



RAHANDUSMINISTEERIUM

Riigikogu
Rahanduskomisjon
rahanduskomisjon@riigikogu.ee

02.05.2024

1.1-10.1/2099-1

**Seisukohad krüptovaraturu
seaduseelnõu (SE 398) täiendamiseks**

Austatud komisjoni esimees

Käesoleva kirja lisas on esitatud Rahandusministeeriumi seisukohad (ettepanekud) krüptovaraturu seaduse eelnõu (SE 398) täiendamiseks.

Ettepanekute aluseks on rahanduskomisjonile esitatud huvirühmade arvamused, sealhulgas 16. aprillil rahanduskomisjoni avalikul istungil suuliselt esitatud ettepanekud.

Lugupidamisega

(allkirjastatud digitaalselt)

Mart Vörklaev
rahandusminister

Lisa:
Muudatusettepanekute loetelu

Thomas Auväärt
611 3633
Thomas.Auvaart@fin.ee
Endla 13 / 10122 Tallinn / 611 3558 / info@rahandusministeerium.ee / www.rahandusministeerium.ee /
registrikood 70000272

Muudatusettepanekute loetelu krüptovaraturu seaduse eelnõu (398 SE I) juurde

I Rahapesu ja terrorismi rahastamise tõkestamise seaduse muutmine

Lähtuvalt Pangaliidu ja FinanceEstonia ettepanekust seoses isikusamasuse kaugtuvastamise regulatsiooniga ning RAB-i palvest jätta välja dokumendihoidjate sobivusmenetlus, teeme ettepaneku muuta Riigikogu menetluses olevat krüptovaraturu seaduse eelnõu (398 SE I) teksti järgmiselt:

1. Teha eelnõus järgmised muudatused:

1.1. Täiendada § 55 pärast punkti 6 uute punktidega, muutes järgmiste punktide numbreid, järgmises sõnastuses:

„7) paragrahvi 14 täiendatakse lõikega 1¹ järgmises sõnastuses:

„(1¹) Krediidiasutus ja finantseerimisasutus peavad enne käesoleva seaduse §-s 31 sätestatud hoolsusmeetmete erisuste kohaldamist kehtestama turvalist isikusamasuse tuvastamist ja andmete kontrollimist tagavad protseduurireeglid, millega tõhusalt maandatakse ja juhitakse riske, mis seonduvad hoolsusmeetmete rakendamisega isikuga samas kohas viibimata.“;

8) paragrahvi 14 lõiget 4 täiendatakse pärast tekstiosa „lõike 1 punktis 2“ tekstiosaga „ja lõikes 1¹“;

***Selgitus:** Punktiga 7 täiendatakse RahaPTS § 14 lõikega 1¹. Lisatavas lõikes sätestatakse, et juhul kui krediidiasutus või finantseerimisasutus soovib RahaPTS § 31 lõikes 1 sätestatud olukordades isikusamasuse tuvastamist ja andmete kontrollimist teostada isikuga samas kohas viibimata, siis peab kohustatud isik enne hoolsusmeetmete rakendamist kehtestama protseduurireeglid, millega tõhusalt maandatakse ja juhitakse riske, mis seonduvad hoolsusmeetmete rakendamisega isikuga samas kohas viibimata.*

Järelevalveasutuste ja Euroopa Pangandusjärelevalve (EBA) juhustega arvestamise kohustust laiendatakse punktiga 8 ka nendele protseduurireeglitele, mis puudutavad isikusamasuse kaugtuvastamist. EBA kaugtuvastamise suuniste kohaselt krediidi- ja finantseerimisasutused peaksid kehtestama ja säilitama poliitika ja menetlused, et täita direktiivi (EL) 2015/849 artikli 13 lõike 1 punktidest a ja c tulenevaid kohustusi (Eesti õigusesse üle võetud RahaPTS §-dega 19-21) olukordades, kus klienti kaugtuvastatakse. See poliitika ja need menetlused peaksid olema riskitundlikud ning sisaldama vähemalt järgmist:

- a) sellise lahenduse üldkirjeldus, mille krediidi- ja finantseerimisasutused on kasutusele võtnud, et koguda, kontrollida ja dokumenteerida teavet kogu klientide kaugtuvastamise protsessi jooksul; see peaks hõlmama lahenduse omaduste ja toimimise selgitust;*
- b) olukorrad, kus saab kasutada klientide kaugtuvastamise lahendust, arvestades riskitegureid, mis on tuvastatud ja hinnatud direktiivi (EL) 2015/849 artikli 8 lõike 1 (Eesti õigusesse üle võetud RahaPTS §-ga 13) kohaselt ning kogu äritegevust hõlmavas riskihindamises, sealhulgas selliste kliendiliikide, toodete ja teenuste kirjeldus, mis sobivad kaugtuvastamiseks;*
- c) mis etapid on täielikult autonoomsed ja mis etapid nõuavad inimsekkumist;*
- d) kehtestatud kontrollid, millega tagatakse, et esimene tehing äsja registreeritud kliendiga sooritatakse alles siis, kui on kohaldatud kõiki esialgseid kliendi suhtes rakendatavaid hoolsusmeetmeid;*

