Isikut tõendavate dokumentide seaduse muutmise ja sellega seonduvalt
teiste seaduste muutmise seaduse eelnõu seletuskiri
Lisa 2

Kooskõlastustabel

Esitaja/märkuse sisu	Märkuse arvestamine/mittearvestamine
Justiitsministeerium	
1. Isikuandmete töötlemine on PS §-s 26 sätestatud isiku eraelu puutumatuse riive, mida võib teha ainult kooskõlas seadusega (PS § 3 ja § 11). Sealjuures tuleb tagada, et põhiõiguse riive on vajalik ja proportsionaalne taotletava eesmärgi suhtes. Olukorras, kus regulatsioon riivab isikute põhiõigusi, tuleb teha põhiõiguse riive proportsionaalsuse analüüs. Põhiõiguste riive on põhiseaduspärane üksnes siis, kui see on põhjendatud. Selleks et riive oleks põhjendatud, peab riive aluseks olev meede olema proportsionaalne. Proportsionaalne on meede siis, kui ta järgib legitiimset eesmärki, on kohane ehk sobiv, vajalik ja proportsionaalne kitsamas tähenduses. Igasuguse isikuandmete töötlemise puhul tuleb lähtuda andmetöötluse üldpõhimõtetest vastavalt isikuandmete kaitse üldmääruse (IKÜM) artiklile 5. See tähendab, et isikuandmete töötlemine peab olema seaduslik, õiglane ja läbipaistev, andmeid kogutakse konkreetsel eesmärgil, minimaalselt ja kogutavad andmed on kooskõlas kogumise eesmärgiga, tagatakse andmete õigsus, sätestatud on säilitamistähtajad ning töötlemine on turvaline. Isikuandmete töötlemise eesmärk peab olema täpselt ja selgelt määratletud. Isikuandmete töötlemiseks peab olema õiguslik alus vastavalt IKÜM artiklile 6. Märgime, et pelgalt andmekogudes andmetele juurdepääsu andmise kaudu ei saa kehtestada õiguslikku alust isikuandmete töötlemiseks. Seaduse tasandil tuleb kehtestada selge ja konkreetne eesmärk, milleks on andmetöötlus vajalik. Eesmärgi piisav täpsuse aste on vajalik selleks, et andmesubjektile oleks tema andmete kasutamine eeldatav ja ettenähtav. Ka isikuandmete teisesel eesmärgil töötlemine peab olema kehtestatud õigusaktiga ning vajalik ja proportsionaalne saavutatava eesmärgi suhtes	<u>Arvestatud osaliselt</u> Eelnõu seletuskirja täiendatud selgitustega. Eelnõu väljatöötamisel on arvestatud IKÜM nõuetega. Eelnõu seletuskirja on täiendatud põhiseaduspärasuse analüüsiga muudatuste osas, millega antakse õigus e-residendi andmete väljastamiseks ja nende töötlemiseks Ettevõtluse ja Innovatsiooni Sihtasutusele (eelnõu § 1 p 11) ning muudatuse osas, millega võib nõuda Eesti kodaniku dokumendi taotlejalt DNA-ekspertiisi, kui täiskasvanu taotleb esimest korda Eesti kodaniku dokumenti ning PPA-l tekib põhjendatud kahtlus, kas välisriigis väljaantud Eesti kodakondsuse õigust tõendav dokument või selle alusandmed on õiged (eelnõu § 1 p-d 7 ja 21), samuti isikut tõendava dokumendi taotluses märgitud kontaktandmetele teavituste saatmise osas. Teised kooskõlastuskirjas välja toodud isikuandmete töötlemisega seotud muudatused kehtivad ka praegu ja eelnõuga üksnes täpsustatakse kehtivat regulatsiooni, isikuandmete töötlemise põhimõtete muutmist eelnõuga ei kavandata ja seega ei ole vaja üle hinnata, kas muudatusega taotletud eesmärki on võimalik saavutada ka isiku põhiõigusi vähem riivaval moel. Isikuandmete kaitse seaduse § 56 lõike 1 kohaselt teostab isikuandmete kaitse seaduses, selle alusel kehtestatud õigusaktides ning Euroopa Parlamendi ja nõukogu määruses (EL) 2016/679 sätestatud nõuete ning muudes seadustes isikuandmete töötlemisele kehtestatud nõuete täitmise üle riiklikku ja haldusjärelevalvet Andmekaitse Inspektsioon. Kui isikuandmete töötlemise kehtiva regulatsiooniga on probleeme või ei vasta andmetöötlus õigusaktides sätestatud nõuetele, peaks see kehtivate sätete puhul olema selgunud ja rikkumine kõrvaldatud

(IKÜM art 6 lõige 4) ning kooskõlas IKÜM artikli 23 nõuetega. IKÜM põhjenduspunktis 50 on selgitatud, et selleks, et teha kindlaks, kas edasise töötlemise eesmärk vastab eesmärgile, mille jaoks isikuandmed algselt koguti, peab vastutav töötleja võtma pärast kõikide esialgse töötlemise seaduslikkuse seisukohast vajalike nõuete täitmist muu hulgas arvesse mis tahes seoseid sellise eesmärgi ja kavandatava edasise töötlemise eesmärgi vahel, isikuandmete kogumise konteksti, eelkõige andmesubjekti ja vastutava töötleja vahelisel suhtel põhinevaid andmesubjekti mõistlikke ootusi andmete edasise kasutamise suhtes, isikuandmete laadi, kavandatava edasise töötlemise tagajärgi andmesubjekti jaoks ning asjakohaste kaitsemeetmete olemasolu nii esialgsetes kui ka kavandatavates edasistes isikuandmete töötlemise toimingutes. Lisaks märgime, et arvesse tuleb võtta ka läbipaistvuse nõuet andmesubjekti jaoks (IKÜM art 5 lg 1 punkt a). Tuleb luua konkreetsed, selged ja isikutele läbipaistvad ning arusaadavad õiguslikud alused andmetöötluseks ja teha õigusaktides vajalikud muudatused. Eelnõus kavandatud muudatuste osas ei ole läbi viidud põhiseaduspärasuse analüüsi. Tegemist on olulise puudusega, kuna eelnõus kavandatud isikuandmete töötlemist sisaldavate muudatuste puhul ei ole võimalik hinnata, kas muudatusega taotletud eesmärki on võimalik saavutada ka isiku põhiõigusi vähem riivaval moel. Eelkõige puudutab ülaltoodu järgnevaid eelnõu sätteid, milles sisalduvate puuduste kohta juhime tähelepanu ka käesoleva kirja järgmistes punktides: 1) e-residendi digi-ID andmete väljastamine järelevalvemenetluses (§ 1 p 9 ja 12); 2) andmete väljastamine Ettevõtluse ja Innovatsiooni Sihtasutusele (EIS) ja nende töötlemine EIS-i poolt (§ 1 p 11); 3) Rahapesu Andmebüroo (RAB) õigus töödelda e-residendi isikuandmeid (§ 1 p-d 51 ja 52); 4) dokumendi taotleja DNA-ekspertiis (§ 1 p-d 7 ja 21); 5) dokumendi kontrollimine (§ 1 p 41);	järelevalvemenetluses. Kehtivate sätete põhiseaduspärasust hindab kohus. Täpsemad selgitused kooskõlastuskirjas esitatud väidetavate puuduste osas on toodud järgmistes punktides.

6) andmekogudes andmete säilitamise tähtajad (§ 1 p 38 ja 40, § 2 p 6 ja 8, § 3 p 2, § 4 p 2, § 7 p 2, § 9 p 7 ja 12, § 10 p 2). Palume eelnõu seletuskirja täiendada kavandatud muudatuste osas ka põhiseaduspärasuse analüüsiga.	
2. Eelnõu § 1 punkt 11 reguleerib PPA õigust edastada andmeid EIS-ile ja EIS-i õigust neid töödelda. EIS-ile soovitakse anda õigus töödelda e-residendi digitaalse isikutunnistuse väljastamise menetluses kogutud andmeid selleks, et analüüsida isikut tõendavate dokumentide seaduse (ITDS) § 20^5 lõikes 2 nimetatud eesmärgi täitmise tulemuslikkust ja mõju ning osutada selle eesmärgi täitmiseks vajalikke personaliseeritud teenuseid ning lisaks tuvastada ja maandada e-residendiga seotud riske. Tekib küsimus, kas EIS-i poolt kavandatakse automatiseeritud andmetöötlust IKÜM artikli 22 mõttes? ITDS § 20^5 lg 2 kohaselt on e-residendile digitaalse isikutunnistuse väljaandmise eesmärk soodustada Eesti majanduse, teaduse, hariduse või kultuuri arengut, luues võimaluse kasutada e-teenuseid Eesti digitaalse dokumendiga. Sisuliselt kavandatakse EIS-ile järgnevate ülesannete andmist: 1) e-residendile digitaalse isikutunnistuse väljaandmise tulemuslikkuse ja mõju analüüsimine; 2) e-residendile personaliseeritud teenuste osutamine; 3) e-residentidega seotud riskide tuvastamine ja maandamine. Selleks antakse EIS-le õigus töödelda isikuandmeid järgnevas andmekoosseisus: e-residendi ees- ja perekonnanimi, isikukood, kui see on olemas, sünniaeg, sugu, kodakondsus ning kontaktandmed, e-residendi digitaalse isikutunnistuse väljastamise koht, väljaandmise aeg, kehtivusaeg ja kehtetuks tunnistamise aeg, e-residendi digitaalse isikutunnistuse taotlemise eesmärk ja plaanitava tegevuse kirjeldus ning taotlemise põhjendus.	Arvestatud osaliselt Eelnõuga ei anta EIS-ile uusi täiendavaid ülesandeid, EIS-i põhikirja[2] kohaselt on EIS-i eesmärk muu hulgas: 2.1.5 luua kapitalile ligipääsu parandamise ning riskide maandamise, toetuste ja teenuste abil võimalusi ettevõtluse ja ekspordi arenguks; 2.1.6 kaasata välismaiseid otseinvesteeringuid Eestisse ja edendada välismaiste ettevõtjatega osalust ja koostööd Eesti majandusega; 2.1.8 arendada ja toetada Eesti iduettevõtlusvaldkonda. EIS-i põhiülesanneteks riiklikest arengukavadest ja poliitikatest lähtudes on põhikirja kohaselt muu hulgas: 2.2.7 riiki, ärikeskkonda, siin tegutsemise võimaluste ja riigi teenuseid tutvustavate turundustegevuste elluviimine ja tulemuslikkuse mõõtmine; 2.2.8 ettevõtete arengu toetamiseks ja tööjõukriisi leevendamiseks kõrgemat lisandväärtust loovate välisspetsialistide kaasamise tegevused: meelitamine, saabumise ja kohanemise teenused; 2.2.11 oma vastutusvaldkondades andmete ja informatsiooni kogumine, süstematiseerimine, analüüsimine ja edastamine; 2.2.12 riiklike strateegiliste ja muude poliitikadokumentide sisu, ettevõtlusega seotud avalike teenuste ja ärikeskkonna arendamise kohta oma valdkondades ettepanekute tegemine. Eelnõuga kavandatakse anda EIS-ile õigus töödelda e-residendi isikuandmeid, millega võimaldatakse EIS-il täita põhikirjast tulenevaid ülesandeid eesmärgipäraselt. Seega ei ole tulemuslikkuse ja mõju analüüsimise puhul tegemist uuringuga IKS § 6 mõttes.

[2] EIS-i põhikiri. Vaadatud 06.03.2024.

Ebaselge on, kas tulemuslikkuse ja mõju analüüsimise puhul on tegemist uuringuga isikuandmete kaitse seaduse (IKS) § 6 mõttes. Kui sellel juhul on silmas peetud poliitika kujundamise uuringute tegemist, siis on vastav pädevus IKS § 6 lg 5 mõttes ainult täidesaatva riigivõimu asutusel. EIS sellele määratlusele ei vasta. Sellele asjaolule on Justiitsministeerium juhtinud tähelepanu ka 22.01.2023 väljatöötamiskavatsuse kooskõlastuskirjas. Põhjalikumat hindamist vajab, kas andmete töötlemise õiguse laiendamine personaliseeritud teenuste osutamiseks on kooskõlas IKÜM artikli 5 lõikes 1 punktis b sätestatud eesmärgipiirangu põhimõttega (täpsemalt selgitatud käesoleva kirja punktis 1). E-residentidega seotud riskide hindamine ja maandamine on olemuselt järelevalvetegevus, millele viitab ka seletuskiri (lk 9). Märgime, et vastavat pädevust EIS põhikirja järgi ei oma ja küsitav on sellise ülesande andmine avaliku võimu teostamise õigust mitteomavale asutusele. Eelnevalt välja toodud ebaselguste tõttu ei ole võimalik hinnata ka eelnõus sätestatud EIS-ile edastatava andmekoosseisu vastavust andmetöötluse eesmärkidele. Kavandatud andmetöötluse puhul puudub ka info, kuidas on reguleeritud andmetöötlus EIS-i poolt. Selgitame, et seaduse tasandil pelgalt andmete edastamise ja saamise õiguse kehtestamisel ei looda andmetöötlemiseks õiguslikku alust IKÜM artikli 6 mõttes ning see ei ole kooskõlas IKÜM artiklis 5 sätestatud isikuandmete töötlemise põhimõtetega. Seletuskirjas (lk 9) viidatu kohaselt on e-residente hinnanguliselt 105 000. Eelnõuga kavandatud EIS-i ülesanded näevad näiteks tegevuse hindamise ja profiili alusel teenuste osutamise näol ette e-residentide isiklike aspektide süstemaatilise ja ulatusliku hindamise, mille tulemused võivad isikutele olulist mõju avaldada. Juhul, kui isikuandmete töötlemise laad, ulatus, kontekst või eesmärk võib kaasa tuua inimestele suure ohu (andmelekked,	Lisaks ei ole õige eristada e-residendile digitaalse isikutunnistuse väljaandmise tulemuslikkuse ja mõju analüüsi personaliseeritud teenuste osutamisest, sest personaliseeritud teenuse pakkumine on otseses seoses analüüsi tulemustega. Personaliseeritud teenust pakutakse e-residendile, kellel täpselt seda teenust vaja on. Personaliseeritud teenus ei ole seotud turundustegevusega, samuti ei töötle EIS e-residendi andmeid selleks, et reklaam oleks paremini sihistatud. VTK kooskõlastuskirja osas selgitame, et kooskõlastamisel toimus MKM-i ja JUM-i kohtumine, mille tulemusel edastas JUM MKM-ile e-kirja, milles on öeldud: *„/.../ Vaadates Ettevõtluse ja Innovatsiooni Sihtasutuse põhikirja punkte 2.2.7 ja 2.2.11 ning VTK-s toodud ülesandeid, milleks on e-residentsuse programmi edendamine ja eesmärkide elluviimine e-residentide kohta andmete kogumine, analüüsimine, turundustegevuste ellu viimine ja tulemuslikkuse (mõju) mõõtmine. Samuti seda, et tegemist on avalikes huvides oleva ülesande täitmisega, mille igakülgne ja efektiivne teostamine sõltuvana e-residendi nõusolekust võib osutuda keeruliseks ega pruugi anda usaldusväärset tulemust. Seega võib jaatada sellisel eesmärgil andmete töötlemisel nõusolekust loobumist ning andmete töötlemisele seadusliku aluse sätestamist. /.../“* Lisaks rõhutame, et EIS ei võta andmetöötluse tulemusena vastu andmesubjekti mõjutavaid otsuseid, mis toovad kaasa teda puudutavaid õiguslikke tagajärgi või avaldavad talle märkimisväärset mõju. E-residendi staatuse andmise otsustab dokumendi väljaandja ehk PPA ning otsus on enne EIS-ile andmete edastamist juba tehtud ehk EIS-iga jagatakse vaid e-residendi andmeid. Enne positiivse otsuse tegemist ei edastata EIS-ile andmeid taotleja ega taotluse kohta. EIS töötleb e-residendi andmeid, et pakkuda e-residendile paremat tuge ettevõtlusega alustamisel ja vajaduse korral selgitada välja, mis takistab e-residendil saavutada e-residentsuse taotlemise eesmärki ning pakkuda tuge sellise takistuse ületamiseks. Seega ei ole

väärkasutuse jms) ning andmetöötlus on ulatuslik ja süsteemne, tuleb töötlemise kavandamiseks läbi viia andmekaitsealane mõjuhinnang vastavalt IKÜM artiklile 35[1]. Palume koostada andmekaitsealane mõjuhinnang, mis peab muuhulgas kajastama kooskõla IKÜM artiklis 5 sätestatud andmetöötluse põhimõtetega, st milliseid andmeid, mis eesmärgil jne töödeldakse. Täiendavalt juhime tähelepanu, et isikuandmete töötlemisel tuleb seaduse tasandil sätestada ka töötlemise kestus ehk säilitamise tähtaeg. Palume need küsimused eelnõus lahendada.	tegemist automatiseeritud andmetöötlusega IKÜM artikkel 22 mõttes. IKÜM artikli 5 lõige 1 punkt b sätestab, et isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus. EIS jälgib e-residendi digi-ID taotluse aluseks olnud eesmärgi saavutamist takistavate või selle saavutamist negatiivselt mõjutavate riskide esinemist ning vajaduse korral pakub e-residendile selle eesmärgi saavutamiseks vajalikke personaliseeritud teenuseid. Selgitame, et e-residendi andmete töötlemine personaliseeritud teenuse osutamiseks ei ole vastuolus andmete töötlemise eesmärgipiirangu põhimõttega. E-resident on välismaalane, kellele Eesti on hüvena loonud isiku kodakondsusjärgse riigi identiteedi alusel digitaalse identiteedi ja andnud välja digitaalse isikutunnistuse – e-residendi digi-ID. E-residendi digi-ID on digitaalne dokument, mis on kasutatav üksnes elektroonilises keskkonnas isiku tuvastamiseks ja digitaalse allkirja 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. Siinkohal rõhutame, et Eesti e-residendiks saamine on välismaalase privileeg, mitte õigus. ITDS § 20[6] kohaselt on e-residentsuse saamisel aluseks olemasolev seos Eesti riigiga või põhjendatud huvi Eesti e-teenuseid kasutada. Eesti riik kasutab kaalutlusõigust ja taustakontrolli, et anda e-residentsus ainult usaldusväärsetele ja õiguskuulekatele välismaalastele. Riigil on õigus e-residentsust mitte anda, selle kehtivus peatada või kehtetuks tunnistada. Selleks, et tagada e-residentsuse jätkusuutlik usaldusväärsus, viiakse ellu äriprotsesside ja

[1] Eestis on andmetöötluse ulatuslikkuse kriteeriumiks muuhulgas isikuandmete töötlemine 50000 ja enama isiku kohta. Täpsemalt Andmekaitse Inspektsiooni selgitus: https://www.aki.ee/uudised/mojuhinnang-riskide-kaardistamine-ja-hindamine

	infosüsteemide riskianalüüse. EIS jälgib ITDS-i § 20^5 lõikes 2 nimetatud eesmärgi saavutamist takistavate või nende saavutamist negatiivselt mõjutavate riskide esinemist ning vajaduse korral pakub e-residendile selle eesmärgi saavutamiseks vajalikke personaliseeritud teenuseid. Samuti toimub pidev e-residendi programmiga seotud riskide ülevaatamine ja hindamine, et koordineerida riskide maandamist. Isikuandmete töötlemise põhimõtted on kättesaadavad EIS-i veebilehel. Andmete säilitamise tähtaja osas on veebilehel info, et juhul, kui andmete säilitamise tähtaeg on määratud õigusaktiga, siis lähtutakse õigusaktis toodud tähtajast. Andmete säilitamise tähtaeg on eelnõusse lisatud. E-residendi digi-ID kehtib viis aastat. EIS võib e-residendi andmeid säilitada kuni viis aastat arvates e-residendi digi-ID väljaandmisest või kui e-residendi digi-ID tunnistatakse kehtetuks enne kehtivusaja lõppu, siis selle kehtetuks tunnistamiseni. Dokumendimenetluses kantakse andmed isikut tõendavate dokumentide andmekogusse (edaspidi: *ITDAK*). ITDS § 15^2 lõike 2 kohaselt on ITDAK-i pidamise eesmärk avaliku korra ja riigi julgeoleku tagamine isiku tuvastamise ja ITDS-i § 15 lõikes 4 sätestatud isikut tõendavate dokumentide väljaandmise ning kehtetuks tunnistamisega seotud andmete ja neid dokumente taotlenud isikute andmete töötlemise kaudu. ITDS § 20^6 lõike 4 kohaselt võib e-residendi digitaalse isikutunnistuse (edaspidi *e-residendi digi-ID*) tunnistada kehtetuks, kui ilmneb mõni ITDS § 20^6 lõikes 2 või 3 nimetatud e-residendi digi-ID väljaandmisest keeldumise alus. Lõike 2 kohaselt keeldutakse e-residendi digi-ID väljaandmisest muu hulgas, kui isik ohustab avalikku korda või riigi julgeolekut (ITDS § 20^6 lg 2 p 1). E-residendi digi-ID väljastatakse kindlal eesmärgil ja taotleja plaanitvast tegevusest lähtudes. E-residendi digi-ID taotleja on kohustatud taotluse esitamisel tõendama või põhistama e-residendi digi-ID väljaandmise

	aluseks olevaid asjaolusid. Seega väljastatakse e-residendi digi-ID igal juhul konkreetseks tegevuseks ja e-resident on sellega edaspidi seotud. Eeltoodust tulenevalt tehakse riiklikku järelevalvet ka üksnes e-residendi digi-ID (mitte ühegi teise isikut tõendava dokumendi) kasutamise üle. Kui personaliseeritud teenuse osutamise käigus saavad EIS-ile teatavaks asjaolud, mis võivad olla e-residendi digi-ID kehtetuks tunnistamise või kehtivuse peatamise aluseks, on EIS kohustatud edastama selle teabe PPA-le (põhikirja punkt 2.2.11). Kui PPA menetluse tulemusena 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. EIS-i tegevus ei ole seotud järelevalve teostamisega. EIS toetab e-residenti, lähtudes tema profiilist ning e-residendi digi-ID taotlemise eesmärgist ja plaanitavast tegevusest, näiteks 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 vajaduse korral selgitada välja, mis takistab e-residendil liikuda soovitud eesmärgi poole, mille saavutamiseks ta e-residendiks hakkas. Kui EIS avastab oma tavapärase tegevuse käigus võimalikke e-residendi digi-ID väärkasutuse mustreid ja e-residendi profiilist tulenevaid riske, edastab ta vastava info järelevalveasutusele. EIS ise järelevalveasutus ei ole ja järelevalvet ei teosta. IKÜM artikli 35 lõike 3 kohaselt on andmekaitsealase mõjuhinnangu tegemine nõutav 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, või c) avalike alade ulatuslik süstemaatiline jälgimine. EIS-ile andmete edastamisel ei esine ühtegi IKÜM artikli 35 lõikes 3 nimetatud olukorda. Seega ei ole andmekaitsealase mõjuhinnangu tegemine kohustuslik.
3. Eelnõu § 1 punktid 7 ja 21 reguleerivad dokumendi taotlejalt tasulise DNA-ekspertiisi nõudmist. Muudatusega soovitakse kehtestada DNA-ekspertiisi kohustus isikule esmakordsel Eesti kodaniku dokumendi taotlemisel juhul, kui PPA-l tekib põhjendatud kahtlus, kas välisriigis väljaantud Eesti kodakondsuse õigust tõendav dokument on ehtne või kas selle alusandmed on õiged. Märgime, et isiku DNA-andmed on IKÜM artikli 9 kohaselt eriliigilised andmed, mille töötlemine on üldjuhul keelatud, välja arvatud art 9 lõikes 2 sätestatud tingimustel. Eelnõu seletuskirjas ei ole avatud, millisel alusel andmetöötlust kavandatakse. Kui selleks aluseks on IKÜM art 9 lg 2 punkt g, mille kohaselt on töötlemine vajalik olulise avaliku huviga seotud liikmesriigi õiguse alusel, siis peab see olema proportsionaalne saavutatava eesmärgiga, austama isikuandmete kaitse õiguse olemust ning tagama sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks. Seletuskirjas (lk 23) on öeldud, et kui PPA-l on alust kahelda dokumendi taotleja esitatud lisaandmete õigsuses või tõendite ehtsuses võib nõuda DNA-ekspertiisi tegemist. Põhjendatud on seda nii, et kui isik ei esita täiendavaid tõendeid ega dokumente, jätab PPA taotluse läbi vaatamata ja kuna sageli sellised otsused vaidlustatakse, siis tekib riigile aja- ja ressursikulu. Muudatuse eesmärk on mõistetav, kuid antud juhul ei ole kaalutud, kas sama eesmärki on võimalik saavutada ka teiste vahenditega, nt täiendavate dokumentaalsete tõenditega, dokumendile ekspertiisi tegemisega vms. Seletuskirja põhjal on neid juhtumeid vähe, kuid eelnõuga kehtestatakse sisuliselt kohustus isikule DNA-ekspertiisi tegemiseks, kui dokumentide põhjal tekib kahtlus isiku päritolus. Samas ei ole selgitatud, kuidas toimub ekspertiisi tegemine ning ekspertiisi tulemuste töötlemine PPA poolt, millisesse andmekogusse	Arvestatud Seletuskirja täiendatud selgitustega, et DNA-ekspertiis on kohtuekspertiisi seaduses sätestatud tasuline ekspertiis ja selle tegemine toimub nagu tavalise tasulise ekspertiisi tegemine. Seletuskirja punktis 3.3.2. selgitatakse eelnõu § 1 punkte 7 ja 21, selgituste punktis 2 on öeldud, et DNA-ekspertiisi tellib ja selle kulu katab isik. KES § 11 lõike 5 kohaselt kehtestab tasuliste ekspertiiside loetelu ning nende tegemise ja vormistamise korra ning säilitatavate andmete loetelu valdkonna eest vastutav minister määrusega. Kuivõrd kord on praeguseks kehtestamata, siis on meil väga raske seletuskirjas täpsemalt kirjeldada, kuidas tasulise ekspertiisi tegemine praktikas hakkab välja nägema. Plaanis ei ole kehtestada eritingimusi, DNA-ekspertiis toimub nagu iga teine tasuline ekspertiis. KES § 11 lõike 4 kohaselt võib ekspertiisiasutus teha füüsilistele ja juriidilistele isikutele menetlusasjadega mitteseotud tasulisi ekspertiise, kui see ei takista tema menetlusasjades tehtavate ekspertiisidega seotud ülesannete täitmist. Kui DNA-ekspertiisi tellija oleks PPA, siis oleks see haldusorgani menetlusasjaga seotud ekspertiis ja viidatud lõige 5 ei kohalduks. Lisaks on eelnõu punktis 7 kavandatud ITDS § 9^2 lõikes 6^2 ning seletuskirjas vastava lõike selgituses öeldud, et DNA-ekspertiisi tellib ja kulud kannab isik. Seega, isik ise tellib ekspertiisi ja selle eest maksab samuti isik ise otse EKEI-le. Et DNA-ekspertiisi tulemuse võltsimise kahtlus juba ennetavalt kõrvaldada, peaks DNA-ekspertiisi tulemus laekuma otse EKEI-lt PPA-le ja seda peaks võimaldama kavandatav ITDS § 9^2 lõige 6^3.

