihtrühmale **väheoluline mõju**.

6.7. Koondmõju haldus- ja töökoormusele

Koondmõju **inimeste halduskoormusele on positiivne, kuid väheoluline**. Digitaalse isikutunnistuse väljaandmise lõpetamine toob ühelt poolt selle kasutajale kaasa mõningal määral ebamugavusi, kuid teiselt poolt suurendab ühe dokumendi kasutamine tema jaoks turvalisust.

⁹¹ Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määrus (EL) nr 604/2013, millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest (uuesti sõnastatud). – [ELT L 180, 29.6.2013, lk 31–59](#).

Inimesed ei saa enam taotleda digitaalset isikutunnistust, kuid nad saavad selle asemel jätkuvalt kasutada isikutunnistust või mobiil-ID-d.

E-residentsuse riskiriigi kodanikele muutub e-residendi digi-ID taotlemine keerukamaks, kuid see pole täiesti välistatud. Kui e-residentsuse riskiriigi kodanik soovib Eestis luua ettevõtte, saab ta seda teha notari juures. Sellega kaasneb talle suurem halduskoormus, kuna tal puudub võimalus kasutada ettevõtte loomiseks, asjaajamiseks ja aruandluseks e-residendi digi-ID-d ja Eesti e-teenuseid. Edaspidi aga, kui ettevõtte on loodud ja seos Eestiga olemas, on tal võimalik taotleda Eesti e-teenuste kasutamiseks ka e-residendi digi-ID-d.

Ametiasutuste töökoormusele on mõju samuti **positiivne, kuid väheoluline**. PPA ametnike töökorraldus ei muutu oluliselt ja töökoormus võib pigem väheneda. Muudatused võivad osaliselt vähendada töökoormust näiteks seetõttu, et PPA ei anna enam välja digitaalseid isikutunnistusi. Kuna digitaalse isikutunnistuse väljaandmine lõpetatakse, ei ole PPA-l edaspidi vaja hankida selle isikustamiseks spetsiifilist riistvara.

Lisaks väheneb PPA töökoormus, sest pärast IT-arendustööde valmimist ei pea PPA ametnik edaspidi minema sõrmejälgede võtmiseks vanglasse kohapeale, ja vangla töökoormus väheneb, sest vangla ei pea korraldama PPA ametniku sisenemist pääsلاس. Samuti võib PPA töökoormus väheneda tänu võimalike kohtumenetluste äralangemisele, kui inimese tõsikindel õigus Eesti kodakondsusele ja dokumendile selgitatakse välja objektiivsete tõendite alusel väljaspool kohtumenetlust.

Eesti välisesinduste töökoormus väheneb, sest välismaal elavad Eesti elanikud, kellel on kehtiv eID vahend, saavad oma dokumendi edaspidi kätte kulleriga.

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

Eelnõu rakendamine toob kaasa riigieelarve kulude kokkuhoiu tänu sellele, et lõpetatakse ITDS-i § 20¹ lõike 2 alusel digitaalse isikutunnistuse väljaandmine. Kaasnevad kulud on seotud peamiselt vajadusega arendada infosüsteeme. SMIT hindab arendusmahtu PPA esitatavate arendusvajaduste alusel ja kulud kaetakse SMIT-i eelarvest.

- 1) Muudatus, millega antakse kinnipidamisasutuse volitatud ametnikule või töötajale **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 e-residentsuse riskiriigi kodanikele**, võib mõjutada riigi maksulaekumist, kuna e-residentsuse riskiriigi kodanikud, kellele erisused ei kohaldu, ei saa edaspidi e-residendi digi-ID-d taotleda ega seeläbi Eestis lihtsamalt ettevõtlusega alustada. Muudatuse rakendamine toob kaasa ka PPA iseteeninduse arendamise kulud, 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) Muudatusega, millega **luuakse võimalus kontrollida isikusamasust Eesti teabevärava mobiilirakenduse vahendusel**, kaasnevad Siseministeeriumi valitsemisalale täiendav analüüsivajadus ja infotehnoloogilised kulud, sealhulgas andmekogude toimeleotika ja baastaristu arendamise kulud, mis on vajalikud eriti ABIS-e ja ITDAK-i tehniliste rakenduste, sealhulgas serverite ja andmesidevõrgu võimsuse ja mahu suurendamiseks.