- e) *sissejuhatus- ja regulaarsete koolitusprogrammide kirjeldus, et tagada töötajate teadlikkus ja ajakohased teadmised klientide kaugtuvastamise lahenduse toimimisest, seotud riskidest ning klientide kaugtuvastamise selliste riskide maandamise poliitikast ja menetlustest.*

1.2. Täiendada § 55 pärast punkti 7 (uues numeratsioonis punkt 9) uue punktiga, muutes järgmiste punktide numbreid, järgmises sõnastuses:

„**10)** paragrahvi 24 lõike 2 punkti 3 muudetakse ja sõnastatakse järgmiselt:

3) muule isikule, kes kohaldab käesolevas seaduses sätestatud hoolsusmeetmeid ja andmete säilitamise nõudeid või osaleb hoolsusmeetmete kohaldamisel ning kellel on lepinguline kohustus säilitada ja teha järelevalveasutusele kättesaadavaks hoolsusmeetmete kohaldamise käigus kogutud andmed.“;

***Selgitus:** Punktiga muudetakse RahaPTS § 24 lõike 2 punkti 3 sõnastust, täpsustades, et isik, kellele tegevus edasi antakse ei pea ise hoolsusmeetmet tervikuna kohaldama, vaid võib ka osaleda hoolsusmeetmete täitmisel. Muudatus on seotud isikusamasuse kaugtuvastamise regulatsiooni muudatustega, kuna selle hoolsusmeetme teostamisel on levinud väliste teenuspakkujate teenuste kasutamine. Kehtivas sättes sõnastatud hoolsusmeetmete täitmise nõue viitaks nagu hoolsusmeetmetega seotud ülesannet saab edasi anda üksnes kohustatud isikule, kuid see pole olnud sätte eesmärk. Muudatus võtab arvesse praktikat, mille kohaselt üleantav tegevus ei pruugi seisneda terve hoolsusmeetme teostamise üleandmisel vaid üksnes mõne etapi, tehnilise lahenduse või teenuse üleandmisel, mis toetab või osaliselt teostab hoolsusmeetmet. Lisaks täpsustatakse, et isik ise ei pea hoolsusmeetmetele sätestatud nõudeid täitma, vaid võib ka osaleda nende nõuete täitmisel, arvestades, et nõuete täitmise vastutus jääb seaduse kontekstis täielikult kohustatud isikule ja täpne sisemine jaotus nõuete täitmise teostamise osas on kohustatud isiku ja isiku, kellele hoolsusmeetmega seotud tegevus edasi antakse, vaheline küsimus. Muudetud sõnastus tagab suurema selguse, et § 24 lõike 2 punktis 3 on silmas peetud muid isikuid kui kohustatud isikuid, keda on juba mainitud sama lõike punktis 1. Lisaks sätestatakse täpsemalt, et lepingulised kohustused peavad tagama, et hoolsusmeetmetega kogutavad ja töödeldavad andmed peavad olema kättesaadavad järelevalveasutustele.*

1.3. Täiendada § 55 pärast punkti 14 (uues numeratsioonis punkt 17) uute punktidega, muutes järgmiste punktide numbreid, järgmises sõnastuses:

„**18)** paragrahvi 31 pealkirja muudetakse ja sõnastatakse järgmiselt:

„Krediidiasutuse, finantseerimisasutuse ja notari kohaldatavate hoolsusmeetmete erisused isikusamasuse kaugtuvastamisel“;

19) paragrahvi 31 lõike 1 sissejuhatav lauseosa muudetakse ja sõnastatakse järgmiselt:

„Krediidiasutus ja finantseerimisasutus on kohustatud isikusamasuse tuvastama ja andmeid kontrollima käesoleva seaduse § 14 lõikes 1¹ sätestatud nõuetele vastavate turvalist isikusamasuse tuvastamist ja andmete kontrollimist tagavate protseduurireeglite alusel ja kasutades käesoleva paragrahvi lõikes 3 nimetatud või lõikes 3¹ sätestatud nõuetele vastavat vahendit või teenust, kui hoolsusmeetmeid ei kohaldata isikuga samas kohas viibides ja kui:“;

20) paragrahvi 31 lõike 1 punkt 1 muudetakse ja sõnastatakse järgmiselt: „kliendi elu- või asukoht on Euroopa Majanduspiirkonna välises riigis;“;

21) paragrahvi 31 täiendatakse lõikega 1¹ järgmises sõnastuses:

„(1¹) Krediidiasutus ja finantseerimisasutus on kohustatud käesoleva paragrahvi lõikes 1 sätestatud kohustust täitma, kasutades lõikes 3 nimetatud vahendit või teenust, kui kliendi või juhuti tehingut tegeva isiku elu või asukoht on suure riskiga kolmandas riigis või riigis või jurisdiktsioonis, mis vastab käesoleva seaduse § 37 lõige 4 punktis 4 nimetatud tingimustele.“;