ekspertiisi tulemused kantakse, mil viisil töödeldakse ja kui kaua neid säilitatakse. Seega ei ole selge, kas valitud meede on põhjendatud kavandatud eesmärgi täitmiseks. Palume nii eelnõu kui ka seletuskirja täiendada. Lisaks juhime tähelepanu, et seletuskirjas (lk 23) räägitakse isaduse tuvastamisest, kuid Eesti Kohtuekspertiisi Instituudi (EKEI) andmetel on oluliselt rohkem hakatud küsima ka emaduse tuvastamise võimalusi. Seega oleks õigem rääkida põlvnemisest, mis on laiem mõiste. Samuti on märgitud (lk 23), et tasuline DNA-ekspertiis maksab 70 eurot. Palume seda selgitust täpsustada, et hind on 70 eurot ühe analüüsitud isiku kohta. Lisaks palume seletuskirjas täpsemalt kirjeldada, kuidas sellise DNA-ekspertiisi tellimine praktikas välja nägema hakkab. Kas isikud lähevad ise EKEI-sse ja tellivad ekspertiisi nagu tavalise tasulise ekspertiisi korral, EKEI sõlmib nendega lepingu ja väljastab neile eksperdiarvamuse, mille isik esitab seejärel PPA-le? Või tellib ekspertiisi PPA ning EKEI saadab vastuse ja õiendi tasumiseks PPA-le, kes nõuab ise kulud isikult välja?	Kuidas andmevahetus praktikas toimima hakkab, kas tehakse automaatne andmevahetus või lepitakse kokku muud moodi, on rakendusasutuste omavaheline kokkulepe. Kuivõrd DNA ekspertiis tellitakse dokumendimenetluses ja see on tõendiks konkreetses menetluses otsuse tegemisel, siis hoitakse ekspertiisi tulemust koos isiku taotluse ja muude taotlusele lisatud andmete ning tõenditega ITDAK-s.
4. Eelnõu § 1 punkt 8 näeb haldusorganile ette õiguse isiku kontaktandmeid kasutada talle menetluse kohta teavituste saatmiseks. Seletuskirjas (lk 24) on selgitatud, et PPA-le antakse selge õigus töödelda isikuandmeid ka selleks, et saata ITDS-s sätestatud menetluste kohta teavitusi, näiteks dokumendi väljaandmise menetluse staatuse või kehtivuse lõpptähtaja kohta, kasutades selleks varasema dokumendi väljaandmise menetluse andmeid. ITDS-s sätestatud menetluste raames võib isikut teavitada menetluse asjaoludest haldusmenetluse seaduse § 25 lõike 1 alusel. Juhul, kui eesmärgiks on isikute täiendav teavitamine, peab sellise õiguse kehtestamine olema põhjalikult kaalutud ja vajalik. Leiame, et eelnõus ei ole sellist vajadust veenvalt põhjendatud. Juhul, kui isikute täiendav teavitamine siiski kehtestada, on see võimalik ainult juhul, kui isik on andnud varasemas menetluses selleks nõusoleku ning ka siis peab isikule jääma võimalus nõusolek igal ajal tagasi võtta. Palume eelnõu vastavalt muuta.	Arvestatud HMS § 25. Kättetoimetamise viisid (1) Haldusakt, kutse, teade või muu dokument toimetatakse menetlusosalisele kätte postiga, dokumendi väljastanud haldusorgani poolt või elektrooniliselt. Kavandatav muudatus ei käsitle ITDS-s sätestatud menetluste raames teavitamist ja ka mitte selle menetluse asjaoludest teavitamist. ITDS-is sätestatud dokumendi väljaandmise menetlus lõpeb dokumendi väljaandmisega. HMS § 25 lõiget 1 saab kohaldada juhul, kui tõlgendada väga laialt ja väita, et dokumendimenetlus kestab kogu dokumendi kasutamise aja jooksul. Sättega soovisime rohkem selgust just andmekaitse seisukohast. Kuna tegemist on meeldetuletusega, et inimese dokument aegub kuu aja pärast ja on aeg hakata taotlema uut dokumenti, on kindlasti tegemist kaalutletud ja vajaliku teenusega. Praktikas unustatakse tihti uut dokumenti õigeaegselt taotleda. Seletuskirja täiendatud.

5. Eelnõu § 1 punktid 9–12 reguleerivad haldusorgani õigust edastada isikuandmeid järelevalvemenetluses ning **eelnõu § 1 punktid 51 ja 52** RAB-i õigus töödelda e-residendi andmeid. Muudatusega soovitakse anda PPA-le õigus edastada ja RAB-ile õigus riiklikus järelevalves töödelda e-residendi digi-ID väljaandmise menetluses kogutud andmeid ning e-residendi digi-ID kasutamise andmeid, et RAB saaks täita rahapesu ja terrorismi rahastamise tõkestamise seaduse (RahaPTS) § 54 lg 1 punktides 1 ja 2 sätestatud ülesandeid. E-residendi digi-ID kasutamise logiandmetest on RAB-il võimalik kontrollida oma seadusjärgsete ülesannete täitmisel näiteks seda, kas e-residendi digi-ID-d on kasutatud riskiriigis (seletuskiri lk 10-11). Eelnõus ja seletuskirjas ei ole eristatud erinevate ülesannete täitmiseks vajalikke andmeid ega selgitatud, miks näiteks on vajalik isikuandmete kasutamine RahaPTS § 54 lõike 1 punktis 2 sätestatud strateegilise analüüsi tegemiseks.[3] Riikliku järelevalve osas on digi-ID kasutamise üle järelevalve tegemiseks edastatavate andmetena seletuskirjas viidatud digi-ID logiandmetele, et tuvastada, kas digi-ID-d on kasutatud riskiriigis. Selgusetu on, millisest allikast pärit ja millisel viisil logiandmeid edastatakse ning millised tagajärjed kaasnevad isikule muuhulgas riskiriigis digi-ID kasutamisel. Seetõttu ei ole võimalik hinnata andmetöötluse vajalikkust ja eesmärgipärasust. Palume nii eelnõu kui ka seletuskirja täiendada.	Osaliselt arvestatud **Eelnõu § 1 punktidega 9 ja 12** kavandatakse muuta ITDS § 9^2 lõikeid 8 ja 9. Sätted lisati ITDS-i isikuandmete kaitse seaduse rakendamise seadusega, mis jõustus 15.03.2019, eelnõu on leitav: 778 SE. Eelnõu seletuskirja kohaselt on selle koostanud Justiitsministeerium. Eelnõuga muudetakse 126 seadust ja seletuskirjas on välja toodud seaduse eesmärk: *Seaduse eesmärk on tagada isikuandmete kaitse üldmääruse ja õiguskaitsevaldkonna direktiivi rakendumine eri õigusvaldkondades. Isikuandmete kaitse seadus koosmõjus isikuandmete kaitse üldmäärusega on liialt üldine, et detailsemal tasemel tagada seadusliku aluse põhimõtte korrektset järgimist. Seetõttu on vajalik avaliku võimu poolseks töötlemiseks ette näha täpsemad alused, eesmärgid ja isikuandmete töötlemise ulatus.* Kooskõlastamisel olnud isikut tõendavate dokumentide seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõus kavandatavate muudatustega soovime täpsustada üksnes sõnastust e-residendi digi-ID järelevalve ja sertifikaatide peatamise ning uuendamise osas, andmetöötluse põhimõtete muutmist eelnõuga ei kavandata. Eeltoodust tulenevalt leiame, et andmete töötlemise osas oleks tulnud põhiseaduspärasuse analüüs teha siis, kui töötati välja andmetöötluse regulatsioon. Leiame, et praegu, kui sätete jõustumisest on möödunud üle viie aasta, ei ole kõnesolevate sätete osas põhiseaduspärasuse analüüsi tegemine hädavajalik. Kui peate seda siiski vajalikuks, tuleks selle tegemiseks pöörduda eelnõu autorite poole. **Eelnõu § 1 punktidega 51 ja 52** täiendatakse ITDS § 20^8 ja sätestatakse õigusselguse huvides RAB-i kui järelevalveasutuse pädevus lisaks RahaPTS-le ka ITDS-s. RahaPTS § 53 lõike 1 kohaselt on RAB Rahandusministeeriumi valitsemisalasse kuuluv valitsusasutus, mis teeb riiklikku järelevalvet ning kohaldab riiklikku

[3] Strateegiline analüüs ei eelda isikustatud andmete kasutamist. The Financial Action Task Force (FATF) metoodika p 29.4 (b): https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.coredownload.pdf

	sundi käesolevas seaduses ette nähtud alustel ja ulatuses autonoomselt. RAB-i täpsed ülesanded on sätestatud RahaPTS §-s 54. RahaPTS § 60 lõikest 4 ja 5^1 tulenevalt on RAB-il õigus teha järelevalvet e-residendi digi-ID kasutamise üle. Kuigi järelevalve pädevus tuleb RAB-ile RahaPTS-st, siis kavandatava ITDS § 20^8 täiendusega tuuakse RAB järelevalve asutusena eraldi välja sarnaselt PPA-le, KAPO-le ning MTA-le. Praegu jääb selgusetuks, miks ei ole RAB-i ITDS-i § 20^8 järelevalveasutuste loetelus, sest see on erisäte, mis reguleerib järelevalve teostamist üksnes e-residendi digi-ID kasutamise üle ja RahaPTS § 53 lõike 1 kohaselt on RAB-i ülesannete täitmine RahaPTS-s sätestatud alustel ja ulatuses riiklik järelevalve. Kuna andmetöötluse põhimõtteid eelnõuga ei muudeta. Eeltoodust tulenevalt leiame, et andmete töötlemise osas oleks tulnud põhiseaduspärasuse analüüs teha siis, kui töötati välja RAB-i andmetöötluse regulatsioon. RahaPTS jõustus 27.11.2017. Leiame, et praegu, kui sätete jõustumisest on möödunud üle kuue aasta, ei ole kõnesolevate sätete osas põhiseaduspärasuse analüüsi tegemine hädavajalik. Kui peate seda siiski vajalikuks, tuleks selle tegemiseks pöörduda Rahandusministeeriumi poole, kes on RahaPTS eelnõu autor ja oskab RAB-i ülesannete kirjeldamisel ning RAB-i tegevuse põhjendamisel kindlasti paremini kaasa rääkida. E-residendi digi-ID kasutamise logiandmeid on RAB-il võimalik küsida vajaduspõhiselt ametliku päringuga PPA lepinguliselt partnerilt, kes osutab e-identimise ja e-tehinguteks vajalikku sertifitseerimisteenust ja kvalifitseeritud usaldusteenust. Vastus päringule edastatakse krüpteeritult. Logiandmete kasutamine järelevalvemenetluses aitab kaasa rahapesu tõkestamise ja terrorismi rahastamise kahtlustuste tõendamisele. Kuna strateegiliseks analüüsiks ei ole vaja isikustatud andmeid töödelda, on eelnõust välja jäetud viide RahaPTS § 54 lõike 1 punktile 2.
6. Eelnõu § 1 punktiga 14 asendatakse ITDS § 11^3 lõikes 3 ja § 12^2 lõikes 2 sõna	Arvestatud

„vanglatöötaja“ sõnaga „vanglaametnik“. Samuti kasutatakse „vanglaametnik“ ka eelnõu § 1 punktis 17, 18 ja 20. Kuigi seletuskirjas (lk 24) on märgitud, et tegemist on tehnilise muudatusega, toob antud muudatus kaasa olukorra, kus taotluse saab esitada ja dokumendi väljastada ainult vanglaametnikule. Vangistusseaduse (VangS) § 111 kohaselt on vanglaametnik vanglas teenistuses olev ametnik, kelle ülesanne on kinnipeetava ja vahistatu kinnipidamine ja järelevalve, julgeoleku tagamine vanglas ning kohtueelse menetluse või kohtuvälise menetluse toimetamine vanglas toimepandud süütegudes, samuti sellealase tegevuse juhtimine. Peamiselt tegelevad dokumentidega aga välismaalaste koordinaatorid ja sotsiaaltöötajad, kes ei ole vanglaametnikud, vaid ametnikud, kes vanglas töötavad. Seega on kavandatud muudatus liigselt piirav ega täidaks eesmärki, mistõttu me seda muudatust esitatud kujul ei toeta. Näiteks välismaalaste seaduses on sarnasel juhul kasutatud „selleks volitatud kinnipidamisasutuse ametnik või töötaja“.	Eelnõu muudetud ja kasutatud väljendit „selleks volitatud kinnipidamisasutuse ametnik või töötaja.“
7. Eelnõu 1 punkt 17 reguleerib vanglas kinni peetava isiku dokumendi väljaandmise taotlust. Seletuskirjas (lk 24) on välja toodud, et dokumendi taotlus on põhjendatud ka kinnipeetava vanglast vabanemise korral. Kui kinnipeetaval ei ole kehtivat dokumenti, võimaldatakse tal paremaks taasühiskonnastumiseks taotleda kohustuslikku dokumenti ja toimetatakse see talle tema vabanemise ajaks kätte. Juhime tähelepanu, et kinnipeetavatel on võimalik taotleda ennetähtaegset vabastamist ning kohus võib (sh korduvalt) otsustada kinnipeetavat mitte ennetähtaegselt vabastada. See tähendab, et kuna vangla ei tea, kas ja millisel korral kohus kinnipeetava ennetähtaegselt vabastada otsustab, siis tuleb vanglal esitada kinnipeetava dokumenditaotlus esimese ennetähtaegse vabastamise menetluse käigus. Seega selleks, et kinnipeetaval oleks vabanemise hetkeks kindlasti dokument olemas, võidakse seda taotleda ajal, mil kinnipeetava (ennetähtaegne) vabanemine ei ole veel kindel. Palume seda asjaolu ka seletuskirjas täpsustada.	Arvestatud Seletuskirjas täpsustatud, et põhjendatud dokumendi vajaduseks loetakse ka kinnipeetava ennetähtaegset vabastamist.
8. Eelnõu 1 punktiga 18 nähakse ette vanglas kinni peetava isiku biomeetriliste andmete	Mitte arvestatud

võtmine. Juhime tähelepanu, et VangS § 86 lõige 7 nimetab juhud, kui andmeid võtta ei tule. Palume vähemalt seletuskirjas VangS § 86 lõikes 7 sätestatule viidata.	ITDS-i muudatusega ei reguleerita vanglasse karistust kandma saabunud isiku (VangS § 18 lg 1) ja arestialuse (VangS § 86 lg 6) daktüloskopeerimist. Muudatus kohaldub kitsalt dokumendimenetlusele ehk vanglas kinni peetava isiku sõrmejälgede võtmisele isikut tõendava dokumendi taotlemise korral. ITDS § 11^5 lõikes 4^1 on ka selge viide sama paragrahvi lõikele 4, mis välistab dokumendimenetluses biomeetriliste andmete võtmise reeglite kohaldamise muudele vanglas läbiviidavatele menetlustele. Seetõttu puudub koosmõju VangS-s sätestatud daktüloskopeerimise nõuetega ja puudub vajadus viidata VangS § 86 lõikes 7 välja toodud erisustele.
9. Eelnõu § 1 punkt 33 sätestab e-residendile kohustuse hoida oma kontaktandmeid ajakohasena. Juhime tähelepanu, et isiku kohustamisel riigile oma andmete andmiseks ja pidevaks ajakohastamiseks peab olema selge ja põhjendatud avaliku huvi eesmärk. Seletuskirjas (lk 10) on toodud, et säte on vajalik selleks, et PPA saaks vajadusel saata e-residendile tema dokumendi kohta teavitusi. Eelduslikult peaks olema isikul endal huvi neid teavitusi saada, mistõttu avaliku huvi eesmärk teavituste saatmiseks on antud juhul küsitav. Lisaks on olemuselt tegemist deklaratiivse sättega, millel puuduvad õiguslikud tagajärjed. Eeltoodust tulenevalt palume säte eelnõust välja jätta.	<u>Mitte arvestatud</u> Eesti e-residendiks saamine on välismaalase privileeg, mitte õigus. ITDS § 20^6 kohaselt on e-residentsuse saamisel aluseks 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, võib Eesti e-resident asuda ükskõik kus. Kui Eesti annab välismaalasele juurdepääsu oma e-teenustele, siis avalik huvi seisneb selles, et riik võiks teada, kes, kus ja milleks riigi teenuseid kasutab. Lisaks võib avalik huvi esineda avaliku korra ja julgeoleku kaalutlustel, kui isik paneb toime teo, mis on e-residendi digi-ID kehtetuks tunnistamise aluseks. Järelevalvemenetluses soovitakse e-residendile tagada ärakuulamisõigus, kuid sageli on e-residendi e-posti aadress selleks ajaks muutunud ja teda ei ole võimalik e-residendi digi-ID kehtetuks tunnistamisele eelnevalt ära kuulata. Aktuaalseks võib kontaktandmete küsimus muutuda ka siis, kui e-residendi digi-ID kehtetuks tunnistatakse ja välismaalasele on vaja kätte toimetada e-residendi digi-ID kehtetuks tunnistamise otsus. Seletuskirja täiendatud selgitustega.
10. Eelnõu § 1 punkt 35, § 2 punkt 3 ning § 9 punktid 5 ja 10 sedastavad andmekogude andmekoosseisud. Seletuskirja kohaselt on tegemist kehtivates andmekogude põhimäärustes sätestatud andmekoosseisude toomisega seaduse tasandile. Toetame muudatuse eesmärki, kuid kuna andmekoosseisud võivad seaduse tasandil olla	<u>Arvestatud</u> Seletuskirja täiendatud. Andmekoosseisude muudatused võrreldes kehtiva regulatsiooniga välja toodud ja lisatud põhjendused.

üldisemad ning neid võib põhimääruses täpsustada, tuleb seletuskirjas selguse eesmärgil arusaadavalt lahti kirjutada, millised põhimääruse andmekoosseisus toodud andmed kuuluvad seaduse tasandil reguleeritavatesse andmekategooriatesse ning juhul, kui andmekoosseise on hetkel kehtivaga võrreldes laiendatud, tuua see koos põhjendusega seletuskirjas välja. Ühe näitena võimalikust andmekoosseisu laiendamisest on eelnõu § 9 punktis 10 sätestatud Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu andmekoosseisu punkti 16, mis erineb põhimääruse §-s 8 sätestatust, mistõttu tekib küsimus ka andmekoosseisu kooskõlast andmekogu pidamise eesmärgiga.	
11. Eelnõu § 1 punktides 38 ja 40, § 2 punktides 6 ja 8, § 3 punktis 2, § 4 punktis 2, § 7 punktis 2, § 9 punktides 7 ja 12, § 10 punktis 2 ning rakendusaktide kavandites 1 ja 2 sätestatakse andmekogu andmete säilitamise tähtajad. Andmete säilitamise tähtaegade kehtestamist ei ole seletuskirjas ammendavalt põhjendatud. Eriti hoolikalt vajavad kaalumist pikad säilitustähtajad, nt tähtajatu ja 75 aastat, kuid põhjendada tuleb kõiki kehtestatavaid tähtaegu. Palume seletuskirja täiendada säilitustähtaegade võrdlusega, kust nähtub säilitustähtaegade muutmine võrreldes kehtiva regulatsiooniga (näiteks sissesõidukeeldude riikliku registri põhimääruse § 17 lõike 1 kohaselt säilitatakse alalise sissesõidukeelu andmeid 50 aastat, kuid eelnõu § 9 punktis 7 sätestatakse nendele andmetele alaline säilitusaeg) ja muudatuse põhjendus.	Osaliselt arvestatud Andmekogu andmete säilitustähtaegade sätestamisel tuleb arvestada, et omavahel peavad olema kooskõlas andmekogu põhimääruses sätestatud säilitustähtaeg, andmekogu ABIS põhimääruses sätestatud biomeetriliste andmete säilitustähtaeg ja põhimäärustest kõnesoleva eelnõuga seaduse tasemel sätestatavad andmekogu ABIS ja iga andmekogu andmete maksimaalsed säilitustähtajad. Andmekogus ABIS säilitatakse biomeetrilisi andmeid ja kui nt andmekogu ABIS andmete säilitustähtaeg on pikem kui selle andmekogu andmete säilitustähtaeg, kust andmekogusse ABIS andmed saadetakse, siis võivad biomeetrilised andmed küll andmekogus ABIS alles olla, kuid neid ei ole enam võimalik konkreetse isikuga siduda ehk andmekogu ABIS andmete pikemal säilitamisel puudub mõte, selline andmete säilitamine koormab digivõrku ja kasutab muid ressursse ebaotstarbekalt. Seetõttu on mõnel juhul eelnõuga seadusesse kavandatavad andmete säilitustähtajad võrreldes konkreetse andmekogu põhimäärusega muudetud. Andmekogu põhimäärused viiakse seadusega kooskõlla pärast selle vastuvõtmist. Kuna seni on andmekogu andmete säilitustähtajad kehtestatud andmekogu põhimääruses, siis ei ole eelnõuga kavandatava regulatsiooni tarbeks uusi tähtaegu välja mõeldud. Andmekogu ABIS põhimäärus on kehtestatud 23. detsembri 2021 Vabariigi Valitsuse määrusega, seega andmekogu andmete

	säilitustähtaegade täpsemad põhjendused on leitavad nimetatud määruse seletuskirjast. **ITDAK (eelnõu § 1 p 38 ja 40)** – ITDS § 15^2 lõige 5^2: eelnõuga kavandatakse, et andmekogu andmeid võib säilitada alaliselt. Andmetele võib kehtestada lühema säilitustähtaja andmekogu põhimääruses. Andmekogu ABIS põhimääruse § 38 kohaselt säilitatakse andmekogusse kantud andmeid andmekogus **aktiivselt 15 aastat**, peale mida kantakse andmed eraldi andmekogu arhiiviosasse, kus andmeid säilitatakse **50 aastat**. ITDAK[4] põhimääruse § 18 kohaselt säilitab vastutav töötleja andmekogukaarte 50 aastat vastavalt arhiiviseaduses sätestatule. ITDAK-it ei peeta üksnes dokumenditaotluste menetlemiseks. ITDAKi laiem/peamine eesmärk on avaliku korra ja riigi julgeoleku tagamine ja selleks peab andmekogu võimaldama tuvastada riikliku identiteedi saanuid. ITDAK on üks riigi peamine andmekogu, mille andmetele tuginevad nii riigiasutused, notarid ja muud vabade kutsete esindajad kui ka erasektor. Seega on ITDAK-i andmeid vaja kasutada läbi kogu inimese elu. Kuna inimeste keskmine eluiga aja jooksul pikeneb, ei ole andmekogu ABIS põhimääruses sätestatud tähtaeg (maksimaalselt 65 aastat) enam piisav ja andmekogu ABIS arhiiviandmete säilitamist pikendatakse 60 aastale, so kokku hoitakse dokumendimenetlusega seotud andmeid 75 aastat. Teatud juhtudel on vaja inimese andmeid ka pärast tema surma, näiteks põlvnemis- ja kodakondsusküsimustes või identiteedikonflikti lahendamisel. PS § 8 esimese lõigu kohaselt on igal lapsel, kelle vanematest üks on Eesti kodanik, õigus Eesti kodakondsusele sünnilt. Sama paragrahvi kolmanda lõigu kohaselt ei tohi kelleltki võtta sünniga omandatud Eesti kodakondsust. Seega võib Eesti kodakondsusesse kuulumise tõendamise vajadus tekkida ka mitmeid põlvi hiljem ja kuna Eesti kodakondsusesse kuulumine sünnilt tehakse kindlaks just dokumendimenetluses, hoitakse vastavaid andmeid ITDAK-is. Seetõttu on vaja sätestada seaduses ITDAK-i andmete säilitamine alaliselt. Muude ITDAK-i andmete säilitamise tähtajad