Juhul kui Eesti teabevärava mobiilirakenduse vahendatud kontrollpäringute tippkoormus langeb töövälisele ajale, võivad kasvada ka personalikulud, eriti rakenduse kasutamise algfaasis. Samuti kaasnevad turvatestimise kulud. Kõigi selliste kulude katmiseks on vaja planeerida raha SMIT-i eelarvesse. Kulude suurusjärgu hindamiseks on vajalik sisuline lähteülesanne, milles on muu hulgas planeeritud päringu andmekoosseis, maksimaalne samaaegsete päringute arv ning eeldatav tippkoormuse aeg nädalapäeva ja kellaaja täpsusega. Kulude katmine lepitakse kokku eraldi.

Eesti teabevärava mobiilirakenduse loomisega kaasnevad kulud MKM-i valitsemisalale. Rakendus koondab erinevaid riiklikke e-teenuseid ja selle kogumaksumus on 799 990 eurot. Eelnõuga võimaldatakse rakendada esmalahendust, mis võimaldab ruutkoodi abil Eesti piires isikusamasust kontrollida. MKM-i valitsemisala 2024. aasta eelarves on lisaks 400 000 eurot jätkuanalüüsiks ja -arenduseks ning järgnevatel aastatel on planeeritud hinnanguliselt 600 000 eurot iga-aastasteks arenduskuludeks. RIA-s on ka majasisene alaline arendusmeeskond.

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, 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“;
- 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** „Suurema rahapesu või terrorismi rahastamise riskiga riikide ja Eestiga justitiis-, julgeoleku- või õiguskaitsealase koostöösuhteta riikide loetelu ning nende riikide kodanikele e-residendi digitaalse isikutunnistuse väljaandmise erisused“. Volitusnormi vajalikkust, selle eesmärki, sisu ja ulatust ning selle alusel kavandatava rakendusakti vastavust PS-ile on põhjendatud seletuskirja punktides 2.3 ja 3.1.5.

Rakendusaktide kavandid on seletuskirja lisa 1. 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.

- Eelnõu **§ 1 punktid 14 ja 43, § 3 punktid 8–10 ning § 6** on seotud riigilõivuseaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduses sätestatud uue riigilõivumääraga ning jõustuvad selle seadusega samal ajal: 2025. aasta 1. jaanuaril.
- Muudatused, mille rakendamiseks on vaja teha infotehnoloogilisi arendustöid, jõustuvad pärast nende valmimist.
 - Eelnõu **§ 1 punktid 2–4, 9, 12, 13, 25, 46 ja 50**, millega lõpetatakse sertifikaatide kehtivuse peatamine ja taastamine ning suurendatakse perekonnanime tähemärkide arvu dokumendil, jõustuvad 2025. aasta 15. novembril.
 - Eelnõu **§ 1 punkt 23**, millega võimaldatakse dokumendi taotlejal aktiveerida ID-1 formaadis dokument ja sertifikaadid elektrooniliselt, jõustub 2026. aasta 1. juunil.

10. Eelnõu koostöölastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitati eelnõude infosüsteemi (EIS) kaudu koostöölastamiseks ministriumidele ning arvamuse avaldamiseks Andmekaitse Inspeksioonile, EIS-ile, KAPO-le, PPA-le, RAB-ile ja SMIT-ile.

Eelnõu oli esimesel koostöölastusringil⁹² 23.01.–16.02.2024. Kultuuriministeerium koostöölastas eelnõu märkusteta. Haridus- ja Teadusministeerium, Kliimaministeerium, Regionaal- ja Põllumajandusministeerium ning Sotsiaalministeerium koostöölastuskirja ei esitanud. EIS ja KAPO eelnõu kohta arvamust ei avaldanud.

JUM-i, Kaitseministeeriumi, MKM-i, RAM-i, VÄM-i, Andmekaitse Inspeksiooni, Eesti Info- tehnoloogia ja Telekommunikatsiooni Liidu, PPA, RAB-i ning SMIT-i esitatud ettepanekuid on võimaluse piires arvestatud (vt seletuskirja lisa 2).

Algatab Vabariigi Valitsus 2024

⁹² Eelnõude infosüsteemi toimiku nr [24-0064](#).