[4] Isikut tõendavate dokumentide andmekogu pidamise põhimäärus

	on lühemad ja need kehtestatakse ITDAK-i põhimääruses. Säilitustähtaja muutmise vajadust on selgitatud eelnõu seletuskirja punktis 3.4.1. **Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu (eelnõu § 1 p 6 ja 8)** – ITDS § 15^2 lõige 5^2: eelnõuga kavandatakse, et andmekogu andmeid võib säilitada alaliselt. Andmekogu põhimääruse § 20 lõike 1 kohaselt lähtutakse andmete säilitamisel, arhiveerimisel ja hävitamisel arhiiviseadusest ning selle alusel kehtestatud õigusaktidest ja vastutava töötleja kehtestatud korrast. Sama paragrahvi lõike 2 kohaselt andmekogusse ABIS kantud foto või näokujutis, mis on kantud andmekogu infotehnoloogilisse andmekogusse, kustutatakse viivitamata pärast isiku tuvastamise või isikusamasuse kontrollimise võrdlusuuringu tegemist. Andmekogu ABIS põhimääruse § 20 lõike 1 kohaselt säilitatakse andmekogusse kantud andmeid aktiivselt 20 aastat, peale mida kantakse andmed eraldi andmekogu arhiiviosasse, kus andmeid säilitatakse alaliselt. Seega tuleb selle andmekogu maksimaalne säilitustähtaeg kehtivast andmekogu ABIS põhimäärusest ja seda võrreldes kehtiva regulatsiooniga ei muudeta. **Konsulaarseaduses (eelnõu § 3 p 2)** – KonS § 12^1 lõige 7^1: eelnõuga kavandatakse, et andmekogu ABIS andmeid säilitatakse neli kuud isikut tõendava dokumendi taotluse Politsei- ja Piirivalveametile edastamisest arvates. Andmekogu ABIS põhimääruse § 42 kohaselt säilitatakse andmekogusse kantud andmeid neli kuud arvates taotluse edastamisest Politsei- ja Piirivalveametile. Seega tuleb andmekogu maksimaalne säilitustähtaeg kehtivast andmekogu ABIS põhimäärusest ja seda võrreldes kehtiva regulatsiooniga ei muudeta. **Kriminaalmenetluse seadustikus (eelnõu § 4 p 2**) – KrMS § 109^2 lõige 5^1: eelnõuga kavandatakse, et andmekogu ABIS andmeid säilitatakse kuni 75 aastat andmekogusse ABIS kandmisest arvates. Andmetele võib kehtestada

	lühema säilitustähtaja andmekogu ABIS põhimääruses. Andmekogu ABIS põhimääruse § 41 kohaselt säilitatakse andmekogusse kantud andmeid: 1) Daktüloskopeerimisel ja näokujutise võtmisel saadud biomeetrilisi andmeid säilitatakse **40 aastat** kandmisest arvates, kui seaduses ei ole sätestatud teisiti. Pärast nimetatud tähtaja möödumist kantakse andmed eraldi andmekogu arhiiviosasse; 2) arhiiviosas säilitatakse daktüloskopeerimisel ja näokujutise võtmisel saadud biomeetrilisi andmeid **35 aastat**, mille järel need kustutatakse; 3) sündmuskohalt kogutud või muult objektilt võetud naha papillaarkurrustiku jälgi ja näokujutist säilitatakse andmekogus kuni isikuga seostamiseni, mille järel isikuga seostatud jälg suletakse, või isikuga seostamata jäämise korral **75 aastat**, mille järel need kustutatakse. Seega tuleb andmekogu maksimaalne säilitustähtaeg kehtivast andmekogu ABIS põhimäärusest (mis omakorda on seotud kohtuekspertiisiseaduse §-s 21 sätestatud säilitustähtaegadega) ja seda võrreldes kehtiva regulatsiooniga ei muudeta. **Vangistusseaduses (eelnõu § 7 p 2**) – VangS § 5^5 lõige 5^1: eelnõuga kavandatakse, et andmekogu ABIS andmeid säilitatakse kuni 75 aastat andmekogusse ABIS kandmisest arvates. Andmetele võib kehtestada lühema säilitustähtaja andmekogu ABIS põhimääruses. Andmekogu ABIS põhimääruse § 41 kohaselt säilitatakse andmekogusse kantud andmeid: 1) Daktüloskopeerimisel ja näokujutise võtmisel saadud biomeetrilisi andmeid säilitatakse 40 aastat kandmisest arvates, kui seaduses ei ole sätestatud teisiti. Pärast nimetatud tähtaja möödumist kantakse andmed eraldi andmekogu arhiiviosasse; 2) arhiiviosas säilitatakse daktüloskopeerimisel ja näokujutise võtmisel saadud biomeetrilisi andmeid 35 aastat, mille järel need kustutatakse; 3) sündmuskohalt kogutud või muult objektilt võetud naha papillaarkurrustiku jälgi ja näokujutist säilitatakse andmekogus kuni isikuga seostamiseni, mille järel isikuga

	seostatud jälg suletakse, või isikuga seostamata jäämise korral 75 aastat, mille järel need kustutatakse. Seega tuleb andmekogu maksimaalne säilitustähtaeg kehtivast andmekogu ABIS põhimäärusest (mis omakorda on seotud kohtuekspertiisiseaduse §-s 21 sätestatud säilitustähtaegadega) ja seda võrreldes kehtiva regulatsiooniga ei muudeta. **Väärteomenetluse seadustikus (eelnõu § 10 p 2)** – VtmS § 31^6 lõige 5^1: eelnõuga kavandatakse, et andmekogu ABIS andmeid säilitatakse kuni 75 aastat andmekogusse ABIS kandmisest arvates. Andmetele võib kehtestada lühema säilitustähtaja andmekogu ABIS põhimääruses. Andmekogu ABIS põhimääruse § 41 kohaselt säilitatakse andmekogusse kantud andmeid: 1) Daktüloskopeerimisel ja näokujutise võtmisel saadud biomeetrilisi andmeid säilitatakse 40 aastat kandmisest arvates, kui seaduses ei ole sätestatud teisiti. Pärast nimetatud tähtaja möödumist kantakse andmed eraldi andmekogu arhiiviosasse; 2) arhiiviosas säilitatakse daktüloskopeerimisel ja näokujutise võtmisel saadud biomeetrilisi andmeid 35 aastat, mille järel need kustutatakse; 3) sündmuskohalt kogutud või muult objektilt võetud naha papillaarkurrustiku jälgi ja näokujutist säilitatakse andmekogus kuni isikuga seostamiseni, mille järel isikuga seostatud jälg suletakse, või isikuga seostamata jäämise korral 75 aastat, mille järel need kustutatakse. Seega tuleb andmekogu maksimaalne säilitustähtaeg kehtivast andmekogu ABIS põhimäärusest (mis omakorda on seotud kohtuekspertiisiseaduse §-s 21 sätestatud säilitustähtaegadega) ja seda võrreldes kehtiva regulatsiooniga ei muudeta. **Sisesõidukeeldude riiklik register (eelnõu § 9 p 7)** – VSS § 33^2 lõige 5^2: eelnõuga kavandatakse, et registri andmeid säilitatakse: 1) alalise sissesõidukeelu andmed – alaliselt; 2) tähtajalise sissesõidukeelu andmed – aktiivselt kuni kümme aastat pärast tähtajalise

	sissesõidukeelu lõppemist ja arhiiviosas kuni 40 aastat. Tähtajalise sissesõidukeelu andmetele võib kehtestada lühema säilitustähtaja registri põhimääruses. Andmekogu põhimääruse § 17 lõike 1 kohaselt säilitatakse andmekogu andmeid alalise sissesõidukeelu puhul 50 aastat ja lõike 2 kohaselt tähtajalise sissesõidukeelu puhul aktiivselt kümme aastat pärast tähtajalise sissesõidukeelu tähtaja lõppemist, pärast mida kantakse andmed andmekogu arhiiviosasse, kus neid säilitatakse 40 aastat. Andmekogu ABIS põhimääruse § 47 lõike 1 kohaselt säilitatakse andmekogusse kantud alalise sissesõidukeelu andmeid alaliselt. Lõike 2 kohaselt säilitatakse andmekogusse kantud tähtajalise sissesõidukeelu andmeid aktiivselt kümme aastat pärast tähtajalise sissesõidukeelu tähtaja lõppemist, peale mida kantakse andmed eraldi andmekogu arhiiviosasse, kus andmeid säilitatakse alaliselt. Seega kehtib kooskõlastusele esitatud eelnõukohane andmekogu maksimaalne säilitustähtaeg juba praegu andmekogu ABIS põhimääruses. Pärast kooskõlastusringi on eelnõus säilitustähtaegu korrigeeritud ja pakutud välja säilitustähtajad järgmiselt: 1) alalise sissesõidukeelu andmed – 75 aastat alates isiku sünnist; 2) tähtajalise sissesõidukeelu andmed – aktiivselt kuni kümme aastat pärast tähtajalise sissesõidukeelu lõppemist ja arhiiviosas kuni 40 aastat. Eelnõuga kavandatakse lühendada sissesõidukeelu säilitustähtaegu. Sissesõidukeeld kehtestatakse välismaalasele ja üle 75 aasta ei ole vaja selle andmeid säilitada, sest välismaalasele kehtestatud sissesõidukeeld ei mõjuta tema järeltulija võimalusi Eestisse saabuda. Arvestades inimese keskmist eluiga ning asjaolu, et VSS § 30 punkti 1 kohaselt ei saa kohaldada sissesõidukeeldu alla 13-aastasele isikule, oleks sissesõidukeelu andmete säilitamine alaliselt põhjendamatu ja koormaks

	digivõrku, mistõttu nähakse eelnõus ette, et sissesõidukeelu andmeid säilitatakse 75 aastat. **Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu (eelnõu § 9 p 12)** – VSS § 33^{14} lõige 7^{1}: eelnõuga kavandatakse, et andmekogu andmeid säilitatakse aktiivselt kuni kümme aastat välismaalase lahkumiskohustuse täitmise päevast arvates ja arhiiviosas kuni 40 aastat. Andmetele võib sätestada lühema säilitustähtaja andmekogu põhimääruses. Andmekogu ABIS põhimääruse § 48 lõike 1 kohaselt säilitatakse andmekogusse kantud andmeid andmekogus aktiivselt kümme aastat välismaalase lahkumiskohustuse täitmise päevast arvates, peale mida kantakse andmed eraldi andmekogu arhiiviosasse, kus andmeid säilitatakse alaliselt. Lõike 2 kohaselt, kui välismaalase lahkumiskohustus tühistatakse või tunnistatakse kehtetuks, säilitatakse andmeid andmekogus aktiivselt kümme aastat välismaalase lahkumiskohustuse tühistamise või kehtetuks tunnistamise päevast arvates. Seega tuleb selle andmekogu andmete alaline säilitustähtaeg kehtivast andmekogu põhimäärusest ja andmekogu ABIS põhimäärusest. Eelnõuga kavandatakse lühendada sissesõidukeelu andmete säilitustähtaegu. Sissesõidukeeld kehtestatakse välismaalasele ja kauem kui 50 aastat arvates lahkumiskohustuse täitmisest, ei ole vaja selle andmeid säilitada, sest välismaalase täidetud lahkumiskohustus ei mõjuta 50 aastat hiljem tema võimalusi Eestisse saabuda. Seega oleks välismaalase lahkumiskohustuse andmete säilitamine alaliselt põhjendamatu ja koormaks digivõrku[5].

[5] Andmekogude säilitustähtaja regulatsiooni sätestamisel seaduse tasemel on näiteks võetud tervise infosüsteemi regulatsioon. Andmekogu andmekoosseis ja andmete säilitustähtajad on lisatud tervishoiuteenuste korraldamise seadusesse isikuandmete kaitse seaduse rakendamise seaduse eelnõuga, mille seletuskirjas on lk 111 § 106 punkti 23 selgitus, mille kohaselt: *täiendatakse TTKS § 59[1] lõigetega 4–6, sätestades kokkuvõtva andmekoosseisu ja andmete säilitamise tähtajad ka tervise infosüsteemi puhul seaduses. See hõlmab endas suurel hulgal eriliiki isikuandmeid ning ka siin on oluline sätestada andmetöötlus kui isikustatud andmete säilitamine seaduses. Ka tervise infosüsteemi puhul on lähtutud kehtivast korrast. Suur osa andmetest säilitatakse tähtajatult, tehes erisuse vaid teatud andmete korral. Kuna kiirabi töö põhineb e-lahendustel ja andmeid sisestatakse elektrooniliselt, on säilitamise tähtaeg sarnane §-s 42 sätestatuga. Logisid säilitatakse 30 aastat, et tagada ka siin erinevate nõuete esitamise võimalus. Tegemist on olulise andmekoguga, mis hõlmab endas olulisel hulgal teenuse osutamisega seotud materjali. Tõsi, tervise infosüsteemi kogutakse vaid teatud andmeid, kuid see on oluline andmete kokkuvõttev hulk, mis demonstreerib raviprotsessist olulisemat. Lõige 6 muudatus on vajalik, et infosüsteemi andmed oleksid seotud õige isikuga.* Analoogsed selgitused säilitustähtaegade kohta on antud ka

12. Eelnõu § 1 punkt 41 kohaselt juhul, kui dokument ei vasta nõuetele dokumendi väljaandja tõttu, antakse dokumendi kasutajale välja sama kehtivusajaga uus dokument ning PPA võib võtta uue dokumendi väljaandmiseks selle kasutaja biomeetrilised andmed. Juhime tähelepanu, et kuna biomeetriliste andmete töötlemise puhul on tegemist eriliigiliste andmete töötlusega, siis kehtivad sellisele andmetöötlusele rangemad nõuded. Vajalik on põhjalikult kaaluda, millistel juhtudel on vältimatult vajalik isiku biomeetriliste andmete uuesti kogumine. Lubatud juhud tuleb seaduses täpselt sätestada.	Arvestatud ITDS § 16 täiendatakse teise lõikega, mille kohaselt võib PPA võtta uue dokumendi väljaandmiseks selle kasutaja biomeetrilised andmed, kui dokument ei vasta ITDS § 16 lõike 1 punktides 3 ja 4 sätestatud nõuetele dokumendi väljaandja tõttu ja dokumendi kasutajale tuleb seetõttu välja anda sama kehtivusajaga uus dokument. Biomeetriliste andmete uuesti kogumine on vältimatult vajalik juhul kui varasemalt võetud sõrmejäljed ei ole koostalitusvõimelises formaadis, mistõttu neid ei ole võimalik töödelda. Lisaks võetakse uued sõrmejäljed juhul, kui inimene seda ise soovib, st dokument vahetatakse küll välja, kuid see on peatselt aegumas ning uute sõrmejälgede võtmine annab inimesele võimaluse taotleda uus dokument iseteeninduses ilma isiklikult kohale minemata, sest sõrmejäljed on kehtivad. ITDS § 9^2 lõigete 1 ja 7 kohaselt võib isikut tõendavate dokumentide seaduses sätestatud menetluste puhul isikult võtta biomeetrilisi andmeid ja neid töödelda. Muudatusega luuakse õigusselguse huvides alus biomeetriliste andmete võtmiseks dokumendi väljavahetamisel, kui see on vältimatult vajalik või kui dokumendi kasutaja seda ise soovib. ITDS § 11^6 lõike 3 kohaselt dokumendi taotluse esitamisel taotleja daktüloskopeeritakse. See kehtib kõigi dokumendi taotlejate kohta, välja arvatud erandid, nt alaealised ja isikud, keda terviseseisund ei võimalda daktüloskopeerida. Dokumendi taotleja daktüloskopeerimise nõue (ITDS § 9^2 ja § 11^6) jõustus 28.08.2006. aastal. Praegu, st 18 aastat pärast sätte jõustumist, oleks veider hakata hindama selle põhiseaduspärasust, kui keegi dokumendi taotleja daktüloskopeerimist seni vaidlustanud ei ole.
13. Eelnõu § 1 punktiga 43 luuakse võimalus isikusamasuse kontrollimiseks mRiigi kaudu. Seletuskirjas (lk 21) tuuakse välja, et isikusamasuse kontrollimiseks teeb teenuseosutaja dokumendi ruutkoodi, triipkoodi	Selgitus Tegemist on täiendava vabatahtliku võimalusega nii inimestele kui teenuseosutajatele, mille kasutamine eeldab, et mitmed eeltingimused oleks täidetud:

isikut tõendavate dokumentide seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskirjas.

või lähiväljaside abil kontrollpäringu X-tee kaudu riiklikkusse andmekogusse, mis on isikutunnistuse ja passi puhul ITDAK. Kavandatud muudatuse osas jääb selgusetuks, kas isikul on õigus nõuda, et ta peab saama oma isikusamasust tõendada mRiigi lahendusega või sõltub see siiski teenuseosutaja soovist ja võimalustest, kuna kontrollpäringu tegemine eeldab ka tehnilisi vahendeid. Palume seletuskirjas selgitada, sh mõju vaatest, kuidas täpsemalt rakendamine mõeldud on.	1) isikul on kehtiv dokument; 2) teenuseosutajal on tehniline võimekus ja soov kontrollpäringut teha ja selle võimaluse kastutamist isikutele pakkuda. Seletuskirja täiendatud.
14. Eelnõu § 5 punktiga 1 täiendatakse PPVS-i §-ga 19^2, millega võimaldatakse piirikontrolli andmekogus biomeetriliste andmete töötlemine andmekogu ABIS kaudu. Seletuskirja (lk 32–33) kohaselt on tegemist täiendava võimalusega lisaks piirikontrolli andmekogule ja Schengeni infosüsteemile. Lisaks selgitatakse seletuskirjas, et võrdlust ABISega kasutatakse vaid piiratud juhtudel. Juhul, kui on vaja kehtestada täiendav võimalus andmete töötlemiseks, tuleb täpselt sätestada õiguslik alus ja eesmärk, millistel juhtudel on lisaks juba kasutatavatele andmekogudele lubatud biomeetriliste andmete töötlemine andmekogu ABIS kaudu.	Selgitus Kavandatud PPVS § 19^2 on kaks eesmärki: 1. PIKO[6] biomeetriliste andmete võrdlemine andmekogu ABIS kaudu; 2. PIKO biomeetriliste andmete võrdlemine andmekogu ABIS andmetega. Schengeni välispiiri riigina on Eestil EL kindlaksmääratud juhtudel kohustus teha piirikontrollis isikute biomeetriliste andmete päringuid ja vajaduse korral biomeetriliste andmete võrdlust. Nagu seletuskirjas selgitatud, käsitleme siin eeskätt Schengeni infosüsteemi päringuid, kus infosüsteemi sõrmejälgede automaatse tuvastamise süsteem (SIS AFIS) pakub SIS-ist PIKO-le päringutabamuse, mida võib olla vaja üle kontrollida. PIKO-l ei ole tehnilist võimekust biomeetrilisi andmeid omavahel võrrelda, seetõttu tuleb võrdlus teostada andmekogu ABIS võrdlusmootorit kasutades, sest muud tehnilist lahendust ei ole. Muudatuse teine eesmärk on lubada piirikontrollis hõivatud biomeetriliste andmete võrdlust andmekogu ABIS andmetega, sest andmekogu ABIS üheks eesmärgiks on võimaldada sinna kantud andmete kasutamist isiku tuvastamiseks või isikusamasuse kontrollimiseks juhul, kui see on seadusest tuleneva ülesande täitmiseks vajalik. Piirikontrolli tegemine välispiiril on riigi ülesanne, mille üheks osaks on piiriületaja isikusamasuse kontrollimine või vajadusel isiku tuvastamine. Praktikas andmekogu ABIS andmeid piirikontrollis kasutatud ei ole, kuid tulevikus ei saa sellist vajadust välistada. Seetõttu eelistame, et õiguslik alus

[6] Piirikontrolli andmekogu

	piirikontrollis andmekogu ABIS biomeetriliste andmete töötlemiseks oleks selge. Teise astme kontroll on Schengeni piirieeskirjade järgi lisakontroll, mida tehakse eemal kohast, kus kontrollitakse kõiki (teisi) isikuid ning teise astme kontrolli suunatakse üksnes need piiriületajad, kelle isikusamasuses on kahtlusi või kelle isikut ei ole võimalik tuvastada. Seega, kui tuleb täpselt sätestada õiguslik alus ja eesmärk, siis kõnesoleva muudatuse eesmärk on andmetöötlusele õigusliku aluse sätestamine. Biomeetrilisi andmeid töödeldakse aga piiriületaja isikusamasuse kontrollimise või tema isiku tuvastamise eesmärgil. Lisaks selgitame, et piirikontrolli teostatakse Schengeni piirieeskirjade kohaselt ning kuigi sellist põhimõtet nimetatud õigusaktis sõnaselgelt kirjas ei ole, tuleks biomeetriliste andmete alusel päringuid teha juhul, kui isikusamasust ei ole võimalik kindlaks teha või isikut ei ole võimalik tuvastada muul viisil (nt tähtnumbriliste andmete alusel, visuaalne kontroll). Eelnõu sätet täiendatud
Kaitseministeerium	
1. Andmete säilitamise tähtajad. Eelnõus määratakse mitmel juhul, et andmekogu põhimääruses võib kehtestada seaduses sätestatust lühema säilitustähtaja. Seetõttu on oluline, et pärast plaanitud muudatuste seadusena vastuvõtmist kooskõlastataks Kaitseministeeriumi valitsemisalaga ka asjassepuutuvad andmekogude põhimääruste eelnõud.	Arvestatud Enamik andmekogu andmete säilitustähtaegu on juba põhimäärustega, sh andmekogu ABIS põhimäärus, kehtestatud. Nende muutmisel esitatakse põhimääruse muutmise eelnõud kooskõlastamiseks Kaitseministeeriumile.
2. Sõjaväestatud organisatsioonides teenimise andmed. **2.1.** Eelnõu §-dega 1, 2 ja 9 muudetakse ITDS-i, KodS-i ja VSS-i ning tuuakse seaduse tasemele nende seaduste alusel peetavate andmekogude andmekoosseisud. Andmekogudes töödeldakse muu hulgas andmeid isiku seotuse kohta sõjaväeliselt korraldatud organisatsiooni või tegevusega. Nende andmete koosseis on sõnastatud eri õigusaktides erinevalt. Teeme ettepaneku asjassepuutuvaid sätteid hinnata ja vajadusel ühtlustada. ITDS § 15^2 lõike 3 punktis 17 sätestatakse, et isikut tõendavate dokumentide andmekogu	Arvestatud

(edaspidi *ITDAK*) pidamise eesmärgi täitmiseks võib töödelda dokumendi taotleja relvajõududes teenimise ja sõjaväelises operatsioonis osalemise andmeid. Seevastu KodS § 2^1 lõike 3 punktis 13 ja VSS § 33^{14} lõike 3 punktis 16 sätestatakse, et Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu ning Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu pidamise eesmärgi täitmiseks võib töödelda (...) menetluses kogutud isiku/välismaalase ajateenistuses, relvajõududes, kaadrisõjaväelasena või luure- või julgeolekuteenistuses teenimise ja töötamise andmeid, väljaspool Eestit sõjaväelises operatsioonis osalemise andmeid ning riiklikus või mitteriiklikus relvastatud organisatsioonis või üksuses teenimise andmeid.

Kui ITDAK-is töödeldakse üksnes andmeid isiku relvajõududes teenimise kohta, ei hõlma see mitmesuguseid muid sõjaväestatud organisatsioone, näiteks erasõjafirmasid või riigi eriteenistusi, mis võivad kaasaegses praktikas asendada riiklikke relvajõude. Arvestades, et ITDAK-i pidamise eesmärk on tagada loetletud esitatud andmete töötlemise kaudu avalik kord ja riigi julgeolek, tasub kaaluda, kas laiendada ITDS § 15^2 lõike 3 punktis 17 esitatud loetelu teiste seaduste eeskujul. Sel juhul tuleks punkt 17 sõnastada järgmiselt: „17) taotleja 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;“.

Andmete töötlemine andmekogus saab olla võimalik siis, kui nende kogumine asjakohase menetluse raames on õigusaktis ette nähtud. Seega on ITDS § 15^2 muutmise korral vaja muuta vastavalt ka siseministri 18.12.2015 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“ § 24[1] punkti 13, milles loetletakse e-residendi digitaalse isikutunnistuse taotluses esitatavad lisaandmed. Kui aga soovitakse neid andmeid koguda ka muudel juhtudel, kui välisriigi kodanik taotleb mis tahes isikut tõendava dokumenti, siis tuleb muuta sama määruse § 24 lõiget 5. **2.2.** Eelnevaga seoses teeme ettepaneku kaaluda ka välismaalaste seaduse (VMS) § 124 lõike 2 analoogset täiendamist. Selle lõike punktide 5 ja 6 järgi on tähtajalise elamisloa andmisest keeldumise aluseks muu hulgas see, kui välismaalane on teeninud kaadrisõjaväelasena välisriigi relvajõududes, sealt reservi arvatud või erru läinud või kui ta on välisriigi relvajõududes tegevteenistuses või lepingulises teenistuses. Kuigi riiklikus või mitteriiklikus relvastatud organisatsioonis või üksuses teenimine võib olla sisuliselt kaetud ka sama lõike punktidega 10–14, oleks otstarbekas see ka punktides 5 ja 6 selgemalt esile tuua. Ühtlasi võimaldaks VMS muudatus viia seaduse sõnastuse paremasse kooskõlla selle alusel antud määrustega. Alates 01.01.2023 kehtib siseministri 12.01.2017 määruse nr 7 „Tähtajalise elamisloa ja selle pikendamise ning pikaajalise elaniku elamisloa ja selle taastamise taotlemise kord ning legaalse sissetuleku määrad“ §-de 49–51 sõnastus, mille järgi tuleb elamisloa andmise, pikendamise ja taastamise taotlemisel esitada andmed ka selle kohta, kas taotleja teenib või on teeninud välisriigi kohustuslikus ajateenistuses, relvajõududes, kaadrisõjaväelasena või luure- või julgeolekuteenistuses, osaleb või on osalenud sõjaväelises operatsioonis väljaspool Eestit või töötab või on töötanud riiklikus või mitteriiklikus relvastatud organisatsioonis või üksuses.	Selgitus VMS muutmise ettepanek vaadatakse läbi välismaalaste seaduse muutmise seaduse ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu väljatöötamise käigus.
3. Mõiste isiku üldandmed. Eelnõus on läbivalt kasutusel mõiste isiku üldandmed, kuid selgusetuks jääb, milliseid isikuandmeid täpsemalt silmas peetakse. Kas eelnõu kohaselt on isikukood ja sünniaeg, ees- ja perekonnanimi või ka elukoht ja kontaktandmed isiku üldandmed? Näiteks saab oletada, et ITDAK-s töödeldavate taotleja ja kasutaja üldandmed	Arvestatud Isiku üldandmete selgitus lisatud seletuskirja punkti 4. Isiku üldandmeteks on nimi, isikukood (sünniaeg), sugu, kodakondsus, kontakt, sh aadress, emakeel.

sisaldavad sünniaega, kuid sissesõidukeeldude riikliku registrisse kantavad üldandmed ei sisalda, kuna kavandatava muudatusega nimetatakse VVS § 33 lõikes 3 registris töödeldavate andmete koosseisus punktis 1 välismaalase üldandmed ja punktis 2 välismaalase isanimi, sünniaeg ja –koht, rahvus ning usulise kuuluvuse andmed. Õigusselguse huvides palume vähemalt seletuskirjas nimetada üldandmete täpne andmekoosseis.	
4. Riskiriikide loetelu. Kaitseministeerium juhib tähelepanu asjaolule, et mitmed Eesti kaitsetööstusettevõtted omavad Saudi-Araabias juba lepinguid ning mitmetel on koostööläbirääkimised. Vaadates ka teiste NATO riikide tegutsemist Saudi-Araabias, palume tõsiselt kaaluda, kas on kohane ja mõistlik Saudi-Araabia hoidmine riskiriikide nimekirjas. Oleme seisukohal, et lõplik seisukoht tuleb kujundada Vabariigi Valitsuses eri ministeeriumite seisukohti ja rahvusvahelist praktikat arvestades.	Mitte arvestatud Saudi Araabia on sunniislami sünnihäll, islamifundamentalismi kese, usuäärmusluse koolituskeskus ja mittedemokraatlikku ideoloogiat toetav riik, kelle õigussüsteem on rajatud Koraanile ning Sunnale ja kus kriitikahääli monarhia suhtes vaigistatakse muu hulgas terrorismivastase seadustiku raames. Nende seisukohad ja tõekspidamised lähevad vastuollu demokraatliku riigi elukorralduspõhimõtetega, mis on rajatud inimõigustele ning nende kaitsele. 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. aastal. Saudi Araabia on kõrgema terrorismi rahastamise riskiga riik RABi avaldatud nimekirja[7] kohaselt. Eesti läbis 2022. aastal Euroopa Nõukogu rahapesu ja terrorismi rahastamise tõkestamise meetmeid hindava eksperdikomitee (Moneyvali) hindamise ning hindamise aruandes toodi e-residentsuse programmi ühe suurima riskina välja, et see võimaldab välismaalasel kasutada e-residentsust ebasoovitavaks ettevõtluseks ning varjata ettevõtluse tegelikku sisu ja eesmärki ning sellest kasu saajaid. See on eriti probleemne riskiriikide kodanike puhul. Moneyvali hindamise tulemusena võib hinnatav riik sattuda riskiriikide halli või musta nimekirja. 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

[7] kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid

	Moneyvali hindamisel tõsiseid pingutusi, et selgitada rahvusvahelistele ekspertidele e-residentsuse programmi olemust ja põhjendada, miks Eesti ei ole juba kehtestanud riskiriigi kodanikele piiranguid. Moneyvali hindamise ekspertide tõsiste kahtluste korral on Eesti riskiriikide nimekirja sattumise tõenäosus suur. Selle tulemusena viiksid Eestis tegutsevad rahvusvahelised ettevõtjad suure tõenäosusega oma ettevõtted mujale ning Eesti ettevõtjatel ja eraisikutel oleks pangakonto avamine keerulisem ning tõuseks laenuintress. Ka üldine asjaajamine ja arveldamine oleks Eesti ettevõtjatega raskem, kuna maksed peaksid läbima tihedama sõela. Ettevõtjad peaksid täpsemalt tõestama raha päritolu ja kinnitama, et tehing pole teeseldud. Saudi Araabiale erandi tegemine muudab Eesti majanduskeskkonna terrorismi rahastamisele haavatavamaks. Terrorismi rahastamise faasid on 1) kogumine, 2) edastamine ja 3) kasutamine. Saudi Araabia on terrorismi rahastamise seisukohalt haavatavaim esimeses ehk vahendite kogumise faasis. Eesti on haavatav teises ehk edastamise faasis. Saudi Araabiale erandi tegemine tugevdaks RABi hinnangul lüli nende kahe faasi, terroristlikul eesmärgil vahendite kogumise ja edastamise vahel, mõjutades seega Eesti majanduskeskkonna haavatavust terrorismi rahastamise ees, millel kokkuvõttes võivad olla tagajärjed ka Eesti julgeolekule. PPA, kui e-residendi digi-ID väljaandja peab kontrollima taotleja tausta ja veenduma, et ta ei kujuta ohtu Eesti julgeolekule, kuid riskiriikide kodanike tausta on raske kontrollida ning järelevalve teostamise võimalused on nende suhtes väga piiratud, sh raskendab seda õigusalase koostöö ja ka Eesti välisesinduse puudumine Saudi Araabias. Küll aga ei välista Saudi Araabia käsitlemine riskiriigina lõplikult e-residendiks saamist. Eelnõu kohaselt võimaldatakse riskiriigi kodanikel 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.

Majandus- ja Kommunikatsiooniministeerium	
1. Eelnõu § 1 punkti 3 ehk ID-kaardi kohustuslikkuse kaotamisega kaasnevad riskid: 1) Strateegiline risk läbi elektroonilise identiteedi kasutuse vähenemise ühiskonnas ja sellest tulenevate teiseste mõjude. Eesti digiriigi oluline vundament ja tema edu eeldus on ajalooliselt olnud elektrooniline identiteet ja eriti selle laiapõhjaline kasutuselevõtt ühiskonnas. Tänaseks on küll turule tulnud mitu teist eID vahendit ning nende populaarsus on ID-kaardi oma juba osaliselt ületanud, kuid seadusemuudatus kaotab olemuslikult eID kohustuslikkuse nõude üleüldse. Viimase ID-kaardi kriisi järeldus oli, et peaksime püüdlema situatsiooni poole, kus kodanikel on paralleelselt mitu eID-d. Nüüd aga vähendame tervikuna survet eID-d omada. Teisalt on meil 2–4 aasta perspektiivis ees situatsioon, mil tegelik eID-de valik väheneb. eIDAS määruse muutmismääruse jõustudes mobiil-ID hääbub ning kuni digiidentiteedikukru saabumiseni jääb ainsaks riiklikuks eID-ks ID-kaart. Selle kõrvale jääb ainsa alternatiivina siseriiklik Smart-ID. Seega riskime eID-de, aga eriti riiklike eID-de arvukuse ja selle läbi e-teenuste kasutuse vähenemisega ühiskonnas.	Arvestatud Vastav muudatus on eelnõust välja jäetud.

2) Taktikaline risk läbi teiste eID skeemide sõltuvuse ID-kaardist ja ID-kaardi rolli nn tagavaraidentiteedina. Nii Smart-ID kui mobiil-ID on sõltuvuses Sertifitseerimiskeskuse infrastruktuurist. ID-kaart on ainus oluliselt teistsuguse arhitektuuriga lahendus. ID-kaardi arvukuse vähenemisega väheneb ka nende inimeste hulk, kellel on „sahtlist võtta“ alternatiivlahendus Sertifitseerimiskeskuse rikke korral – väheneb eID-de kasutamise paindlikkus. Täna saab inimene ühe eID probleemide korral isiklikult kohale ilmumata (näiteks välismaal olles) kas blokeerida või algatada uue eID aktiveerimise. ID-kaardi arvukuse vähenemisega väheneb nende inimeste hulk, kellel see võimalik on. Tagavaralahenduse olemasolu vajadust tõestas juba 2017. aasta ROCA kriis. Lisaks, arvestades pingestunud julgeolekuolukorda võib tekkida äkiline vajadus eID vahendi olemasolu järele. Siinkohal on oluline märkida, et ID-kaart on paremini kaitstud mõne serverikeskuse füüsilise hävitamise korral, kui alternatiivsed kasutusel olevad eID lahendused. Kui näiteks kõik Sertifitseerimiskeskuse teenused peaksid olema häiritud, on võimalik ID-kaardiga autentimine e-teenustes tagada (12h CRL baasil, seejärel on võimalik ajutiste *whitelistide/blacklistidega* jätkata). Allkirjastamist antud lahendus ei puuduta.	
3) Kui ID-kaardi omamine pole enam kohustuslik, siis puudub inimestel motivatsioon selle omamiseks ja e-teenuste pakkujatel selle tehniliseks toetamiseks. Siinkohal näeme riski taandarenguks e-teenuste kasutamisel (vajadus hakata taaskord pakkuma rohkem teenuseid kohapeal/paberkandjal), kuna tekib juurde inimesi, kellel puudub eID vahend, kuid säilib vajadus teenuste kasutamiseks. Tuleb kindlasti arvestada, et käesoleval ajal on palju avalikke teenuseid, mida pakutaksegi ainult e-teenusena.	
4) ID-kaart on ainus eID vahenditest, mis võimaldab krüpteerida ja dekrüpteerida, lisaks krüptopulkadele. Kohustuslikkuse ära kadumisega väheneb ka paljudel krüpteerimise võimalus. Kokkuvõttes, nagu juba öeldud, siis ID-kaardi üldise kohustuslikkuse nõudest loobumist me ei toeta, kuid oleme nõus olukorraga, kus ID-kaardi omamine ei ole	

kohustuslik näiteks teatud vanusegruppidele või siis erivajadustega inimestele.	
5) ID-kaardi olemasolu ja selle elektroonilise kasutamise võimalusega on tänaseks arvestanud oma teenusprotsessides esmase valikuna ka ettevõtjad. Kliente suunatakse e-teenuseid kasutama, saadetakse neile digiallkirjastatud või krüpteeritud dokumente ning kasutatakse kaardil olevat triipkoodi äriprotsessis. Näiteks digiretseptiga ravimite ostmine apteekides, lotopiletite ostmine, kliendi tuvastamine telekommunikatsioonieettevõtete esindustes jne. ID-kaardi kohustuslikkuse kadumisel peavad ka äriinfosüsteemide omanikud tegema muudatusi oma infosüsteemides, on risk ka erasektori e-teenuste kasutamise vähenemiseks ning teenuste osutamine võib muutuda aeglasemaks. Eelmärgitud riskide tõttu saame eelnõu kooskõlastada ainult meie märkuste ja ettepanekutega arvestamise korral ID-kaardi kohustuslikkuse kaotamise osas. Teeme ettepaneku täiendavalt analüüsida eelnõu § 1 p 3 riske ja mõjusid. Tuleb kaaluda selle sätte jõustumise aja hilisemat sätestamist rakendussätetes. Sätte hilisema jõustumise aeg saab olla seotud eIDAS määruse muutmismääruse jõustumisega ning alternatiivse eID vahendi reaalse olemasolu ja kasutuse ajaga.	
2. Ettepanek **eelnõu § 1 punktis 7** esitatud sätted §-st 1 välja jätta ja viia eelnõu §-i 2. Sätted sisaldavad kodakondsuse tuvastamise meetmeid, mistõttu tegemist ei ole isikut tõendavate dokumentide seaduse reguleerimisalaga.	Mitte arvestatud Kõnesolev säte kuulub ITDS-i reguleerimisalasse, kuna esmakordse dokumendi väljaandmise menetluse käigus tuvastatakse isiku sünnijärgne kodakondsus. Kodakondsuse seaduse reguleerimisalasse ei kuulu see seetõttu, et sünnijärgsed Eesti kodanikud ei taotle mitte kodakondsust, vaid taotlevad kohe Eesti kodaniku dokumenti ning selle käigus peavad nad esitama ka tõendid Eesti kodanikust põlvnemise kohta. See on ka kehtivas õiguses selliselt sätestatud. Eelnõuga lisatakse üheks Eesti kodanikust põlvnemise tõendiks DNA-ekspertiis. Seega täiendatakse eelnõuga dokumendi väljaandmise taotlemisel esitatavate tõendite loetelu, mitte ei muudeta kehtivat protsessi ja põhimõtteid.
3. Ettepanek **eelnõu § 1 punktis 20** asendada sõnad „põhjendatud kinnituse, mis tõendab isiku vajadus taotleda dokumenti“ sõnadega	Arvestatud Eelnõu muudetud selliselt, et kinnipidamisasutuse volitatud ametnik või

„omapoolse kinnituse, et kinnipeetava suhtes esineb taotluses kirjeldatud vajadus isikut tõendava dokumendi väljastamiseks“. Vanglaametnik ei saa oma kinnitusega esitada tõendit vajaduse kohta. Vanglaametnik saab kinnitada, et taotleja poolt kirjeldatud vajadus isikut tõendava dokumendi järgi on reaalne.	töötaja lisab kinnipeetava taotlusele kinnituse, mis tõendab isiku põhjendatud vajadust taotleda dokumenti.
4. Eelnõu § 1 punkti 22 kohta märgime, et kehtiv eIDAS määrus nõuab kvalifitseeritud sertifikaatide väljastamisel isiku näost näkku tuvastamist. Palume selgitada, kuidas hakkab protsess käima peale eelnõus sätestatu jõustumist.	Arvestatud Vastav muudatus on eelnõust välja jäetud.
5. Eelnõu § 1 punkti 25 kohta märgime, et kehtiv eIDAS määrus võimaldab allkirjastamise sertifikaatide väljastamise ilma isikliku ilmumiseta, kui esimene kord on väljastatud isiklikult. Kolmandat korda väljastamine peab toimuma jälle isiklikult. eIDAS määruse muutmismäärusega võib nõue muutuda. Palume üle vaadata sätte jõustumise aeg.	Arvestatud eIDAS määruse art 24 lõige 1 määratleb identiteedi kontrollimise tingimused. Kehtiva art 24 lõike 1 punkti b kohaselt toimub kontrollimine: *kaughindamise teel, kasutades e-identimise vahendeid, mille puhul enne kvalifitseeritud sertifikaadi väljastamist tagati füüsilise isiku või juriidilise isiku volitatud esindaja füüsiline kohalolek ja mis vastavad artiklis 8 kehtestatud nõuetele seoses märkimisväärse või kõrge usaldusväärsuse tasemega*. Artiklit 24 muudetakse eIDAS2.0-ga. Paralleelselt eIDAS2.0 jõustumisega tuleb Euroopa Komisjon välja määruse rakendamiseks vajalike ettepanekutega, millest lähtuvalt täpsustame vajaduse korral siseriiklikku õigust või korrigeerime jõustumistähtaega. Praegu eelnõu ja eIDAS2.0 määruse tekstid omavahel vastuolus ei ole ning eelnõuga kavandatav säte jõustub juunis 2026. eIDAS2.0 vastava muudatuse jõustumine on kavandatud 2025. aasta kevadel.
6. Ettepaneku **eelnõu § 1 punktis 28** asendada sõna „teeb“ sõnaga „muudab“. Vt sätte kehtivat sõnastust.	Arvestatud
7. Ettepanek **eelnõu § 1 punktis 40** olevat sätet muuta järgmiselt: „(6^1) Käesoleva seaduse alusel andmekogusse ABIS kantud andmeid säilitatakse kuni 75 aastat andmekogusse ABIS kandmisest arvates. Andmetele võib kehtestada lühema säilitustähtaja andmekogu ABIS põhimääruses.“. Andmekogu ABIS volitus esineb mitmetes seadustest ning eelnõus pakutud sõnastus ei erista esinevaid esitamise aluseid, mistõttu on	Selgitus Selgitame, et andmekogu ABIS volitusnormid asuvad erinevates seadustes ja seega on vaja kõiki neid täpsustada. Iga eriseaduse volitusnorm reguleerib konkreetse seaduse alusel andmekogusse ABIS kantud andmete säilitamist. Viidatud andmekogu ABIS reguleerivad sätted muudetakse kas kõnesoleva eelnõuga või ettevalmistamisel oleva välismaalaste seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse

vajalik toonitada, et vastav tähtaeg on vaid andmete osas, mis esitatakse ITDS alusel. Siinjuures juhime tähelepanu, et eelnõu ei sisalda vastavasisulist muudatusi kõigi andmekogu ABIS andmeid sisaldavate seaduste kohta, mistõttu on eelnõuga kavandatavad muudatused ilma täpsustuseta õigusselgusetust soodustavad.	eelnõuga. Osaliselt on andmekogu ABIS regulatsioon muudetud uue KES-ga, mis jõustus 01.09.2023. Lisaks märgime, et andmekogu ABIS reguleerivad seadused viitavad, et andmekogusse ABIS kantud andmete töötlemisele kohaldatakse ITDS-i §-s 15^5 sätestatut, so ITDS kohaldamine on sätestatud paragrahvi täpsusega (KES § 23 lg 2, KodS § 2^4 lg 4, KonS § 12^1 lg 4, KrMS § 109^2 lg 2, VMS § 279^4 lg 4, VRKS § 13^7 lg 4, VSS § 33^{15} lg 4, VTMS § 31^6 lg 2), seega jääb ebaselgeks, kuidas põhjustab eelnõu tekst õigusselgusetust ja mis olukordades tuleks viidatud seaduste puhul kohaldamisele ITDS § 15^4 lõige 6^1, kus sätestatakse ITDS-i alusel andmekogusse ABIS kantavate andmete maksimaalne säilitustähtaeg. AKI hinnangul peab andmekogusse kogutavate isikuandmete koosseis ja säilitamine kui eraelupuutumatuse riive tulenevalt põhiseaduse § 26 sõnastusest ja olulisuse põhimõttest olema reguleeritud seaduse tasemel.
8. Eelnõu § 1 punkti 41 kohta märgime, et sätte kohaselt toimub dokumendivahetus väljaandja vea tõttu ja samaks tähtajaks, mis väljavahetatav dokument. Seega on põhjendamatu uute andmete küsimine, sest ka dokumendi väljaandmisel võetud biomeetrilised andmed on kehtivad. Biomeetriliste andmete uuesti küsimine on põhjendatud, kui dokument väljastatakse pikemaks tähtajaks kui senine dokument. Seetõttu teeme ettepaneku välja jätta lisatava sätte teine lause.	Mitte arvestatud ITDS § 16 lg 1 p 1 kohaselt on dokument kehtiv, kui see on välja antud ja andmed on dokumenti kantud õiguspäraselt selleks pädeva asutuse poolt. Praktikas on ette tulnud juhtumeid, kui dokument on välja antud ja andmed on dokumenti kantud õiguspäraselt ja selleks pädeva asutuse poolt ning töötab korrektselt. Viga võib ilmneda alles mõne aasta möödumisel (nt kiip ei tööta enam viieks aastaks välja antud dokumendil kolme aasta pärast), sellisel juhul ei saa öelda, et dokumendi väljaandmise protsessi on rikutud või andmed pole dokumenti kantud õiguspäraselt. Kui ilmnenud viga on seotud biomeetriliste andmetega või näiteks selgub, et varasemalt hõivatud andmete võrdlusvõimekuse tagamine ei ole enam tehniliselt võimalik, siis on vaja uue dokumendi välja andmiseks võtta biomeetrilised andmed uuesti. Samuti võib dokumendi kasutaja selleks ise soovi avaldada, nt kui ta peab garantiimenetluse läbiviimiseks tulema isiklikult PPA teenindusse, et tuua dokument kontrolli ja tema väljavahetatava dokumendi kehtivusaeg on peatselt lõppemas, siis on tal mõistlik anda kohe ka uued sõrmejäljed, sest siis kehtivate sõrmejälgede olemasolul on võimalik tal uut dokumenti

Samuti palume selgitada, et miks ei kata lisatav lõige ITDS § 16 lg 1 p 1 võimalikku juhtumit, kui väljaandja poolt on rikutud dokumendi väljaandmise protsessi.	taotleda PPA iseteeninduses. Praktikas ei soovitata isikul taotleda uut dokumenti, kui kontrolli toodud dokument kehtib veel üle ühe aasta, sest sellega kaasneb riigilõivu maksmise kohustus. Kui kasutatav biomeetria on PPA-l olemas ja tagab võrdlusvõimekuse, siis biomeetriat uuesti ei võeta. Lisaks on eelnõu täiendatud täpsete alustega, millal on uute biomeetriliste andmete võtmine lubatud. Selgitame, et ITDS § 16 lõike 1 punkti 1 kohaselt on dokument kehtiv, kui see on välja antud õiguspäraselt. Dokument ei ole välja antud õiguspäraselt, kui selle väljaandmise protseduuri reegleid on rikutud.
9. Ettepanek **eelnõu § 1 punktiga 43** lisatava sätte sõnastust täiendada dokumendi kasutaja nõusolekuga järgmiselt: „(1^1) Kui dokumendi kasutaja isikusamasust kontrollitakse dokumendi kasutaja nõusolekul päringuga saadud dokumendiandmete alusel, mis on tehtud kättesaadavaks avaliku teabe seaduse § 32^1 lõikes 1 nimetatud Eesti teabevärava kaudu, on see samaväärne käesoleva paragrahvi lõike 1 kohase isikusamasuse kontrollimisega.“.	Mitte arvestatud Isikusamasuse kontrollimise riikliku mobiilirakenduse vahendusel algatab inimene ise enda seadmest mobiilirakendusse sisselogimisel. Nii mobiil kui mobiilirakenduses olevad andmed on inimese enda valduses ja oma andmete esitamise käivitamiseks tuleb tal isiklikult aktiveerida ja teenuseosutajale esitada ruutkood. Lisaks sisaldab mobiilirakendus selget andmekaitse alast teavet ja hoiatusi. Seeläbi on isiku nõusolek enda andmete esitamiseks selgelt väljendatud.
10. Ettepanek eelnõu seletuskirja punkt 3.2.7. tekst asendada järgnevaga: „Eelnõu § 1 punktiga 43 täiendatakse ITDS-i § 18^1 lõikega 1^1, et luua võimalus isikusamasuse kontrollimiseks Eesti teabevärava kaudu. Teabeväravas kuvatakse isikutunnistust, passi ja juhiluba ning erinevaid teenuseid (näiteks andmed laste, retseptide, töövõimetuslehtede ja sõidukite kohta), mille leiab ka tulevasest riiklikust mobiilirakendusest. Dokumendivaade on teabeväravas ehk eesti.ee-s infoteenusena kättesaadav ning sarnaselt ka riiklikust mobiilirakendusest, st inimesele kuvatakse tema dokumendi andmed. Muudatus võimaldab isikul teabevärava, sh riikliku mobiilirakenduse kaudu esitada isikusamasuse kontrollimiseks oma dokument füüsilises keskkonnas, näiteks poes oma vanuse tõendamisel. Sellega antakse teabevärava ja mobiilirakenduse kaudu isikusamasuse kontrollimisele samaväärne õiguslik tähendus, nagu on füüsilise dokumendi alusel isikusamasuse kontrollimisel. Nii eesti.ee-sse kui ka riiklikusse mobiilirakendusse	Mitte arvestatud Riikliku mobiilirakenduse isikusamasuse kontrollimise tehniline lahendus on vahepeal selgemaks saanud ning seletuskirja on täiendatud lähtuvalt uuest tehnilisest lahendusest ja kontseptsioonist.

sisselogimisel kasutaja autenditakse ja talle kuvatakse tema dokument ehk sisselogimisel tehakse päring X-tee kaudu riiklikusse andmekogusse, mis on isikutunnistuse ja passi puhul ITDAK. Riiklik mobiilirakendus võimaldab lisafunktsioonina isikusamasuse kontrollimiseks kuvada teenuseosutajale dokumendi ruutkoodi või triipkoodi, mille abil teenuseosutaja saab soovi korral täiendava X-tee päringu läbi valideerida mobiilirakenduse vahendusel kuvatut. Dokumendi näitamisel ja valideerimisel saab dokumendi kasutaja valida, kas ta jagab teenuseosutajaga kõiki dokumendi andmeid või ainult osa, näiteks ainult sünniaega ja fotot vanuse kontrolliks või isikukoodi kliendisoodustuse saamiseks. Muudatus on seotud Vabariigi Valitsuse tegevusprogrammi 2023–2027 eesmärgiga 3.2.4 „Loome e-riigi mobiilirakenduse, mille kaudu riik jõuab informatsiooni ja teenustega personaalselt iga eestimaalaseni“.	
11. Palume kaaluda **eelnõu § 1 punktide 45 ja 46** eelnõust välja jätmist. Peame vajalikuks digitaalse isikutunnistuse jätkuvat väljastamist. Seda kasutatakse näiteks tööülesannete täitmisel, kui on vaja autentida ennast pidevalt erinevatesse e-teenustesse. Põhjuseks on toodud asjaolu, et ID-kaardi kiip võib kuluda kaardilugejasse sagedasel sisestamisel ja muutuda kasutamiskõlbmatuks. Kui eelnõuga loobutakse ID-kaardi kohustusliku omamise nõudest, siis võib vajadus digitaalse isikutunnistuse järgi pigem suureneda.	Mitte arvestatud PPA viis 2023.a läbi hanke ID-1 formaadis isikut tõendavate dokumentide plankide tootmiseks, isikustamisteenuse ja teiste seonduvate teenuste ostmiseks. Hankele eelnes eelanalüüs ja PPA otsusega moodustati hankekomisjon, kuhu kuulub ka MKM-i esindaja. Nimetatud hanke ettevalmistamisel otsustati, et uue hankega sõlmitava lepingu raames ei hangita edaspidi digitaalset isikutunnistust, seega ei sisalda uus ID-1 leping digitaalse isikutunnistuse tootmise võimalust ja kõnesoleva muudatusega viiakse õigus kooskõlla hankekomisjonis kokku lepituga. Kui tööülesanded nõuavad sagedast eID vahendi kasutamist, siis on võimalik selleks kasutada nt mobiil-ID-d või Smart-ID-d, mille puhul ei ole kiibi kulumise ohtu.
12. Ettepaneku **eelnõu § 2 punktist 6** välja jätta andmete alalise säilitamise kohustus ning näha ette säilitamise tähtajaks kuni 75 aastat. Juhime tähelepanu, et suuresti kattuvad andmed teistes registrites oleva teabega, mistõttu nende alaline säilitamine ei ole põhjendatud. Nii näiteks on Eesti kodaniku ja Eesti residendi andmed rahvastikuregistris alaliselt säilitatavad ning samalaadsete andmete teises kohas säilitamisel puudub vajadus. Nii samuti on küsitav hariduse või maksu võlgnevuse või karistatuse andmete tähtajatu säilitamise eesmärk, kuivõrd selline	Mitte arvestatud Eesti kodakondsuse saanud, taastanud või kaotanud isikute puhul on PPA andmeandjaks rahvastikuregistrile, mitte vastupidi. Seega kõik alusandmed on PPA andmekogudes ja rahvastikuregistrisse kõiki andmeid ei kanta. Kui PPA andmekogu andmetele kehtestada lühem säilitusaeg ja need säilitustähtaja möödumisel kustutada, siis hiljem ei ole neid võimalik enam kunagi üle kontrollida. Praktikas on tulnud ette vaidlusi, kas inimesele on antud õigetel alustel kodakondsus, kas tal olid kõik

teave ei saa kuidagi mõjutada nende järeltulijate õigust Eesti kodakondsusele.	nõuded täidetud jne. Samuti ei ole kodakondsuse andmise korraldustes isikute kohta üldjuhul toodud muid andmeid, kui ainult nimi ja sünniaeg. Ka rahvastikuregistrisse kantakse üksnes VV korralduse kuupäev ja korralduse nr, kuid kõik muud andmed on üksnes PPA andmekogus. Lisaks märgime, et eelnõuga ei ole kavandata kõigi andmekogu andmete säilitamist alaliselt. Seaduses sätestatakse andmete maksimaalne säilitusaeg, mis on alaline. Eelnõuga antakse võimalus kehtestada põhimääruses andmetele lühem säilitustähtaeg. Erinevate andmekategooriate täpne säilitusaeg kehtestatakse andmekogu põhimäärusega.
13. Ettepanek **§ 4 punkt 2** eelnõust välja jätta. Vt märkust eelnõu § 1 p 40 kohta.	Mitte arvestatud Eelnõu § 4 punktis 2 sätestatakse seaduses KrMS-i alusel ABIS-esse kantavate andmete maksimaalne säilitustähtaeg. Andmekogu ABIS põhimääruse §-d 17 ja 18 sätestavad KrMS-i alusel ABIS-esse kantavad andmed ja § 41 andmete säilitustähtajad andmekategooriate kaupa ning andmete kustutamise.
14. Ettepanek **§ 7 punkt 2** eelnõust välja jätta. Vt märkust eelnõu § 1 p 40 kohta.	Mitte arvestatud Eelnõu § 7 punktis 2 sätestatakse seaduses VangS-i alusel ABIS-esse kantavate andmete maksimaalne säilitustähtaeg. Andmekogu ABIS põhimääruse § 21 sätestab VangS-i alusel ABIS-esse kantavad andmed ja § 41 andmete säilitustähtajad andmekategooriate kaupa ning andmete kustutamise.
15. Ettepanek üle vaadata **eelnõu § 9 punktis 7** sätestatav alalise sissesõidu keelu andmete säilitamise tähtaeg. Leiame, et puudub selge vajadus säilitada alaliselt andmeid, mis on seotud ainult konkreetse isikuga. Teeme ettepaneku määrata andmete säilitustähtajaks 120 aastat isiku sünnist arvates. Põhjendamatu andmete säilitamine koormab nii digivõrku kui ka kasutab muid ressursse.	Arvestatud Eelnõu § 9 punktis 7 kavandatav alalise sissesõidukeelu andmete säilitamise muudetud tähtaeg on 75 aastat arvates isiku sünnist.
16. Ettepanek **eelnõu § 9 punktide 13 ja 14** sätted üle vaadata, kuivõrd viidatakse andmekogule ABIS, samas punktides 10 ja 11 ei ole käsitletu ABIS, seega viide on eksitav.	Mitte arvestatud Eelnõu punktiga 13 muudetakse VSS § 33^{15} lõiget 7 ja eelnõu punktiga 14 muudetakse VSS § 33^{15} lõiget 7^{1}. Mõlemad muudatused puudutavad andmekogu ABIS ja neis pole viiteid punktidele 10 ja 11. AKI hinnangul peab andmekogusse kogutavate isikuandmete koosseis ja säilitamine kui eraelupuutumatuse riive tulenevalt põhiseaduse

	§ 26 sõnastusest ja olulisuse põhimõttest olema reguleeritud seaduse tasemel.
17. Ettepanek **§ 10 punkt 2** eelnõust välja jätta. Vt märkust eelnõu § 1 p 40 kohta.	Mitte arvestatud Eelnõu § 10 punktis 2 sätestatakse seaduses VTMS-i alusel ABIS-esse kantavate andmete maksimaalne säilitustähtaeg. Andmekogu ABIS põhimääruse § 36 sätestab VTMS-i alusel ABIS-esse kantavad andmed ja § 41 andmete säilitustähtajad andmekategooriate kaupa ning andmete kustutamise. AKI hinnangul peab andmekogusse kogutavate isikuandmete koosseis ja säilitamine kui eraelupuutumatuse riive tulenevalt põhiseaduse § 26 sõnastusest ja olulisuse põhimõttest olema reguleeritud seaduse tasemel.
18. Ettepanek seletuskirja lk 13 täpsustamiseks. Nimelt asendada viimases lõigus p 1 all esimeses lauses „Euroopa Liidu liikmesriigis“ lauseosaga „Euroopa Majanduspiirkonna lepinguriigis“. Seega oleks erandi alla kaasatud ka Norra, Island ja Liechtenstein ning see läheks kokku ka RahaPTS § 34 lg 3 p-s 1 tooduga, mille kohaselt väiksemale riskile viitavate asjaolude hindamisel võib geograafiliseks riske vähendavaks asjaoluks lugeda olukorda, kus klient on pärit Euroopa Majanduspiirkonna lepinguriigist.	Arvestatud. Seletuskirja ja rakendusakti kavandit vastavalt muudetud.
19. Eelnõu seletuskiri kasutab läbivalt mobiilirakenduse nimetusena mRiiki. Teeme ettepaneku seletuskirjas kasutada lühendi „mRiik“ asemel lühendit „riiklik mobiilirakendus“. Kuigi tegemist on eelnõu teksti mõistes lihtsalt lühendiga, siis eelistaksime seda mitte selle mõistega nii tugevalt siduda ja nimetada üldisemalt „riiklik mobiilirakendus“, vältimaks tulevikus ootuseid just selle nime kasutamiseks.	Arvestatud
Rahandusministeerium	
1. Eelnõu § 1 punktiga 51 lisatakse RAB järelevalve teostajate hulka ja see seostatakse rahapesu ja terrorismi rahastamise tõkestamise seaduse § 60 lõikest 5^1 tuleneva õigusega edastada teavet Politsei- ja Piirivalveametile vastava otsuse tegemiseks. Palume selgitada seletuskirjas, miks infovahetust võimaldavast sättest tulenevalt tuleb RAB-i lisada järelevalveasutuseks ja täpsustada RAB-i kui järelevalveasutuse pädevuse piirid.	Arvestatud ITDS § 20^8 täiendusega sätestatakse õigusselguse huvides RAB-i kui järelevalveasutuse pädevus lisaks RahaPTS-le ka ITDS-s. RahaPTS § 53 lõike 1 kohaselt on RAB Rahandusministeeriumi valitsemisalasse kuuluv valitsusasutus, mis teeb riiklikku järelevalvet ning kohaldab riiklikku sundi käesolevas seaduses ette nähtud alustel ja ulatuses autonoomselt. RAB-i täpsed ülesanded on sätestatud RahaPTS §-s 54. RahaPTS § 60 lõikest 4 ja 5^1 tulenevalt on RAB-il õigus teha

	järelevalvet e-residendi digi-ID kasutamise üle. Kuigi järelevalve pädevus tuleb RAB-ile RahaPTS-st, siis kavandatava ITDS § 20^8 täiendusega tuuakse RAB järelevalve asutusena eraldi välja sarnaselt PPA-le, KAPO-le ning MTA-le. Praegu jääb selgusetuks, miks ei ole RAB-i ITDS-i § 20^8 järelevalveasutuste loetelus, sest see on erisäte, mis reguleerib järelevalve teostamist üksnes e-residendi digi-ID kasutamise üle ja RahaPTS § 53 lõike 1 kohaselt on RAB-i ülesannete täitmine RahaPTS-s sätestatud alustel ja ulatuses riiklik järelevalve. Praegu edastab PPA RAB-ile e-residendi digi-ID kasutamise üle järelevalve teostamiseks andmeid ITDS § 9^2 lõike 8 alusel. RAB-i kui järelevalveasutuse pädevuse piirid sätestatakse ITDS § 20^8 lõikes 2^1. RAB-le ei panda eelnõuga täiendavaid ülesandeid. Seletuskirja täiendatud.
2. Märgime, et rahapesu ja terrorismi rahastamise risk on erinevad. Eelnõus on kasutatud üksnes RAB-i tavapärasest kõrgema terrorismi rahastamise riskiga riikide loetelu. Seega on lähtutud üksnes terrorismi rahastamise riskist ja viited seletuskirjas rahapesu riski maandamisele pole kohased.	Arvestatud Seletuskirja täpsustatud, et RAB-i avaldatud nimekirjale viidatakse juhul, kui küsimus puudutab vaid kõrgema terrorismi rahastamise riskiga riike.
3. Ühel reeglil põhineval riigipõhisel lähenemisel on väga vähe mõju rahapesu riski maandamisele. Oma tagasisides eelnõu väljatöötamiskavatsusele tõime välja riskipõhise lähenemise ja residentsuse olulisuse rahapesu ja terrorismi rahastamise tõkestamisel. Neid märkuseid pole eelnõu seletuskirjas täiel määral adresseeritud.	Arvestatud osaliselt E-residentsuse programmi riskihaldus toimub läbi e-residentsuse nõukogu, kus on kokku lepitud riskide haldamise meetmed ja toimub riskihalduse monitooring. E-residentsuse nõukoja liikmeks on ka Rahandusministeerium. Riskiriikide nimekirja ja kohaldatavaid erisusi vaadatakse üle lähtuvalt julgeolekuolukorra muutumisest ja ilmnevatest riskidest ning vajadusel on riskiriikide nimekirja võimalik edaspidi lisada ka täiendav sihtgrupp ehk riskiriikides elavad e-residendid. Seletuskirja täiendatud.
4. Eelnõu seletuskirja leheküljel 12 on märgitud: "*e-residentsuse programmis nägid eksperdid rahapesuohte*". Terminoloogiliselt oleks õigem öelda, et seal nähti haavatavusi ning neid nii terrorismi rahastamises kui ka rahapesus.	Arvestatud
5. Eelnõu §-ga 6 muudetakse RLS § 272 lõikeid 6 ja 20 selliselt, et edaspidi on tasutava lõivu suurus ja tasutud lõivu tagastamise küsimus reguleeritud ühes ja samas normis. See ei ole normitehniliselt hea lahendus. Eriti arvestades,	Arvestatud E-residentide puhul jääb riigilõiv täies ulatuses tagastamata, kui e-residendi digi-ID taotlus jäetakse läbi vaatamata. Selgitused ja

et tasutud riigilõivu tagastamise küsimusi reguleerib RLS 2. peatüki 3. jagu. RLS § 15 sätestab nii tagastatava lõivu suuruse kui erandid. Palume kaaluda RLS § 272 lõigete 6 ja 20 korrastamist. Sama puudutab ka kehtiva RLS § 273 lõiget 8. Lisaks juhime tähelepanu, et üldjuhul jäetakse riigilõiv tagastamata kuludega proportsionaalses mahus.	põhjendused on toodud seletuskirja punktis 3.1.7.
Välisministeerium	
1. Ettepanek eelnõu § 1 punktiga 48 lisatavasse isikut tõendavate dokumentide seaduse § 20^6 lõikesse 1^2 lisada, et valdkonna eest vastutava ministri määrus, millega kehtestatakse kõrgema rahapesu- või terrorismi rahastamise riskiga riikide ja Eestiga justiits-, julgeoleku- või õiguskaitsealase koostöösuhteta riikide loetelu ning nende riikide kodanikele e-residendi digitaalse isikutunnistuse väljaandmise erisused, tuleb eelnevalt kooskõlastada Välisministeeriumiga, kuna sellel on oluline välispoliitiline ja –majanduslik mõju.	Arvestatud Vabariigi Valitsuse 13.01.2011 määruse nr 10 „Vabariigi Valitsuse reglement“ § 6 lõike 1 esimese lause kohaselt tuleb enne ministri määruse andmist või õigusakti eelnõu või muu küsimuse Vabariigi Valitsusele esitamist kooskõlastada see teiste ministeeriumide ja Riigikantseleiga, kui neile on eelnõus ette nähtud kohustusi või kui esitatav eelnõu puudutab nende valitsemisala või ülesandeid. Kõnesolev määruse eelnõu esitatakse enne kehtestamist kooskõlastamiseks kindlasti Välisministeeriumile, Kaitseministeeriumile ja teistele puudutatud asutustele.
2. Ettepanek lisada eelnõusse järgmised tehnilist laadi KonS-i muudatused: **2.1.** §-s 12 muuta andmekogu nimetus konsulaarametniku ametitoimingute ja diplomaatiliste passide andmekoguks. 2019. a muudeti välisministri 7. augusti 2017. a määrusega nr 6 kehtestatud andmekogu põhimäärust, mille käigus ajakohastati ka andmekogu nimetus tulenevalt diplomaatiliste passide menetlemise mooduli lisamisest andmekogusse.	Arvestatud
2.2. § 32 lõikest 1 jätta välja sõnad „või aukonsul“ ja lõikest 2 jätta välja teine lause. Aukonsul ei ole konsulaarametnik, seetõttu tuleks aukonsulile anda seadusega konsulaarülesandeid võimalikult minimaalselt, suunates isikuid kasutama eelkõige teisi võimalusi. Eesti dokumendid, mida kasutatakse välisriigis, väljastatakse valdavalt asukohariigi või inglise keeles, millest saab enamuses riikides teha vajadusel tõlke asukohariigi keelde. Samuti puudub võimalus kontrollida aukonsuli pädevust tõlketeenuse osutamiseks. Praktikas ei ole aukonsulid tõlketeenust ka pikema aja jooksul osutanud.	Arvestatud
2.3. § 37 lõikest 1 jätta välja sõnad „või aukonsul“. Aukonsulid ei registreeri elu- või	Arvestatud

viibimiskohti. Vajadusel võivad aukonsulid võtta vastu välisriigis püsiva elukoha registreerimise taotlusi, kuid sel juhul edastavad nad taotluse konsulaarametnikule.	
2.4. § 46 tekst sõnastada järgmiselt: „Eesti Vabariigi välisesindus võib välislepingu või Euroopa Liidu õigusakti kohaselt esindada teist Schengeni liikmesriiki tema nimel viisataotluste läbivaatamisel ja nende kohta otsuste tegemisel. Schengeni liikmesriigi välisesindus võib välislepingu või Euroopa Liidu õigusakti kohaselt esindada Eestit tema nimel viisataotluste läbivaatamisel ja nende kohta otsuste tegemisel.“. Paragrahvi 46 sõnastus viiakse vastavusse viiseeskirjaga. 1. veebruaril 2020 jõustus Euroopa Parlamendi ja nõukogu 20. juuni 2019. a määrus (EL) 2019/1155, millega muudeti määrust (EÜ) nr 810/2009, millega kehtestatakse ühenduse viisaeeskiri (viisaeeskiri). Selle õigusakti (põhjendus 9 ning muudatused viisaeeskirja artiklis 8) kohaselt peaks esindav liikmesriik vastutama viisamenetluse eest algusest lõpuni, ilma et esindatav liikmesriik oleks kaasatud. Vastavaid muudatusi kahepoolsetesse viisaküsimustes vastastikuse esindamise kokkulepetesse on Välisministeerium vastavalt vajadusele juba sisse viinud.	Arvestatud
2.5. § 70 tekst sõnastada järgmiselt: „Konsulaarametnik edastab põhjendatud vajadusel isiku või ametiasutuse kirjalikul taotlusel dokumendi Eesti või välisriigi ametiasutusele, kui välislepinguga või seaduse alusel ei ole ette nähtud teistsugust korda.“. Sätte täiendamine sõnadega „põhjendatud vajadusel“ on oluline seetõttu, et vältida heade alternatiivide olemasolul tasuta postiteenuse pakkumist. Põhjendatud vajaduseks saab lugeda olukordi, kus isikul või ametiasutusel on vältimatu vajadus esitada dokumente teisele riigile, kuid puudub näiteks turvalise postiteenuse võimalus. Vajaduse põhjendatuse üle otsustab Välisministeerium kui teenuse osutaja.	Arvestatud
Andmekaitse Inspektsioon	
Seaduses olev volitusnorm peab andmekogude puhul loetlema, mida andmekogude põhimäärustes reguleeritakse (nt pidamise kord, andmeandjad, andmevahetus teiste andmekogudega, juurdepääs ja väljastamise	Arvestatud Andmekogude sätted eelnõus täiendatud volitusnormiga.

kord jms). Volitusnormist peaks nähtuma, mida lubatakse põhimääruse tasemel reguleerida ja kõik, mida volitusega ei kaeta, peaks olema reguleeritud seaduse tasandil.	
Eesti Infotehnoloogia ja Telekommunikatsiooni Liit	
1. ID-kaardi kohustuslikkuse kaotamine Eelnõu § 1 punktiga 3 kavandatakse asendada senine kohustus omada isikutunnistust ehk ID-kaarti kohustusega omada ID-kaarti või passi. ID-kaardi kohustuslikkus on taganud elektroonilise isikutuvastamise vahendite (eID) laialdase leviku ja kasutuse. Tugeva riigipoolse garantiiga elektroonilist isiku tuvastamist ja digiallkirjastamist võimaldava dokumendi nõue on olnud Eesti digiriigi edu alus. Meile teadaolevalt pole toimunud strateegilisi arutelusid selle kaotamise üle. Samuti puudub eelnõu seletuskirjas adekvaatne mõjuhinnang Eesti digiühiskonna ökosüsteemile. ITL-i hinnangul väheneb selle muudatuse elluviimisel riigi võimekus eelistada ja mõjutada elektrooniliste teenuste arengut. Eelnõu seletuskirja kohaselt on aga muudatuse mõju e-riigile ja infoühiskonnale väheoluline, millega ei saa nõustuda. Toome välja järgmised eelnõu seletuskirja ja mõjuanalüüsi puudused:	Arvestatud Vastav muudatus on eelnõust välja jäetud.
1.1. Eelnõu seletuskirja punktis 6.2.4 (tabel 8) on selgitatud, et nii sotsiaalse kui ka riigiasutuste töökorralduse mõju ulatus on väike ning samuti on ebasoovitavad mõjud väikesed. Samas punktis toodud prognoosi kohaselt on dokumentide taotluste prognoositud arv aastatel 2024-2028 ID-kaardi osas enam-vähem sama või isegi suurem kui viimastel aastatel. Eelnõu koostajate mõte näib olevat, et vähemalt osa inimestest ilmselt ei näe vajalikuks ID-kaarti omada ja saavad võimaluse ID-kaarti enam mitte taotleda. Meie hinnangul peaks see tähendama, et prognoositud dokumentide taotluste arv ei jää samaks ega kasva.	Arvestatud Vastav muudatus on eelnõust välja jäetud.
1.2. Seletuskirjas pole arusaadavalt põhjendatud, miks peab lisaks ID-kaardile kohustusliku dokumendina sätestama passi. Seletuskirjas on ID-kaardi kui ainsa kohustusliku dokumendi kaotamist põhjendatud sellega, et inimesed eelistavad järjest enam mobiilID'd või muid mobiilipõhiseid autentimis- ja allkirjastamisvahendeid (seletuskiri p 3.2.1). Samuti ka, et passi 10-	Arvestatud Vastav muudatus on eelnõust välja jäetud.

aastane kehtivusaeg (võrreldes ID-kaardi 5-aastase kehtivusajaga) on justkui efektiivsem, sest säästab riigilõivule ja dokumendi taotlemisele kuluvat ressurssi (p 3.2.1). Lugedes aga muudatuse mõju asutuste töökorraldusele, prognoositakse järgnevateks aastateks isikutunnistuse taotluste kasvu (p 6.2.2, tabel 8). Samas kirjeldab p 6.2.2 mõju ulatust asutuste töökorraldusele väiksena, muudatused võivad vähendada töökoormust, sest PPA "menetleb vähem isikutunnistuse taotlusi tänu sellele, et edaspidi on võimalik taotleda kohustusliku dokumendina ka passi." Meie hinnangul on taoline mõjuhinnang vastuoluline ja ei klapi kokku muude seletuskirjas toodud põhjendustega. Lisame, et passi kui reisidokumendi eesmärk on võimaldada isikul reisida kolmandatesse riikidesse. Kui soovitakse loobuda ID-kaardi kohustuslikkusest, siis jääb arusaamatuks, milleks teha riigisiseselt kohustuslikuks alternatiivselt passi omamine.	
1.3. ID-kaart on hetkel esmaseks elektrooniliseks identiteediks. Eelnõus nenditakse, et mobiil-ID saab taotleda ka passi alusel. Eelnõu seletuskirjast ei selgu, kas mõjude analüüsimisel on arvestatud sellega, et mobiil-ID taotlemiseks passi alusel tuleb taotlejal isikutuvastamiseks füüsiliselt kohale minna. ID-kaardiga saab mobiil-ID-d ka elektrooniliselt taotleda. Meie hinnangul oleks passiga füüsiliselt kohale minek ebamõistlik ja tagasiminek võrreldes tänase olukorraga, kus mobiil-ID taotlemine on ID-kaardi abil lihtsaks tehtud elektroonsete vahendite abil ja selleks on võimalus end tuvastada, taotlus esitada ning mobiil-ID aktiveerida elektroonselt, füüsiliselt mobiilioperaatori juurde esindusse kohale minemata. Rõhutame, et ID kaardi kasutamine mobiil-ID aktiveerimisel on vajalik selleks, et riik saaks kindluse isikusamasuse osas, mitte ei peaks tuginema kolmandate osapoolte kinnitustele. Ainult isikut tõendava dokumendi põhjal ei pruugita piisava kindlusega isikusamasust tuvastada, samas kui riik saab kasutada identiteedi andmeid andmebaasidest ja isikusamasuse kontrollimise asemel valideerib identiteeti (sealhulgas kontrollib, et baasis ei oleks samad biomeetrilised andmed seotud mõne teise õigusliku identiteediga).	<u>Arvestatud</u> Vastav muudatus on eelnõust välja jäetud.

1.4. Eelnõu mõjude analüüsis ei ole praktiliselt mainitud määrust (EL) nr 910/2014 (eIDAS määrus) ning nõudeid (sh isikusamasuse tuvastamise nõudeid), mis on esitatud nii eID-le kui ka elektroonilise allkirja sertifikaadi väljastamisele. Kuna ID-kaart on teavitatud eID vahendina „kõrge“ tagatistasemele EL-s tunnustamiseks, siis tuleb arvestada eIDAS määruse rakendusaktiga (Komisjoni otsus) kehtestatud nõuetega tasemel „kõrge“ elektroonilise isikutuvastamise vahendi väljastamiseks. Lisaks tuleb arvestada ka kvalifitseeritud elektroonilise allkirjastamise sertifikaadi väljastamise nõuetega, iseäranis eIDAS määrus art 24 lõige 1. Lisaks sellele on hetkel kehtestamise lõppfaasis eIDAS määruse uus versioon ehk nn eIDAS2, kus nimetatud nõudeid on veidi muudetud.	Arvestatud Vastav muudatus on eelnõust välja jäetud.
1.5. Lisaks pole muudatuse puhul analüüsitud siseriiklikku mõõdet. Kui isikutunnistus on kohustuslik dokument, siis on isikul kohustus seda kasutades saada kätte riigi saadetud dokumendid – otsused ja teated. Isikutunnistusel on krüpteerimise ja dekrüpteerimise funktsioon, mis võimaldab turvaliselt saata juurdepääsupiiranguga dokumente mistahes e-posti aadressile, mille isik on riigile andnud. Mitmed sellised teenused puudutavad sotsiaalvaldkonda. Kui isikutunnistus ei ole kohustuslik dokument, siis on ainus võimalus need isikule füüsiliselt kätte toimetada, sest isikul puudub kohustus riigiga elektrooniliselt suhelda. Samuti on erinevatesse e-keskkondadesse kohustuslik sisselogimine võimalik vaid siis, kui isikutunnistus on kohustuslik. Tänu elektroonilisele isikutunnistusele on riigil ja kohalikel omavalitsustel olnud võimalik viia suhtlus valdavalt elektrooniliseks (e-teenuste põhiseks) ja vähendada füüsiliselt pakutavate teenuste mahtu. Pakkudes isikule võimaluse omada kohustusliku dokumendina kas isikutunnistust või reisidokumenti, toob see kaasa vajaduse suurendada uuesti füüsiliselt pakutavate teenuste osakaalu. Eelnõus sellekohane mõjuanalüüs puudub ning pole analüüsitud, mis mõju avaldab selline muudatus e-riigile tervikuna (rahvastikuregistri, kinnistusraamatu ja äriregistri toimingud, kohtudokumentide kättetoimetamine, e-hääletused jne).	Arvestatud Vastav muudatus on eelnõust välja jäetud.

1.6. Arvestamata on ka mõju ettevõtlusele. Võime võlaõiguslikes suhetes isikuid üheselt tuvastada on turvalise ja efektiivse majandustegevuse üks nurgakivisid. Riik pakub läbi isikut tõendavate dokumentide väljastamise menetluse täna kõikidele isikutele võimalust isikusamasuse tõestamiseks ja kontrollimiseks. Praegune lahendus on ökonoomne ja nii riiki kui ka isikut võimalikult vähe koormav - riik saab adekvaatse info isiku tuvastamist võimaldavate andmete kohta ja isik saab isikut tõendava dokumendi, mille andmete õigsust saab eeldada nii eraõiguslikes kui avalikõiguslikes suhetes. Sellise tegevuse juures on just piisav sagedus ja regulaarsus oluline. Eksperdid soovitavadki umbes viie aastast perioodi, sest siis ei jõua inimene veel liiga palju muutuda ja seos eelmise pildiga on lihtsamini valideeritav (pass kehtib 10 aastat). Seetõttu on kohustuslik ID-kaart täna ainuke "mootor", mis seda identiteedihalduse protsessi elus hoiab ja kui me selle katkestame, siis võib hakata riiklikult hallatud identiteedi andmete kvaliteet langema, mis suurendab äririske ja tegelikult pikas perspektiivis põhjustab majanduslikku kahju.	Arvestatud Vastav muudatus on eelnõust välja jäetud.
1.7. Eelnõu ei arvesta mõju tarbijatele. Näiteks kaasneks muudatusega neile olemasolevate kliendikaartide pidev ümbervormistamine erinevatele lahendustele (füüsiliselt kaardilt ID-kaardile, siis järgmisele lahendusele jne ning ka see ei pruugi olla lõplik, kuna EL-i algatusi ei ole arvesse võetud). Kasutaja vaatest on väga ebamugav selline pidev vahetamine. Leiame, et eesmärk võiks olla sujuvam ja valikute vaatest järjepidevam, mitte sundida kasutajaid kogu aeg uusi lahendusi (iga teenuse pakkuja oma rakendusega) kasutusele võtma näiteks soodustuse saamiseks. Eeltoodust järeldame, et eelnõu mõjuanalüüs ei arvesta võimalikke arenguid õigesti ja piisavalt. Eelnõu eesmärk näib olevat kasutusmugavus ja lihtsustamine, kuid samal ajal on kavandatavad muudatused sellega vastuolus ning lõpuni analüüsimata. Passi pikem kehtivusaeg (10 a) võib soodustada passi eelistamist ID-kaardile, mõtlemata muudele kaasnevatele mõjudele ja tagajärgedele. Passiga esindusse, ametiasutustesse minek isikusamasuse tuvastamiseks ega EL-i piires liikumiseks ei ole mugavam ega lihtsam valik. Praktikas selguvad	Arvestatud Vastav muudatus on eelnõust välja jäetud.

ID-kaardiga seotud teenused ja kasutuseelised hiljem, mitte dokumendi taotlemise hetkel. Kokkuvõttes ei toeta ITL sellisel kujul ID-kaardi kohustuslikkuse kaotamist, kuna puudub parem lahendus või toimiv alternatiiv. Tegemist on Eesti e-riigi alustalaga – meie eID on riiklikult toetatud, riik kontrollib ja haldab selle välja andmist. Toimiva süsteemi lõhkumine riigi poolt ilma mõjuva põhjuseta näib olevat vastuolus mõistliku ja jätkusuutliku toimetamisviisiga. Kui riik plaanib selle mõttega edasi minna, siis on kindlasti vaja läbi viia võimalike tagajärgede ja mõjude põhjalik analüüs, põhjendada muudatuse vajalikkust ja arutada seda kõigi seotud osapooltega.	Arvestatud Vastav muudatus on eelnõust välja jäetud.
2. Eelnõu § 1 punktis 43 välja pakutud lahendus ei ole sobilik selleks, et mobiilirakenduses kuvataval dokumendil võiks olla füüsilise dokumendi esitamisega samaväärne juriidiline tähendus teatud tehingute tegemiseks ja isiku tuvastamiseks. Säte on sõnastatud üsna segaselt ega ole kooskõlas seletuskirja selgitusega. Seletuskirja kohaselt näitaks isik teenuse osutajale mRiigi rakenduse abil eesti.ee portaalis olevat dokumenti ja teenuse osutaja teeks isikusamasuse kontrollimiseks päringu X-tee kaudu riiklikusse ITDAK-sse. Eelnõu sõnastuse kohaselt võiks aga justkui piisata vaid telefonil oleva dokumendi näitamisest. Meie hinnangul on korrektseks isikusamasuse kontrollimiseks mRiigi kaudu vaja lahendada eelnevalt mitmed väljakutsed. Hetkel on mRiigi rakendus isikutuvastuse mehhanismina pakutud välja ilma igasuguse mõjuhinnangu ja turvaanalüüsita. Puudu on tingimused turvalisele keskkonnale, kust tõend väljastatakse, sätestamata on millised on vajalikud turvaprotokollid jms. Seaduse tasemel ei pea küll tegelema detailidega, kuid need küsimused tuleb läbi mõelda ja leida sobilik lahendus. Näiteks anda VV-le või ministrile volitus ja kohustus töötada välja tingimused, mis on vajalikud sellise teenuse turvalisuse tagamiseks. Hetkel eelnõu seletuskiri ei selgita neid aspekte. Teine oluline puudus seisneb selles, et ei ole analüüsitud seost mRiigi rakenduse ja eIDAS2 määrusega kohustuslikuks muutuva walleti ehk digikukru vahel. Seletuskirjas on öeldud, et eelnõu pole seotud	Selgitus Mobiilist või mobiilirakendusest lihtsalt oma andmete näitamine ei ole eelnõuga reguleeritav isikusamasuse kontrollimine. RIA on koostöös riikliku hanke võitnud lepingupartneriga analüüsinud ja hinnanud loodava lahenduse turvalisusele kohaldatavaid nõudeid, millest lahenduse arendamisel lähtutakse. Nõustume esitatud seisukohaga, et riik peab arvestama Euroopa Liidu kohustusega luua digiidentiteedikukkur, mis on tasemele „kõrge“ vastav eID vahend ning uued loodavad lahendused peavad toetama nii olemasolevat eID ökosüsteemi kui olema ka võimalusel omavahel koosmõjus. Riikliku mobiilirakenduse ja digiidentiteedikukru omavahelist koosmõju on analüüsitud ja luuakse lahendused, mis arvestavad ja täiendavad üksteist. Riikliku mobiilirakenduse arendamisel lähtutakse Euroopa Liidu eIDAS 2.0 määrusest tuleneva kohustusega võtta kasutusele digiidentiteedikukkur ja isikusamasuse kontrollimise funktsionaalsuses võetakse kasutusele eIDAS 2.0 digiidentiteedikukru standard lahendus. Riikliku mobiilirakenduse lahendusega ei looda uut „kõrge“ tasemega eID vahendit. Samuti ei ole selle näol tegemist uue eraldiseisva (digitaalse) dokumendiliigiga.

EL õiguse ülevõtmisega (p 5). Samas oleme seisukohal, et muudatused vajavad analüüsimist ka EL õiguse, ennekõike uue eIDAS määruse kontekstis. Hetkel vaid nenditakse seletuskirjas, et uue eIDAS määrusega võetakse kasutusele digikukru lahendus (p 3.2.1) ja sellega tundub analüüs ka piirduvat. Meie hinnangul on väga vale jätta arvestamata, et hetkel tegeletakse paralleelselt peagi vastuvõetavas eIDAS2 määruses identiteeditasku lahenduse ning nn elektrooniliste atribuuditõendite teenuste reguleerimisega. Tegemist on samaaegselt identiteedihalduse teemadega tegelemisega erinevate töögruppide poolt ning pole välistatud erinevate lahenduste tõttu isikut tõendavate dokumentide seaduse mitmekordne muutmine ja/või uute lahenduste väljatöötamine paralleelselt. Nende puhul tegeletakse täpselt selliste tõendite (nagu eelnõu seletuskirjas on mRiigi puhul kirjeldatud) jaoks andmete kogumise ja tõendi esitamise usaldusväärust tagavate teenuste osutamise tingimustega (kuidas ning mis tingimustel neid tõendeid identiteeditaskus esitada saab). Eelnõus pole esitatud selles osas mõjuanalüüsi - millisena mRiigi rakendust saab nende muudatuste valguses käsitleda ja kas see oleks ka nende tingimuste kehtima hakkamisel tunnustatav EL-i üleselt. Tekib küsimus, kas mRiigi rakendus plaanitaksegi jätta vaid siseriikliku tähtsusega rakenduseks, millel pole laiemat mõju ega ka usaldusväärsust. Leiame, et riigi eesmärgiks võiks olla lihtsustamine ja arvestamine ühtlasi kohe ka piiriülese identiteedi lahenduse ja võimaldamisega, mitte iga eesmärgi jaoks uue identimisvahendi loomine, mis olemasolevat ei toeta. Seetõttu teeme ettepaneku analüüsida, kuidas seostub mRiigi arendamine ja kasutuselevõtt digikukruga. Samuti tasub analüüsida, kas mRiigist mingi tunnuse näitamine on defineeritav usaldusteenusena jmt. Sellised analüüsid on oluline eeltingimus selleks, et olemasolevat ja kehtivat süsteemi muutma hakata. Selleks tuleb kõiki olulisi aspekte arvesse võtta ning anda seotud osapooltele võimalus tuua välja muudatuse mõjud toimivatele teenustele ja seostele. Kindlasti peab eesmärgiks olema lahendus, mida saab pidada samaväärseks isikut tõendava	Kõnesolev eelnõu ei keskendu digiidentiteedikukru temaatikale, kuna eIDAS 2.0 määruse rakendamise siseriiklikud arutelud alles käivad. Euroopa Liidu määrus on liikmesriikidele otsekohalduv ja MKM-i eestvedamisel on analüüsimisel, kas ja millisel määral tuleb siseriiklikku õigust muuta. Küll aga on otsustatud, et riikliku mobiilirakenduse lahendus on planeeritud kasutamiseks vaid siseriiklikul tasandil. Seletuskirja on muudetud ja täiendatud.

dokumendi esitamisega. Vähemaga ei saa nõustuda. Selline lahendus aga peab olema võimalikult tehnoloogianeutraalne. Juhime veel tähelepanu asjaolule, et eelnõu seletuskirjas viidatud mRiik ei oma iseenesest selgepiirilist definitsiooni ja pelgalt rakenduse nimetamisega ei tohiks siduda riiklikult olulisi tegevusi.	
3. Eelnõu § 1 punktiga 22 saab dokumendi taotleja määrata dokumendi kättesaamiseks volitatud esindaja kogu dokumendi menetluse jooksul. Antud eelnõu punkt ei täpsustata kuidagi ja pole selge, kas taotleja kohalolu ja näost-näkku tuvastamine on vajalik konkreetse eID menetluse jooksul või mingi ajaperioodi jooksul? Analüüsitud ei ole muid isikutunnistuse väljastamisega seotud nõudeid (eIDAS, eID ja e-allkirja sertifikaadi väljastamiseks) ja kavandatava muudatuse mõju. Näiteks vastavalt eIDAS määrusele ja selle alusel kehtestatud rakendusaktidega „kõrge“ tagatistasemega elektroonilise isikutunnistuse väljastamisele ja isikusamasuse tuvastamisele esitatud nõuetele tuleb eID taotleja füüsilisi karakteristikuid võrrelda autoriteetsest allikast pärinevate andmetega (isikut tõendav dokument või ka biomeetrilised andmed andmekogus), see tähendab taotleja füüsilist kohalolu taotlemise protsessis. Võimalikud on ka alternatiivid, kuid nende rakendamiseks on vajalik täita teatud lisatingimusi. Hetkel ei näe, kuidas volitatud esindaja määramine (v.a seaduslik esindaja) nende tingimuste alla mahub, mistõttu palume selles küsimuse esitada põhjalik analüüs. Hetkel on see puudu. Samuti puudub eelnõus mõjude analüüs kaasnevate turvariskide ja n-ö ebasoovitavate mõjude osas. Näiteks kas volitatud esindaja määramine muudab veel kergemaks erinevate kelmuste ja pettuste toimepanemise isiku (elektroonilist) identiteeti ära kasutades või vahet ei ole võrreldes praeguse olukorraga (ja milline see olukord on üleüldiselt)? Nii nagu teise isiku koroona-sertifikaadi pilti esitati vaktsineerituse tõendina, siis samavõrra lihtne võib olla isiku tuvastamisega eksimine mobiili ekraanil kuvatu vahendusel. Kui mobiil-ID puhul on vaja lisaks ka PIN-koodi teada, siis mRiigi turvalisusele ja tuvastamise mitme-astmelisusele või muudele	Arvestatud Vastav muudatus on eelnõust välja võetud.

turvalisust tagavaid meetmeid ei ole hetkel eelnõus käsitletud.	
4. Eelnõu § 1 punktiga 25 kavandatakse muudatust, mille kohaselt võib dokumendi väljaandja kontrollida dokumendi taotleja isikusamasust dokumenti kantud digitaalset tuvastamist või digitaalset allkirjastamist võimaldava sertifikaadi kaudu. Antud juhul on vajalik analüüsida muudatuse mõju ökosüsteemile ja kuidas saavad ökosüsteemi osapooled aru, kas eID on väljastatud füüsilise isikusamasuse tuvastamise kaudu või eID/e-allkirjastamist võimaldava sertifikaadi kaudu. Nimelt on siin jällegi seos eIDAS määruse artikliga 24 lg 1, mis määratleb tingimused, mis peavad olema elektrooniliseks isikutuvastamiseks täidetud. eID/e-allkirjastamist võimaldava sertifikaadi kaudu isikusamasuse tuvastamisel peab veenduma, et selle sertifikaadi väljastamisel on isiku isikusamasus tuvastatud füüsilisel kohalolul. Kuidas riik ise selles veendub ja tagab samas tuginevatele osapooltele informatsiooni isikusamasuse meetodi kohta, näiteks kasvõi mobiil-ID või Smart-ID väljastamiseks? Juhul, kui ID-kaart väljastatakse elektroonilises menetluses, siis mobiil-ID või Smart-ID-d ei tohi selle ID-kaardi sertifikaatidele tuginedes elektroonilises menetluses enam väljastada, vaid peab kasutama muud isikutuvastamise meetodit (mis on lubatud eIDAS määruse viidatud artiklis). Sama probleem tekib ka ID-kaartide endi väljastamisel, kuniks jõuab kätte aeg, kui taotlejad soovivad teist ringi ID-kaarti elektrooniliselt taotleda.	Selgitus eIDAS määruse art 24 lõige 1 määratleb identiteedi kontrollimise tingimused. Kehtiva art 24 lõike 1 punkti b kohaselt toimub kontrollimine: *kaughindamise teel, kasutades e-identimise vahendeid, mille puhul enne kvalifitseeritud sertifikaadi väljastamist tagati füüsilise isiku või juriidilise isiku volitatud esindaja füüsiline kohalolek ja mis vastavad artiklis 8 kehtestatud nõuetele seoses märkimisväärse või kõrge usaldusväärsuse tasemega*. Artiklit 24 muudetakse eIDAS2.0-ga. Paralleelselt eIDAS2.0 jõustumisega tuleb Euroopa Komisjon välja määruse rakendamiseks vajalike ettepanekutega, millest lähtuvalt täpsustame vajaduse korral siseriiklikku õigust või korrigeerime eelnõu jõustumisaega. Praegu eelnõu ja eIDAS2.0 määruse eelnõu tekstid omavahel vastuolus ei ole. Eelnõuga kavandatav säte on planeeritud jõustuma juunis 2026. eIDAS2.0 vastava muudatuse jõustumine on kavandatud 2025. aasta kevadeks.
5. Andmekogu ABIS puudutavate muudatuste puhul jääb mulje nagu oleks tegu pelgalt andmekogu ABIS formaalse toomisega seadusesse. ITL-ile teeb muret avaliku diskussiooni ja läbipaistvuse puudumine, samuti mõjude hindamise pealiskaudsus eelnõus – mis eesmärgil, kuidas ja kelle poolt biomeetrilisi andmeid töödeldakse jms. Samuti milline on garantii, et täidetakse erinevaid turbenõudeid, parimaid praktikaid (näiteks biomeetriliste andmete hõivel, teesklusrünnete tuvastamise mehhanismide rakendamisel, biomeetriliste karakteristikute võrdlemise usaldusväärsuse ja töökindluse tagamisel jms). Lisame, et ka mRiigi edaspidine kasutus, andmete kogumine,	Mitte arvestatud Eelnõus sisalduvad andmekogude regulatsioonide muudatused on formaalsed. Eelnõuga ei muudeta biomeetriliste andmete töötlemise põhimõtteid ega aluseid. Muudatused on tingitud AKI ja JUM-i hinnangust, et andmekogusse kogutavate isikuandmete koosseis ja säilitamine kui eraelu puutumatuse riive, peab tulenevalt PS § 26 sõnastusest ja olulisuse põhimõttest olema reguleeritud seaduse tasemel.

töötlemine, tegevuste logimine jäi eelnõud lugedes esialgu veel ebaselgeks.	
6. Vastuolu hea õigusloome tavaga. ITL-ile on arusaamatu, miks nii fundamentaalsete Eesti eID ökosüsteemi puudutavate muudatuste kohta ei ole koostatud väljatöötamiskavatsust ega peetud huvigruppidega arutelusid. Seda ei ole ka seletuskirjas (p 2) põhjendatud. Samuti miks eelnõud erasektorile arvamuse esitamiseks ei saadetud. Eelnõuga tutvudes paistab silma väga ebaühtlane kvaliteet ehk muudatuste ettevalmistamise tase. Näiteks on e-residentsuse muudatused oluliselt põhjalikumalt ette valmistatud, nende kohta koostati ka väljatöötamiskavatsus. Seetõttu on need muudatused seletuskirjas ka paremini selgitatud ja arusaadavad. Kokkuvõtteks tervitame, et riik on pidanud oluliseks üle vaadata ja ümber mõtestada senist isikut tõendavate dokumentide väljaandamise praktikat ja dokumendikohustust. Samas peame äärmiselt vajalikuks, et selliste oluliste muudatuste kavandamisega käiks kaasas ka sisuline arutelu, millesse on kaasatud huvigrupid ja tulevased kohuslased. Sellisel juhul on tõenäolisem, et tehtavad muudatused on läbi mõeldumad, arusaadavamad ja ettenähtavamad. Antud eelnõu puhul pole aga arvestatud hea õigusloomega ja muudatustega tutvudes tekkis meil ridamisi küsimusi. Seetõttu ei toeta ITL eelnõu sätteid, mille puudulikule ettevalmistusele oleme käesolevas kirjas viidanud. Lõpetuseks teeme Siseministeeriumile ettepaneku korraldada ITL-i kirjas välja toodud murekohtade arutamiseks kohtumine. ITL-i liikmetest eksperdid on valmis meie seisukohti täiendavalt selgitama ja kaasa mõtlema sobivate lahenduste välja töötamisel eelnõu eesmärkide saavutamiseks. Loodame, et ITL-i tagasiside on Teile abiks eelnõu edasisel menetlusel. Palume hoida meid eelnõu edasiste arengutega kursis.	<u>Selgitus</u> Arvamuses tuuakse välja, et dokumendikohustuse täiendamine ja mRiigi kaudu isikusamasuse kontrollimise võimaldamine on fundamentaalsed eID ökosüsteemi puudutavad muudatused. Siseministeerium ei ole samal arvamusel ega hinda nende muudatuste mõju nii oluliseks, mistõttu ei peetud väljatöötamiskavatsuse koostamist vajalikuks. Väljatöötamiskavatsused koostati muudatuste osas, mis on muudatuse sihtrühmale piiravad või mis puudutavad isikuandmete töötlemisega seotud õiguste laiendamist. Seetõttu keskendutakse eelnõus põhjalikumalt nendele teemadele. Kindlasti aga täiendame seletuskirja kooskõlastusringilt laekunud tagasisidest lähtuvalt. Siseministeeriumi hinnangul ei oma eelnõus pakutud riikliku mobiilirakenduse kaudu isikusamasuse kontrollimise rakendust puudutav muudatus nii suurt mõju, sest selle näol ei ole tegemist uue isikut tõendava dokumendi liigiga, vaid luuakse teenuseosutajatele täiendav võimalus isikusamasuse kontrollimiseks. Lahenduse kasutuselevõtt on teenuseosutajale vabatahtlik ja inimese võimalus enda isikut sel moel tõendada sõltub teenuseosutaja valmisolekust kasutada mobiilirakendust. Lisaks selgitame, et ITDS-i muutmise eelnõu oli arvamuse avaldamiseks avalikult eelnõude infosüsteemis kättesaadav kõigile huvigruppidele, sh ITL-ile ja kõigil oli võimalus eelnõu kohta arvamus esitada. Lisaks on ITL ja teenusepakkujate esindajad olnud kaasatud MKM-i korraldatud mRiigi aruteludesse.
Politsei- ja Piirivalveamet	
1. Seletuskirjas on samaaegselt viidatud mRiigis sisalduvale dokumendi kuvale kui ka dokumendile. PPA kui isikut tõendavate dokumentide väljaandja täpsustab, et dokumendikuva ei võrdu dokumendiga, kuid kuna seletuskirjas on viidatud mõlemale mõistele, jääb ebaselgeks, kas mRiigi puhul on	<u>Arvestatud</u> Seletuskirja täiendatud. IKÜM artikli 35 lõike 3 kohaselt on andmekaitsealase mõjuhinnangu tegemine nõutav järgmistel juhtudel:

tegu dokumendi kuva või elektroonilise dokumendiga, mis on mõeldud kasutamiseks füüsilises keskkonnas, nt isikusamasuse kontrollimiseks. PPA teeb ettepaneku see eelnõus selgelt sõnastada ning seletuskirjas arusaadavalt lahti kirjutada, et vältida erinevaid arusaamu ja tõlgendusi, millega mRiigi näol tegu on – dokumendikuva või elektroonilise dokumendiga. Ühtlasi soovib PPA teada, kas seoses mRiigi kasutusele võtmisega on teostatud andmekaitsealane mõjuhinnang, mis mh sisaldaks riskide kaardistust PPA-le jt korrakaitseorganitele, kes peaksid mRiigi alusel isikut tuvastama.	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, või c) avalike alade ulatuslik süstemaatiline jälgimine. Isikusamasuse kontrollimisel riikliku mobiilirakenduse poolt vahendatud kontrollpäringuga saadud dokumendiandmete ning isiku võrdlemise teel ei esine ühtegi IKÜM artikli 35 lõikes 3 nimetatud olukorda. Seega ei ole andmekaitsealase mõjuhinnangu tegemine kohustuslik. Isikusamasuse kontrollija ei salvesta kontrollpäringuga saadavaid andmeid ja päringu kehtivusaeg on piiratud.
2. Seletuskirjas rõhutatakse, et muudatus annab mRiigi kaudu isikusamasuse kontrollimisele samaväärse õigusliku tähenduse nagu füüsilise dokumendi alusel isikusamasuse kontrollimisel. See tekitab põhjendatud ootusi nii inimestes kui ka avaliku ja erasektori teenusepakkujates, kasutada mRiiki füüsilise dokumendi asemel enda isikusamasuse tõendamiseks erinevaid teenuseid kasutades. Eelnõu seletuskirjas on muudatuse kohta antud väga põgus seletus, mis ei analüüsi nt korrakaitseorganite võimalusi isikusamasuse kontrollimisel antud meetodi rakendamiseks. Siinkohal on PPA korrakaitseüksustel tekkinud küsimus, kas on analüüsitud vajadust muuta ka korrakaitseseaduse § 32 isikusamasuse tuvastamise sätteid või katab ITDS § 18[1] muudatus või juba kehtiv erimeetme sõnastus antud olukorra ära? Hetkel kehtiv säte rõhutab olukorda, kus isikul on kaasas isikut tõendav dokument ja korrakaitseorganil on õigus nõuda füüsilise dokumendi esitamist.	Selgitus Loodav lahendus on täiendav võimalus isikusamasuse kontrollimiseks PPA väljaantud kehtiva dokumendi andmete alusel. Tegemist ei ole eraldiseisva digitaalse dokumendiga ega uue dokumendiliigiga. KorS-i muutmise vajadus puudub, kuna uus lahendus loob täiendava võimaluse isikusamasuse tuvastamiseks KorS § 32 vaates.
3. Kui tegemist on elektroonilise dokumendiga, mis on mõeldud isikusamasuse tõendamiseks füüsilises keskkonnas ja mis on õiguslikult samaväärne mistahes muu isikut tõendava dokumendi (v-a digi-ID) alusel tehtud	Mitte arvestatud Tegemist ei ole uue elektroonilise dokumendiga vaid PPA välja antud kehtiva dokumendi andmetel põhineva isikusamasuse kontrollimisega. Isikusamasuse kontrollimine

isikusamasuse kontrolliga, siis näeb PPA siin mitmeid kasutegureid ja lisandväärtust erinevate teenuste protsessides, mh ka kõikidele korrakaitseorganitele, kes kasutavad enda töös KorS § 32 erimeedet. Sellise lähenemise eelduseks on aga esmalt see, et mRiik on seadustes defineeritud kui elektrooniline isikut tõendav dokument ning sellele on kirjeldatud dokumendile omased tehnilised nõuded. Lisaks sellele peab olema tagatud turvalisus.	toimub riikliku mobiilirakenduse vahendatud kontrollpäringuga saadud dokumendiandmete ning isiku võrdlemise teel, tuginedes PPA välja antud dokumendi andmetele, mida säilitatakse ITDAK-is ja andmekogus ABIS. ITDAK-i andmed omavad õiguslikku tähendust. Mobiilirakenduse vahendatud kontrollpäringuga saadavad dokumendi andmed ei ole eraldiseisev elektrooniline dokument, samuti ei ole elektrooniline dokument mobiilirakendus. Elektrooniliselt kuvatavad andmed on varasemalt isikule välja antud kehtiva dokumendi andmed ja loodav lahendus on turvaline kanal andmete kuvamiseks. Loodav lahendus peab tagama isikuandmete kaitstuse ja seotuse dokumendi kasutajaga, vastama turvalisuse nõuetele ja välistama nii võltsitud andmete kuvamise kui ka võltsitud mobiilirakenduse kasutamise.
4. Seaduse tasandil on hetkel defineeritud mõiste „digitaalne isikutunnistus“, millega peetakse silmas digi-ID-d, mis on füüsiline dokument, kasutamiseks üksnes elektroonilises keskkonnas oma isiku tuvastamiseks ja digitaalse allkirja andmiseks. Selle dokumendiga ei saa oma isikut füüsilises keskkonnas tõendada. Kui eelnõus on siiski mõeldud dokumenti ja mitte selle kuva, siis on PPA hinnangul tegu täiesti uue dokumendiliigiga, mis tuleb seaduse tasandil defineerida ja millele tuleb kirjeldada dokumendile omased tehnilised nõuded, välja töötada taotlemise ja väljastamise protsess. Juhul, kui mRiigi näol on siiski tegemist elektroonilise isikut tõendava dokumendiga, mis on mõeldud isikusamasuse tõendamiseks füüsilises keskkonnas, siis palume täpsustada, kus planeeritakse need tehnilised nõuded reguleerida.	<u>Selgitus</u> Tegemist ei ole digitaalse isikutunnistusega, uue dokumendiliigiga ega elektroonilise isikut tõendava dokumendiga. Isikusamasuse kontrollimisel lähtutakse PPA välja antud dokumendi andmetest ja kuvatakse rakenduses selle dokumendi andmed.
5. PPA on veendunud, et mRiigis dokumendikuva päringute teostamisel, suureneb olulisel määral päringute maht isikut tõendavate dokumentide andmekogusse (edaspidi ITDAK), mis võib tekitada probleeme isikut tõendavate dokumentide taotlemise ja väljastamise protsessis, kuna ületab andmekogule seatud piiranguid. ITDAK-i teevad päringuid erinevad PPA teenused, mistõttu on reaalne oht, et päringute hulga suurenemisel halveneb oluliselt kõikide PPA teenuste töö. Seni ei ole PPA-le	<u>Arvestatud</u> Seletuskirja punkti 7 alapunkti 4 täiendatud analüüsi- ja arendusvajaduste kirjeldusega. Täpne jõustumisaeg selgub pärast lähteülesande valmimist.

teadaolevalt hinnatud võimalikke andmemahtusid, kui erasektor alustab mRiigi rakendamisel kontrollpäringute teostamist ITDAK-i, mistõttu ei saa PPA tänase info pinnalt öelda, et see sellisel kujul võimalik on. Oluline on ka ära märkida, et PPA-l ja Riigi Infosüsteemi Ametil (edaspidi RIA) puudub omavahel kehtiv andmevahetusleping, mistõttu puudub PPA-l ka õiguslik alus kõnealuse päringu alusel mRiigile ITDAK-ist andmeid väljastada. Lähtudes puuduvast andmemahtude hinnangust ja andmevahetuslepingust, teeb PPA ettepaneku, mitte sõnastada eelnõus ja seletuskirjas erinevaid protsesse ja päringuid, mis ei ole osapoolte vahel kokku lepitud. Pigem võiks seletuskirjas välja tuua, et seaduseelnõu muudatusega luuakse vastav võimekus õiguslikul tasandil, kuid täpsemad detailid protsesside ja päringute osas on veel selgumisel.	
6. Erinevaid ekraanitõmmiseid on väga kerge võltsida, mistõttu ei pea PPA antud lahendust sellisel kujul turvaliseks. On ebaselge, kuidas maandatakse näiteks riski, kus isik esitab teenusepakkujale mRiigi kuva asemel kuvatõmmise kellegi teise mRiigi kuvast. Tehnoloogiliselt saab teenusepakkuja QR-koodi välja lugemisel mõlemal juhul sama vaste, aga juriidiliselt on ühel juhul tegemist identiteedipettusega, kus esitatakse kellegi teise andmed enda omadena. Kui QR-koodi kasutatakse isikusamasuse kontrollimisel, siis peab see olema nii turvaline kui ka usaldusväärne. Näiteks viisakleebiste ja ELi digitaalsete COVID-tõendite puhul luuakse usaldusväärsus riikliku sertifitseerimisahela kasutamise kaudu, lisaks on võimalus kasutada ka erinevaid krüpteerimislahendusi. Hetkel ei tule seletuskirjast välja, millised on turvalisuse tagamise elemendid QR-koodi kasutamisel.	Arvestatud. Seletuskirja täiendatud ja riikliku mobiilirakenduse turvalisust selgitav dokument on RIA poolt edastatud SiM valitsemisala asutustele.
7. Eelnõus luuakse võimalus mRiigi kaudu esitatud dokumendi kuva alusel isikusamasuse kontrollimiseks ning teenusepakkuja, kes antud lahendust isikusamasuse kontrollimiseks kasutab, hindab ise dokumendikuva esitamisega seotud võimalikke riske konkreetse teenuse kasutamisel. PPA teeb ettepaneku, et riik siiski identiteedipoliitika kujundajana ning identiteedi turvalisuse eest vastutajana, peaks reguleerima, millistel juhtudel on mRiigi kaudu esitatud dokumendikuva alusel tehtud isikusamasuse	Arvestatud osaliselt ITDS reguleerib isikut tõendavate dokumentide kohustust ja Eesti Vabariigi poolt Eesti kodanikele ning välismaalastele isikut tõendavate dokumentide väljaandmist. Seda, kas konkreetses teenuses on riikliku mobiilirakenduse vahendusel isikusamasuse kontrollimine võimaldatud, otsustab teenuseomanik ja riik saab seda reguleerida vastavates eriseadustes. Eelnõud on täiendatud ITDS § 18^1 lõikega 1^2, mis ütleb, et riikliku

kontroll võrdne füüsilise dokumendi esitamisega ja millistel mitte. Hetkel jääb eelnõust ja seletuskirjast ebaselgeks, millistes olukordades on õiguslikult aktsepteeritav mRiigi kaudu isikusamasuse kontroll ning samas tekitab õigustatud ootuse, et see sobib mistahes teenustes.	mobiilirakenduse vahendusel ei saa isikusamasust kontrollida dokumendi taotlemisel ja väljastamisel.
8. Täpsustavalt küsime, kas on plaanis koostada avalikult kättesaadav nimekiri teenustest, kes mRiigi dokumendikuva saaksid kasutada ja millised ettevõtted selle oma teenustes ka kasutusele on võtnud?	Selgitus Käesoleva eelnõuga ei ole kavas taolist nimekirja koostada. Seda, kas konkreetses teenuses on riikliku mobiilirakenduse vahendusel isikusamasuse kontrollimine võimaldatud, otsustab teenuseomanik ja riik saab seda reguleerida vastavates eriseadustes.
9. PPA sooviks võimalusel tutvuda koostatud turu-uuringuga, mis toob välja mRiigi võimalikud kasutusjuhud ja huvitatud osapooled, kes sooviksid mRiiki oma teenustes isikusamasuse kontrollimiseks kasutada.	Selgitus Küsimus edastatud RIA-le.
10. Kuna eelnõuga antakse inimesele valik, kas ta soovib kohustusliku dokumendina omada passi või ID-kaarti, toome välja võimaliku murekoha seoses korrakaitseorganite halduskoormuse suurenemisega isikusamasuse tuvastamisel. Probleemina nähakse eelkõige seda, et inimeste jaoks, kes valivad kohustusliku dokumendina passi, võib olla selle igapäevane kaasas kandmine tülikas, kuid eelnõuga justkui luuakse eeldus ametnikele ja õigustatud ootus dokumendi kasutajatele, et sellistel puhkudel asendab mRiik füüsilist dokumenti ning seda saab kasutada oma isikusamasuse tõendamiseks füüsilises keskkonnas samaväärselt passi või ID-kaardiga. Eelnõu tekstist ega seletuskirjast ei tule üheselt välja piiranguid mRiigi kasutamisel ning kui neid ikkagi esineb (nt avalikes teenustes), siis tuleb see nii kirja panna. Selline täpsustus aitaks vältida olukorda, kus üksnes passi kasutaja ekslikult eeldab, et selle esitamine nt korrakaitseorganitele oma isikusamasuse tuvastamiseks ei ole vajalik ning korrakaitseorganil tuleb teha rida täiendavaid toimingud isikusamasuse kontrollimiseks.	Arvestatud osaliselt Kehtiv regulatsioon ei sätesta nõuet, mis kohustab inimest isikut tõendavat dokumenti kaasas kandma. Dokumendi kaasas kandmise kohustus kehtib vaid juhtudel, kui on tarvis tõendada teatud eriõigusi, näiteks mootorsõiduki juhtimisel juhul, kui juhiluba ei ole kaasas, relva kandmisel või alkoholi ostes vanuse tõendamisel. Seega tuleb ka kehtiva korra kohaselt korrakaitseorganil teha isiku isikusamasuse kontrollimiseks täiendavaid toiminguid, kui inimesel ei ole dokumenti kaasas. Jääb selgusetuks, milliseid täiendavaid toiminguid tuleb korrakaitseorganil eelnõuga tehtava muudatuse jõustumisel isikusamasuse kontrollimiseks teha. Seda, kas konkreetses teenuses on riikliku mobiilirakenduse vahendusel isikusamasuse kontrollimine võimaldatud, otsustab teenuseomanik ja riik saab seda reguleerida vastavates eriseadustes. Eelnõud on täiendatud ITDS § 18^1 lõikega 1^2, mis ütleb, et riikliku mobiilirakenduse vahendusel ei saa isikusamasust kontrollida dokumendi taotlemisel ja väljastamisel.
11. Ettepanek täpsustada, milliseid ja kust pärinevaid kontaktandmeid võib kasutada ITDS muudetud § 9^2 lõige 7^1 kohaselt.	Arvestatud

12. Seoses sertifikaatide peatamise ja peatamise lõpetamise võimaluse kaotamisega, tuleks see muudatus teha ka § 9^2 lg 8 muudatuses.	Mitte arvestatud Vastav muudatus on olemas eelnõu § 1 punktis 10.
13. Seoses ITDS § 11^3 lõike 3 ja § 12^2 lõike 2 muudatusega oleks vaja läbivalt ka rakendusaktides asendada vanglatöötaja sõna vanglaametnikuga.	Selgitus Rakendusaktide muutmisega tegeletakse põhjalikumalt enne seaduse muudatuste jõustumist. HÕNTE § 48 lõike 2 kohaselt peab seaduseelnõu seletuskirjale lisatud määruse eelnõu kavand olema ette valmistatud sellise täpsusega, et oleks võimalik hinnata rakendusakti vajalikkust, volitusnormi ulatust, kohast tasandit ja muid asjaolusid, mis on vajalikud volitusnormi sõnastuse ja rakendusakti vastavuse hindamiseks. Rakendusaktis terminite ühtlustamise eesmärki selles eelnõu menetlemise etapis ei ole. Tuleme ettepaneku juurde tagasi rakendusakti menetlemisel.
14. Ettepanek täiendada ITDS § 11^5 lg 1 sõnastust viisil, et eemaldada taotluse vastuvõtmise nõue ja lisada tähtaeg toimingute sooritamiseks: (1) Kui Eestis viibiva isiku terviseseisund püsivalt ei võimalda tal dokumendi väljaandmise taotluse esitamiseks isiklikult Politsei- ja Piirivalveametisse pöörduda ja isiklik pöördumine on nõutav, võib Politsei- ja Piirivalveamet taotleja isiku tuvastada või kontrollida taotleja isikusamasust ja võtta temalt biomeetrilised andmed tema elukohas või viibimiskohas Eestis hiljemalt 3 kuu jooksul. Palume jätta sõnastusest välja taotluse vastuvõtmise nõue, kuivõrd koduteeninduse puhul oleme palunud taotlejal või esindajal esmalt esitada taotlus koos vajalike dokumentidega ning vastavalt sellele oleme planeerinud koduteeninduse. Taotlejatele või nende esindajatele ei ole aga üheselt selge, millal PPA ametnik tuleb ja see on põhjustanud kaebusi. Põhjusi, miks koduteeninduse korraldamine võib aega võtta on erinevaid – näiteks inimene transporditakse ühest viibimiskohast teise. Tavaliselt jõutakse koduteenindus korraldada 1 kuu jooksul, kuid kuna see võib PPAst sõltumatutel põhjustel ka kauem aega võtta, teeme ettepaneku määrata õigusaktis 3 kuulise tähtaja. Kui meil oleks õigusaktis sätestatud konkreetne tähtaeg, saaksime ka näiteks PPA kodulehel esitada taotlejatele ja nende esindajatele selgemad	Mitte arvestatud Taotluse esitamise muudatus vajab täiendavat analüüsi, kuna puudutab haavatavat sihtrühma. Kõnesoleva eelnõu ettevalmistamisel ei ole muudatust analüüsitud ja sellega kaasnevat mõju hinnatud. Samuti ei ole muudatust kooskõlastamisele esitatud eelnõu versioonis. Eeltoodust tulenevalt ei ole võimalik eelnõule muudatust lisada. Koduteeninduse tähtaja saab kehtestada rakendusaktiga. Tuleme selle ettepaneku juurde tagasi rakendusakti menetlemisel. Tähtaja kehtestamise mõjude hindamiseks tuleb PPA-l esitada statistika senise koduteeninduse praktika ja tähtaja kohta aastate lõikes (mitu koduteenindust aastas, millise aja jooksul keskmiselt koduteenindus toimub).

suunised, juhtida nende ootusi ja paluda alustada dokumendi vahetamise protsessiga aegsasti.	
15. Seoses ITDS § 18^1 lg 1^1 muudatusega palume täpsustada, kas inimese poolt eesti.ee keskkonda sisselogimine ja sealt oma andmete näitamine on võrdsustatud isikusamasuse kontrollimisega.	Selgitus Mobiiltelefonist eesti.ee keskkonda sisselogimine ja ekraanile kuvatavate dokumendi andmete näitamine ei ole võrdsustatud isikusamasuse kontrollimisega. Isikusamasuse kontrollimise funktsionaalsuse kasutamiseks tuleb lisaks mobiilirakendusse sisselogimisele end täiendavalt autentida ja seejärel genereeritakse kasutajale ajutine ruutkood, mis on unikaalne võti ja luuakse vahetult enne andmete küsimist. Seletuskirja täiendatud.
16. Ettepanek ühtlustada kõik arhiveerimise ja kustutamise tähtajad ABIS põhimäärusega. Vastasel juhul võib esineda olukordi, kus andmekogu edastab andmestiku, aga ABIS pilti ei väljasta. Siinkohal tõstame esile, et arhiveerimise reeglistik eeldab olulisi arendusi iga seotud andmekogu poolt. ABIS-e arhiveerimise ja kustutamise tähtajad võiksid olla kooskõlas konkreetse liidestunud andmekogu tähtaegadega.	Arvestatud Eelnõu koostamisel ja andmekogu andmete säilitustähtaegade sätestamisel on lähtutud andmekogu ABIS põhimääruses sätestatud tähtaegadest, seaduses sätestatakse andmekogu andmete kõige pikem võimalik säilitustähtaeg, andmekategooriate kaupa on täpsemad säilitustähtajad reguleeritud ka edaspidi põhimääruses. Säilitustähtaja muudatused, mis võrreldes andmekogu ABIS kehtiva põhimäärusega muutuvad, tehakse edaspidi ka andmekogude põhimäärustes ja andmekogu ABIS põhimääruses.
17. Eelnõu järgi jõustuvad dokumendi sertifikaadi kehtivuse peatamise ja taastamise sätted 01.11.2025. PPA teeb ettepaneku viia antud muudatuse jõustumine kooskõlla hetkel kehtiva lepingu lõppemisega, milleks on 15. november 2025.	Arvestatud
18. Eelnõu järgi jõustub digitaalse isikutunnistuse väljaandmise lõpetamine 01.11.2025. PPA teeb ettepaneku lõpetada digitaalsete isikutunnistuste väljaandmine juba varem, kuna tegemist on dokumendi liigiga, mille kasutajate hulk on äärmiselt väike ning mille isikustamiseks kasutatav tehnoloogia on ajale jalgu jäänud. Soovituslikult võiks see tähtaeg olla 2024. aastal.	Arvestatud Säte jõustub üldises korras.
19. Kriminaalmenetluse seadustiku § 109^2 lõikes 5 asendatakse tekstiosa „andmekogu põhimäärus“ tekstiosaga „andmekogu ABIS põhimäärus, siis tuleks seda teha ka lõikes 4. Samuti tuleks lõikes 6 asendada tekstiosa „Andmekogus ABIS sisalduvad andmed“ tekstiosaga „Andmekogu ABIS andmed“. Lisaks märgime, et analoogsed muudatused	Selgitus Andmekogu ABIS lühend on antud KrMS § 99 lõikes 2. Seega tuleks konkreetse andmekogu puhul kasutada seaduse tekstis edaspidi korrektset lühendit. Suuremas osas seaduste revisjon mõistete ühtlustamiseks ei ole kõnesoleva eelnõu eesmärk.

tuleks teha ka teistes seaduste, sh PPVS, VTMS, PPVS, VRKS, VangS.	
20. Kriminaalmenetluse seadustiku § 109^2 lõike 5^1 muudatusega seoses märgime, et ABIS-e andmete säilitamise osas on kohtuekspertiisiseaduse §-s 21 oluliselt detailsem regulatsioon.	Selgitus Informatsioon võetud teadmiseks. KES § 21 sätestab ka süüteomenetluse biomeetriaregistri andmete säilitamise. Süüteomenetluse biomeetriaregistri ja andmekogu ABIS erineval teel võetud andmete säilitusaeg peab kattuma. Kõik andmekogu ABIS andmete säilitusajad on praegu sätestatud andmekogu ABIS põhimääruses (§ 39 ja § 41). Andmekogu volitusnormi sättes puudub vajadus kõigi andmekategooriate säilitusaegade üksikasjalikuks sätestamiseks. Piisab, kui seaduses sätestada andmete maksimaalne säilitustähtaeg. Andmekategooriate kaupa reguleeritakse andmete säilitustähtaeg andmekogu põhimääruses.
21. Väärteomenetluse seadustiku § 31^6 osas teeme ettepaneku ühtlustada kõik arhiveerimise ja kustutamise tähtajad ABIS põhimäärusega. Vastasel juhul võib esineda olukordi, kus andmekogu edastab andmestiku aga ABIS pilti ei väljasta. Arhiveerimise reeglistik eeldab olulisi arendusi iga andmekogu poolt.	Selgitus Eelnõu koostamisel ja andmekogu andmete säilitustähtaegade sätestamisel on lähtutud andmekogu ABIS põhimääruses sätestatud tähtaegadest, seaduses sätestatakse andmekogu andmete kõige pikem võimalik säilitustähtaeg, andmekategooriate kaupa on täpsemad säilitustähtajad reguleeritud ka edaspidi põhimääruses. Säilitustähtaja muudatused, mis võrreldes andmekogu ABIS kehtiva põhimäärusega muutuvad, tehakse edaspidi ka andmekogude põhimäärustes ja andmekogu ABIS põhimääruses.
22. Rakendusaktide kavand. Ettepanek muuta siseministri 18.12.2015 määruse nr 77 § 3 lõiget 4 järgnevalt: Taotlusele kirjutab alla taotleja, kinnitades taotluses esitatud andmete ja taotlusele lisatud dokumentide õigsust. Isiklikult esitatud taotluse võib kinnitada taotluse vastuvõtmiseks pädeva asutuse infotehnoloogilise vahendiga. Muudatuse vajadus on tingitud sellest, et kui kasutada tehnilist vahendit, näiteks tahvelarvuti ekraanil kasutamiseks mõeldud spetsiaalset pliiatsit, ei ole tegemist allkirjastamisega ning korrektsem oleks õigusakti tasandil sätestada vastav toiming kui „kinnitamine“ nagu teistes õigusaktides on varem sõnastatud.	Selgitus Rakendusaktide muutmisega tegeletakse põhjalikumalt enne seaduse muudatuste jõustumist. HÕNTE § 48 lõike 2 kohaselt peab seaduseelnõu seletuskirjale lisatud määruse eelnõu kavand olema ette valmistatud sellise täpsusega, et oleks võimalik hinnata rakendusakti vajalikkust, volitusnormi ulatust, kohast tasandit ja muid asjaolusid, mis on vajalikud volitusnormi sõnastuse ja rakendusakti vastavuse hindamiseks. Rakendusaktis terminite ühtlustamise eesmärki selles eelnõu menetlemise etapis ei ole. Tuleme ettepaneku juurde tagasi rakendusakti menetlemisel.
23. Rakendusaktide kavand. Ettepanek muuta siseministri 18.12.2015 määruse nr 77 § 16 lõiget 2. Kuna elamisloakaart on kohustuslik dokument ning pass on tulevikus üks taotleja	Selgitus Rakendusaktide muutmisega tegeletakse põhjalikumalt enne seaduse muudatuste jõustumist. HÕNTE § 48 lõike 2 kohaselt peab

valik dokumendikohustuse täitmiseks, teeme ettepaneku nende dokumendiliikide puhul ära kaotada arstitõendi esitamise kohustus. Kuivõrd nende isikute eest teeb samuti toiminguid sotsiaaltöötaja, siis saab sotsiaaltöötaja veenduda selles, et inimene ei ole võimeline isiklikult PPA-sse pöörduma. Sellisel juhul saaks lõiked 1 ja 2 kokku tõsta.	seaduseelnõu seletuskirjale lisatud määruse eelnõu kavand olema ette valmistatud sellise täpsusega, et oleks võimalik hinnata rakendusakti vajalikkust, volitusnormi ulatust, kohast tasandit ja muid asjaolusid, mis on vajalikud volitusnormi sõnastuse ja rakendusakti vastavuse hindamiseks. Rakendusaktis terminite ühtlustamise eesmärki selles eelnõu menetlemise etapis ei ole. Tuleme ettepaneku juurde tagasi rakendusakti menetlemisel.
24. Rakendusaktide kavand. Ettepanek muuta siseministri 18.12.2015 määruse nr 77 § 21 sõnastust „Taotleja, kes soovib, et tema dokument väljastataks tema esindajale, edastab dokumendi väljaandjale selle kohta kirjaliku volituse digitaalselt allkirjastatult või isiklikul ilmumisel.“. Volituse digitaalne allkirjastamine või isiklik ilmumine ei ole vajalik, kui dokumendi kättesaamist taotletakse notariaalse volikirja alusel. Muudatus tagab parema õigusselguse.	Selgitus Rakendusaktide muutmisega tegeletakse põhjalikumalt enne seaduse muudatuste jõustumist. HÕNTE § 48 lõike 2 kohaselt peab seaduseelnõu seletuskirjale lisatud määruse eelnõu kavand olema ette valmistatud sellise täpsusega, et oleks võimalik hinnata rakendusakti vajalikkust, volitusnormi ulatust, kohast tasandit ja muid asjaolusid, mis on vajalikud volitusnormi sõnastuse ja rakendusakti vastavuse hindamiseks. Rakendusaktis terminite ühtlustamise eesmärki selles eelnõu menetlemise etapis ei ole. Tuleme ettepaneku juurde tagasi rakendusakti menetlemisel.
25. Seletuskiri. Ettepanek sõnastada lk 1 p 6 ümber viisil, et me ei räägi millegi kaotamisest vaid vastavate teenuste lõpetamisest. Ettepanek täpsustada, et see muudatus puudutab just ID-1 formaadis isikut tõendavat dokumenti. Sertifikaadid on ka reisidokumentides. Või alternatiivina piisab ka sellest, kui täpsustada, mis sertifikaatidest jutt: sertifikaat autentimiseks ja sertifikaat digiallkirja andmiseks. Lisaks märgime, et punkti joonealuses märkuses peaks olema hanke ametlik nimetus ning seletuskirja tekstis läbivalt võiks olla kasutatud lühendit ID-1 leping.	Arvestatud Seletuskirjas sõnastus muudetud.
26. Seletuskiri. Markeerime lk 1 p 6 selgituse osas veel, et nii ETSI standardid, kui ka eIDAS rakendusmäärus seavad nõude, et on võimalik peatada ja/või kehtetuks tunnistada kas vahend (mille puhul ei saa ka sertifikaate kasutada) või sertifikaadid kiiresti ja tõhusalt. Neil, kellel puudub alternatiivne eID vahend, ei ole kiiret ja tõhusat viisi peatada ID1 formaadis eID vahendi kasutamist kui telefoni teel kaob ära teenus sertifikaatide peatamiseks. See on mure nii kehtiva lepingu kui ka uue lepingu puhul.	Arvestatud Seletuskirja täiendatud.

Lahendus peaks olemas olema, eIDAS vastavushindamine läbitud ja teavitatud vastavas koostöövõrgustikus, kui skeemi muudatus enne jõustumist. MKM/RIA pakutud lahendus või vähemalt kindel plaan selleks võiks olemas olla enne kui konkreetne kuupäev on seadusega määratud.	
27. Seletuskiri. Seletuskirja lk 7 viidatakse e-residendi digi-ID sertifikaatide kehtivuse peatamisele ja kehtetuks tunnistamisele. Kuna eelnõuga lõpetatakse sertifikaatide kehtivuse peatamine, siis kas on asjakohane sellele veel seletuskirjas viidata?	Arvestatud Seletuskirjas sõnastus muudetud.
28. Seletuskiri. RAB-i pädevuse osas lk 10 sõnastust tuleks täiendada, kuna on viidatud e-residendi digi-ID kehtivuse peatamisele, kuid dokumendi kehtivust ei peatata – hetkel saab vaid sertifikaate peatada.	Arvestatud Seletuskirjas sõnastus muudetud.
29. Seletuskiri. Kas on asjakohane seletuskirja lk 17 viidata ühele erasektori teenusele?	Selgitus Kuna seletuskirjas nimetatud erasektori teenus on Eestis nii era- kui avalikus sektoris väga ulatuslikult kasutusel ja see on EUTS § 21[1] kohaselt hinnatud kõrge usaldusväärsuse tasemega e-ID vahendiks, siis on asjakohane seletuskirjas see välja tuua.
30. Seletuskiri. Ettepanek muuta lk 19 sõnastust digitaalse isikutunnistuse kasutusvaldkondade kohta ning märkida üldistatumalt, et seda „võimalik kasutada üksnes elektroonilises keskkonnas“. Kuna hetkel pakutud loetelust on puudu krüpteerimise ja dekrüpteerimise funktsionaalsus.	Arvestatud Seletuskirja sõnastus muudetud.
31. Seletuskiri. Lk 21 viidatud garantiitaotlus vormistatakse vaid garantii korral, veamenetluses isik taotlust ei vormista. Lisaks märgime, et garantiitaotlus arhiveeritakse PPA-s ning inimesele seda ei anta. Inimese soovi korral saame kirjalikult kinnitada, et vastav taotlus on vormistatud. Samuti ei ole vaja alati dokumenti PPA-le anda ning see võib jääda ka inimese kätte.	Arvestatud Seletuskirja sõnastus muudetud.
32. Seletuskiri. Lk 22 väide, et võimalus pikema perekonnanime kandmiseks dokumenti tekib uue ID-1 lepingu rakendamisega, ei ole korrektne. Võimalus oleks ka praegustele ID kaartidele pikem nimi kanda aga piirang tuli seadusest. Kuna see mõjutab kõiki dokumente (sh passe), siis on oluline, et rakendustähtaeg on seotud uue ID-1 lepinguga.	Arvestatud Seletuskirja sõnastus muudetud.

33. Seletuskiri. Lk 41 on hinnatud muudatuste mõju ning märgitud, et pass kohustusliku dokumendina ja mRiigi kasutuselevõtt, puudutab vaid Eestis elavaid Eesti kodanikke. Kas mRiigi rakendust ei saa kasutada Eestis elamisloa alusel elavaid isikuid? Eelnõust vastavat piirangut ei ilmne. Samuti on meie hinnangul ekslik sõnastuses viidata passile, kui kohustuslikule dokumendile, kuna eelnõuga luuakse valikuvõimalus, millist dokumenti omada, aga ei muudeta passi kohustuslikuks dokumendiks.	Arvestatud Seletuskirja muudetud. Selgitame, et mRiik võetakse kasutusele siseriikliku lahendusena ning seda saavad kasutada ka Eestis elamisloa alusel elavad elanikud. Täpsustame, et eelnõu § 1 punktiga 3 muudetakse ITDS § 5 sätestatud dokumendikohustuse nõuet, millega muudetakse ka pass üheks võimalikuks kohustuslikuks dokumendiks. Eelnõu kohaselt peab edaspidi Eestis elaval Eesti kodanikul olema kohustusliku dokumendina kas pass või isikutunnistus.
34. Seletuskiri. Lk 41 on märgitud sertifikaatide peatamise lõpetamise mõju väikeseks, kuid PPA hinnangul sõltub mõju ulatus sellest, kas ja milline alternatiivne lahendus välja töötatakse dokumentide sertifikaatide kehtetuks tunnistamiseks.	Arvestatud Seletuskirjas sõnastus muudetud.
35. Ettepanek lisada eelnõusse riigilõivuseaduse muudatus, mis puudutab soodsamat riigilõivu isikut tõendava dokumendi taotlemisel, kui taotleja valib väljastuskohaks välise teenuseosutaja (Selveri). Riigi kulutused dokumendi väljastamise ja logistikaga jäävad ära, kui dokument väljastatakse välise teenuseosutaja poolt ja seega peaks ka riigilõiv olema inimesele väiksem. Muudatus on oluline, et mõjutada taotlejaid valima oma dokumendi väljastuskohaks Selver. Isikut tõendavate dokumentide Selveris väljastuse osas on prognoositust oluliselt madalam ning seetõttu ei ole see PPA teeninduste töökoormust positiivses suunas mõjutanud.	Mitte arvestatud Riigilõivu erisus pakutakse välja eraldiseisvas RLS muutmise eelnõus, mis on kavandatud jõustuma 01. jaanuaril 2025.
Rahapesu Andmebüroo	
1. Eelnõu § 1 punkti 11 kohaselt täiendatakse ITDS paragrahvi 9^2 lõikega 8^2, mille kohaselt võib Ettevõtluse ja Innovatsiooni Sihtasutuse töödelda e-residendi isikuandmeid selleks, et tuvastada ja maandada e-residendiga seotud riske. Seletuskirjas on muu hulgas riskide hindamisega seonduvalt selgitatud, et 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. Eelnõu seletuskirjast ei selgu täpsemalt kavandatavad	Arvestatud Seletuskirja täiendatud. E-residentide andmete töötlemine annab võimaluse tuvastada võimalikke e-residendi digi-ID väärkasutuse mustreid ja e-residendi profiilist tulenevaid riske. EIS-il tekib võimalus luua riskiaruandeid, anda järelevalveasutustele infot e-residendi digi-ID väärkasutuse kahtlusest ja tõhustada koostööd laiemalt. Ennekõike tähendab see koostööd EIS-i ja PPA vahel. PPA saab EIS-ilt laekunud info alusel viia läbi põhjaliku järelkontrolli.

tegevused, mida Ettevõtluse ja Innovatsiooni Sihtasutus riskide tuvastamise vaates edasiselt teeb, ehk milline on Ettevõtluse ja Innovatsiooni Sihtasutuse täpsem roll riskide hindamisel ja järeltegevustel, ja milline roll ja ootus on järelevalveasutustele siis, kui neile regulaarset infot edastatakse. Eeltoodust tulenevalt teeme ettepaneku seletuskirja vastavas osas täpsustada.	
2. Eelnõu § 1 punktiga 48 täiendatakse ITDS-i § 20^6 lõigetega 11 ja 12, millega luuakse õiguslik alus tagastada riskiriigi kodaniku e-residendi digi-ID taotlus läbi vaatamata ning volitatakse siseministrit kehtestama määrusega riskiriikide nimekirja ja riskiriigi kodanikule e-residendi digi-ID väljaandmise erisused. Seletuskiri toob, et riskiriikide määramisel lähtutakse RAB-i nimekirjast „Kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid“ (edaspidi RAB-i riskiriikide nimekiri), kohaldades erisusi, mis võtavad lisaks julgeolekukaalutlustele arvesse Eesti majanduslikke ja välispoliitilisi huve ning e-residentsuse programmi üldeesmärke. Eelnõu seletuskiri viitab, et RAB-i riskiriikide nimekiri on küll suure terrorismi rahastamise riskiga riikide kohta, kuid kuna rahapesu- ja terrorismi rahastamise risk on üldjuhul suur samades riikides, on muudatusega kaetud ka suure rahapesuriskiga riigid. Esmalt toome välja, et tegemist on küll RAB-i poolt avaldatud nimekirjaga, aga mitte RAB nimekirjaga, palume eeltoodud ebatäpsus seletuskirjas parandada. Riskiriik on eelnõu seletuskirja kohaselt defineeritud kui kõrgema rahapesu või terrorismi rahastamise riskiga riigi või sellise riigi kodanik, millega puudub Eestil justiits-, julgeoleku- või õiguskaitsealane koostöösuhe (ehk mõte on oluliselt laiem, kui RAB avaldataval nimekirjal). RAB-i avaldatav nimekiri ei kata kõiki riike näiteks sanktsioonide kõrvalehoidumise või rahapesu riskiriikide vaatenurgast. Seega sisu osas on ebaõige järeldus, et rahapesu ja terrorismi rahastamise risk on üldjuhul sama suur samades riikides. Koostöös õiguskaitseasutustega valminud ning RAB-i poolt avaldatud nimekirjas on kitsamalt toodud kõrgema terrorismi rahastamise riskiga riigid. RAB koos Kaitsepolitseiametiga vaatab seda nimekirja regulaarselt üle, kuid seda samuti ennekõike terrorismi rahastamise vaates. RAB	Arvestatud Seletuskirja tekst muudetud.

ei uuenda avaldatavat nimekirja riskiriikide FATF halli ja musta nimekirja lisamise põhjal. Eeltoodud arvesse võttes on meie hinnangul toodud regulatsioon ja lähenemine seaduses ebapiisav ning ei võimalda riigil kaitsta ennast selles eest, et e-residentsuse puhul arvestataks riskide tuvastamisel just konkreetsete isikute asukoha- ja päritoluriigi riskidega ning maandatakse efektiivselt ka rahapesu riske. Eeltoodust lähtudes teeme ettepaneku läheneda kõnealusele muudatusele seaduse eelnõus laiemalt ning kindlasti arvestada võimalike riskiriikide määratlemisel ka sanktsioonist kõrvalehoidumise ja rahapesu riskide vaatenurka laiemalt. RAB-i poolt avaldatud nimekiri riskiriikidest ei ole eeltoodud põhjendusel piisav ning riskide efektiivseks maandamiseks tuleks eelnõu kohaselt selgesõnalisena määratleda ka asutus, kes nimekirja riskiriikidest jooksvalt ajakohastab (selleks ei saa olla RAB). Juba rahapesu ja terrorismi rahastamise nimekirjade puhul näeb erisusi (RahaPTS § 3 punkt 18 ja https://finance.ec.europa.eu/financial-crime/high-riskthird-countries-and-international-context-content-anti-money-laundering-and-countering_en ning RAB-i ja õiguskaitseasutustega koostöös avaldatud kõrgema terrorismi rahastamise riskiga riikide nimekiri https://fiu.ee/media/841/download). Lisame täiendavalt, et 27.10.2023 avaldas FATF oma kõige värskema ajakohastatud nimekirja jurisdiktsioonidest, mille rahapesu ja terrorismi rahastamise režiimides tuvastati strateegilisi puudujääke (leitav: https://www.fatfgafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoringoctober-2023.html). Samuti avaldas Suurbritannia 22.01.2024 uuendatud teadaande rahapesu ja terrorismi rahastamise kõrge riskiga kolmandate riikidega seonduvalt (leitav: https://www.gov.uk/government/publications/money-laundering-advisory-notice-high-risk-thirdcountries--2).	
3. 12.06.2023 tagasisides isikut tõendavate dokumentide seaduse muutmise seaduse eelnõu väljatöötamise kavatsuses tõime välja, et puudub analüüs, kuidas majanduslikud kasutegurid Türgi ja Araabia Ühendemiraatide	Selgitus E-residentsuse programmi riskihaldus toimub läbi e-residentsuse nõukogu, kus lepitakse kokku riskide haldamise meetmed ja vajaduse korral täiendavad meetmed. E-residentsuse

puhul kaaluvad üles võimalikud julgeolekuriskid. Eelnõu seletuskirjast jätkuvalt vastav analüüs hetkel puudub.	nõukogu liikmeks on ka Rahandusministeeriumi asekantsler ja edaspidi on nõukogu liikmeks RAB esindaja. E-residentsuse riskiriikide nimekiri kooskõlastati enne VTK ja eelnõu kooskõlastamist e-residentsuse nõukogus, kuhu kuuluvad kõikide e-residentsuse programmiga seotud ministeeriumide ja riigiasutuste esindajad. Riik võtab Türgi ja Araabia Ühendemiraatide nimekirjast välja jätmisega teadliku riski. Järelevalveasutused monitoorivad pidevalt nii järelkontrollis ilmnevaid riske, kui julgeoleku olukorra muutumist ning riskide hindamise tulemusel on võimalik nimekirja muuta.
Siseministeeriumi infotehnoloogia- ja arenduskeskus	
1. mRiigi äpi sisend seletuskirjas ei peegelda praegust arusaama isikusamasuse kontrollimisest ning SMITi ei ole antud lahenduse planeerimisse kaasatud. Me ei tea ega pole olnud võimelised planeerima SK-s kirjeldatud muudatusi, ressurssi ja tehnoloogilist lahendust, mis võimaldaks SK-s kirjeldatud õiguslikku alust: "Muudatus annab mRiigi kaudu isikusamasuse kontrollimisele samaväärse õigusliku tähenduse, nagu on füüsilise dokumendi alusel isikusamasuse kontrollimisel." ABISe vaatest pole teada, kas teostatakse biomeetrilist päringut, milline on volüüm jne. mRiigi osas tuleb arvestada, et see toob kaasa lisainvesteeringuid. Põhjus selles, et meie ITteenuste puhul tähendab muudatus seda, et ITDAK ja ABIS peavad edasi toimima kahe erineva mudeli alusel: 1) nii senise e-riigi toimemudeli järgi, kus andmekogu on loodud menetluse toetamiseks ja päringuid teevad asutused (nn once-only põhimõte), kui ka 2) uue nn personaalriigi toimemudeli alusel, kus päringuid teeb inimene ise ehk piltlikult öeldes tuuakse senine ID-kaardi kasutamine otse vastu ITDAK-it ja ABIS-t (sisuliselt on see uus isikusamasuse kontrolli eesmärgil tehtav päring sama funktsionaalsus, mida eID kasutamisel täidavad TARA, DigiDoc-i ja muud sarnased eID vahendi kasutamist võimaldavad tarkvarad). Praegusel kujul ei ole ITDAK ja ABIS selliseks andmevahetuseks valmis, sest need ei ole sellel eesmärgil loodud. Ka tuleb arvestada sellega, et ükski nende andmekogude	<u>Arvestatud</u> Seletuskirja täiendava analüüsi- ja arendus-vajadusega täiendatud.

senistest eesmärkidest ära ei lange, mis tähendab seda, et mRiigi päring on IKT teenustele lisanduv koormus, mille võimaldamiseks tuleb teha investeeringuid. Suureneva päringute koormusega toimetulekuks ei piisa ainult lisaserverite soetamisest. Päringute mahtude suurendamiseks on vaja suurendada ka ITDAK-i ja ABIS-e rakenduste enda töökindlust ning võimsust. Samuti on vaja suurendada andmesidevõrgu läbilaskvuse võimsust ja seda eriti ABIS vaates, kuna biomeetrilised andmed liiguvad krüpteeritud kujul ja see on andmemahukam kui biograafiliste andmete liigutamine (juhul kui selle uue päringuga tahetakse ka foto kaasa saada). Need ei ole vajadused, mis saaksid oodata kuni päringute maht suurenema hakkab, vaid nende investeeringute tuleb tegeleda juba alustades – sest ITDAK-it teenindaval UUSIS-el on juba praegu aeg-ajalt aeglusega probleeme ja lisapäringute koormusele see enam vastu ei pea, ning andmeside koormuse suurendamine mõjutab väga otseselt kõigi SMIT-i poolt pakutavate teenuste töökindlust. Rahalise vajaduse suurusjärku oskame hinnata siis kui oleme saanud lähteülesande, kus kõige olulisem on info selle kohta, milline on maksimaalne eeldatav samaaegsete päringute arv ja millisele kellaajale ning nädalapäevale see tõenäoliselt langeb. St ei piisa sellest, kui palju päringuid arvuliselt aasta või kuu lõikes juurde tuleb, vaid hinnangu andmiseks on vaja teada just seda, kui palju päringuid võidakse samaaegselt teha, st kui suurele samaaegsele koormusele peavad meie teenused vastu pidama. Samuti on oluline teada, kuhu see ajaliselt tõenäoliselt langeb – et hinnata, kas koormus tõuseb nendel aegadel, mis on juba praegu tippajad või muudel aegadel. Selle alusel saame vaadata, kas planeeritavate tippaegadega samal ajal on koormus kõrge ka PPA teenindustes, piirikontrollis, Selverites, pankades jms, ning kas suurem koormus langeb töövälisele ajale ja vajaks ka SMIT-i meeskondade valvesolekut (praegu nende teenuste puhul töövälisel ajal reageerimise kohtustust meil ei ole, nii oleme PPA-ga kokku leppinud). Ka tuleks ilmselt mõelda sellele, et kas selline uutmoodi andmevahetus nõuab ka täiendavat eIDAS auditeerimist, kuivõrd lisandub nö uus võimalik ründevektor. Lisaks	

eeltoodule juhime tähelepanu, et § 9. Väljasõidukohustuse ja sissesõidukeelu seaduse muutmine - Muudatuse alusel võivad Sissesõidukeeldude riikliku registrit (skeeld) ja Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu (illegaal) ees oodata arendustegevused, mille maht selgib analüüsi käigus peale andmekogu omaniku, PPA, ärilise sisendi andmist arendusvajaduste osas.	
2. Ettepanek täiendada **eelnõu § 1 punkti 43** järgmise lausega: „Eesti teabevärava kaudu isikusamasuse kontrollimise eesmärgil dokumendiandmete pärimist võimaldatakse tehniliste võimaluste piires mahus, mis ei takista isikut tõendavate dokumentide andmekogu ja ABIS andmekogu vastutavatele töötlejatele pandud ülesannete täitmist.“ Praegu on küll ITDAK-i põhimääruses sätestatud, et kolmandatele isikutele antakse juurdepääs andmekogu andmetele mahus, mis ei takista vastutavale töötlejale pandud ülesannete täitmist, kuid kuna Eesti teabevärava kaudu tehtava päringu tegemist võib tõlgendada ka kui andmesubjekti enda poolt tehtavat päringut, siis ei pruugi ITDAK-i põhimääruses toodud piirang anda vastutavale töötlejale piisavat kaitset. Pealegi puudub sarnane säte ABIS põhimääruses.	<u>Arvestatud osaliselt</u> ITDAK-i põhimääruses on sätestatud piirang, mis kohaldub kõikidele kolmandatele isikutele ja on oma olemuselt laiem, kui ettepanekus esitatud sõnastus, mis kohalduks kitsalt riikliku mobiilirakenduse vahendusel tehtud päringutele. ITDAK-i põhimääruses olev alus tagab piisava kaitse vastutavale töötlejale, kui taoline piirang on ka tehniliselt teostatav. Samasisulise piiranguga täiendatakse ka andmekogu ABIS põhimäärust.
3. Ettepanek täiendada seletuskirja ja lisada mõjuhinnang ka selle kohta, et luuakse võimalus kontrollida füüsilises keskkonnas isikusamasust digitaalselt mRiigi kaudu. Meie hinnangul on sellel muudatusel oluline mõju riigiasutuste töökorraldusele ja riigi IKT teenustele, samuti teenusepakkujatele: Isikut tõendavate dokumentide andmekogu ja ABIS andmekogu ning nendega seotud tehniliste rakenduste, teenuste ja muude komponentide ülesehitus ning toimimine põhineb senisel e-riigi toimeloogikal, kus inimene esitab andmed ainult ühe korra ja andmekogust pärivad andmeid asutused, mitte andmesubjektid ehk inimesed ise (nn once-only põhimõte). Plaanitav muudatus võimaldada kontrollida füüsilises keskkonnas isikusamasust digitaalselt mRiigi kaudu loob uue võimaluse, kus nende andmekogude senistele funktsionaalsustele lisanduvad ka niinimetatud transaktsioonipõhised päringud, mida teevad inimesed ise. Selline muudatus erineb senisest e-	<u>Arvestatud</u> Seletuskirja punkti 7 on täiendatud, ettepanekus välja toodud mõju riigiasutuste töökorraldusele ja riigi IKT teenustele väljendub arendusvajaduses ja sellega kaasnevas kulus.

riigi toimeloogikast ja toob kaasa uue funktsionaalsuse, millega nende andmekogude tehnilistes lahendustes seni arvestatud ei ole ja seetõttu ei tule need andmekogud oma praegusel kujul uue vajadusega kaasneva koormusega toime. Kuigi ka praegu on andmesubjektil võimalik riigi teabevärava kaudu oma andmeid isikut tõendavate dokumentide andmekogust ja ABIS andmekogust kontrollida, ei ole praegusel juhul siiski tegemist transaktsiooni põhise päringuga, mistõttu ei saa praeguste päringute pinnalt hinnata tulevaste transaktsiooni põhiste päringute mahtu. Seetõttu tuleb plaanitava muudatuse rakendamiseks vaadata üle nii rakenduste endi toimeloogika kui ka rakendusi teenindav baastaristu, et tagada rakendustes ja taristus piisav võimsus muutunud vajaduste ja koormusega toimetulekuks. Selline muudatus vajab rahalist investeeringut. Samuti on muudatusel mõju teenusepakkujatele, kes plaanivad oma protsessides võimaldada mRiigi kaudu isikusamasuse tuvastamist füüsilises keskkonnas. Info teenusepakkujate valmisolekust selline teenus kasutusele võtta ning samuti info selle kohta, millises ajaraamis on teenusepakkujatel võimalik ja ka huvi selle teenuse kasutuselevõtmiseks vajalikud arendustööd teha, on oluline sisend ka SMIT-i hallatavates infosüsteemides vajalike arendustööde planeerimiseks.	
4. Ettepanek täiendada **seletuskirja punkti 7** muudatusega seotud kuludega seonduvalt ja sõnastada esimene lause järgmiselt: „Eelnõu rakendamine toob kaasa infosüsteemide arendamise kulud, kulud rakenduste võimsuse suurendamiseks ja kulud taristu (sh serverid ja andmesidevõrk) võimsuse suurendamiseks. Samuti võivad eelnõu rakendamisega kaasneda SMIT-ile täiendavad personalikulud ning kulud turvatestimisele. SMIT hindab arendusmahtu PPA esitatavate arendusvajaduste alusel ja kulud kaetakse SMIT-i eelarvest, välja arvatud kulud, mis on vajalikud, et luua võimalus kontrollida füüsilises keskkonnas isikusamasust digitaalselt mRiigi kaudu. Nende kulude katmine lepitakse kokku eraldi.“	Arvestatud Seletuskirja punkti 7 alapunkti 4 täiendatud.
5. Ettepanek täpsustada **seletuskirja puntki 7 alapunkti 4** selgitusega, et mRiigiga seotud muudatuse rakendamiseks on vaja suurendada	Arvestatud Seletuskirja täiendatud.

ITDAK-i ja ABIS andmekogu tehniliste rakenduste ning sellega seotud baastaristu (sh serverid ja andmesidevõrk) võimsust ning mahtu. Juhul kui uute päringute prognoositav tippkoormus langeb töövälisele ajale, võib tekkida vajadus ka täiendavate personalikude katmiseks, eriti uue lahenduse töösoleku algusfaasis. Samuti kaasnevad mRiigiga seotud muudatustega kulud turvatestimisele, mida SMIT-i eelarves praegu planeeritud ei ole. Kõigi vastavate kulutuste katmiseks planeeritakse raha SMIT-i eelarvesse. Kulude suurusjärgu hindamiseks on eelnevalt vaja sisulist lähteülesannet, kus muuhulgas on planeeritud päringu andmekoosseis, maksimaalne samaaegsete päringute arv ning prognoositav tippkoormuse aeg nädalapäevade ja kellaaegade täpsusega.	
6. Ettepanek täpsustada Eesti teabevärava kaudu isikusamasuse kontrollimise eesmärgil dokumendiandmete pärimiseks vajalike muudatuste jõustumisaega, sest SMIT-i IKT teenuste meeskondadel võimalik arendused töösse võtta mitte varem kui 2026. aasta alguses. Kuni 2026. aasta alguseni on asjassepuutuvate IKT teenuste meeskonnad juba hõivatud suures mahus uue ID1 lepingu rakendamisega seotud muudatustega ja muude etteplaneeritud arendusülesannetega. Kuna vastavad muudatused ja arendusülesanded on seotud ITDAK-i ja ABIS andmekogu tehniliste rakendustega, ei võimalda ka lisameeskondade kaasamine vajalikke arendustöid kiiremini töösse võtta.	<u>Arvestatud</u> Täpne jõustumisaeg selgub pärast lähteülesande valmimist.