22) paragrahvi 31 lõiget 3 muudetakse ja sõnastatakse järgmiselt:

„(3) Kui hoolsusmeetmeid ei kohaldata isikuga samas kohas viibides võib isikusamasuse tuvastamiseks ja andmete kontrollimiseks kasutada:

1) e-identimise süsteemi, millest on teatatud Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.08.2014, lk 73–114) artikli 9 kohaselt ja mis vastab määruse artikli 8 lõike 2 punktides b või c sätestatud usaldusvääruse tasemele;

2) kvalifitseeritud usaldusteenust, mis vastab Euroopa Parlamendi ja nõukogu määruses (EL) nr 910/2014 sätestatud nõuetele.“;

23) paragrahvi 31 täiendatakse lõikega 3¹ ja järgmises sõnastuses:

„(3¹) Kui hoolsusmeetmeid ei kohaldata isikuga samas kohas viibides ja pole võimalik käesoleva paragrahvi lõikes 3 nimetatud süsteemi või teenust kasutada, peavad isikusamasuse tuvastamiseks ja andmete kontrollimiseks kasutatav vahend ja teenus tagama:

1) hoolsusmeetmete kohaldamisel kogutud andmete ja dokumentide õigsuse ja ajakohasuse;

2) kujutise, video, heli ja andmete kogumise ja säilitamise turvaliselt, arusaadavas vormis ja piisava kvaliteediga, mis tagab isiku üheselt äratuntavuse;

3) ühenduse ootamatul katkemisel või muude tehniliste puuduste ilmnemisel isikusamasuse tuvastamise ebaõnnestumise.“;

24) paragrahvi 31 lõiget 4 muudetakse ja sõnastatakse järgmiselt:

„(4) Kui hoolsusmeetmeid ei kohaldata isikuga samas kohas viibides ning isikusamasuse tuvastamiseks ja andmete kontrollimiseks kasutatakse e-residendi digitaalset isikutunnistust, siis tuleb kasutada samaaegselt ka mõnda teist käesoleva seaduse § 21 lõikes 3 nimetatud dokumenti.“;

25) paragrahvi 31 lõikest 5 jäetakse välja esimene lause;

26) paragrahvi 31 lõiget 6 muudetakse ja sõnastatakse järgmiselt:

„(6) Käesolevas paragrahvis sätestatud kohustuste täitmisel arvestab krediidasutus ja finantseerimisasutus pädeva järelevalveasutuse ja Euroopa Pangandusjärelevalve Asutuse asjakohastes juhendites ja suunistes sätestatuga.“;

27) paragrahvi 31 lõige 7 tunnistatakse kehtetuks;“;“.

Selgitus: Punktidega 18 kuni 20 muudetakse RahaPTS § 31 pealkirja ja lõiget 1. Kehtiv RahaPTS § 31 lõige 1 sätestab nõude kasutada isikusamasuse kaugtuvastamiseks ja andmete kontrollimiseks infotehnoloogilist vahendit. Muudatusega asendatakse viited infotehnoloogilistele vahenditele viidetega protseduurireeglitele, mis tagavad turvalist isikusamasuse tuvastamist ja andmete kontrollimist, ning eemaldatakse lausest viide ärisuhte loomisele. Sellega seonduvalt muudetakse paragrahvi pealkirja sõnastust, mis senini viitas infotehnoloogilistele vahenditele. Muudatuste eesmärk on RahaPTS § 31 fookus viia vahendite ehk tehnoloogia reguleerimiselt protseduuri reguleerimisele. Lisaks tagab uus sõnastus suurema selguse, et § 31 ei sätesta terviklikult hoolsusmeetmeid, vaid üksnes erisused RahaPTS §-des 21 ja 22 sätestatud isikusamasuse tuvastamise üldregulatsioonist, mida tuleb kohaldada juhul, kui hoolsusmeetmeid kohaldatakse isikuga samas kohas viibimata. Protseuur tervikuna peab tagama tõsikindla isikusamasuse tuvastamise, seega ei piisa üksnes usaldusväärse vahendi kasutamisest, vaid on vaja rakendada täiendavaid kogutavate andmete õigsust, piisavust ja ajakohasust tagavaid meetmeid ning andmeid ka hiljem kontrollida ja säilitada. Kasutatav vahend peab koosmõjus teiste meetmetega tagama piisava rahapesu ja terrorismi rahastamise riski maandamise ja seda saavutatakse läbi tervikliku protseduuri rakendamise.

Sätte muudetud sõnastus on paremas kooskõlas AMLD4¹ artikkel 13 lõike 1 punktiga a), mis kasutab sõnastust "turvalise kaug- või elektroonilise identifitseerimisemenditluse kaudu hangitud dokumentide, andmete või teabe abil". Viidatud AMLD4 punkt sätestab, et võimaluse korral võiks kasutada e-IDAS vahendit, asjakohast usaldusteenust või riiklikult reguleeritud, tunnustatud, heakskiidetud või aktsepteeritud identifitseerimismenetlust. Ka pärast muudatusi soodustatakse e-IDAS vahendite ja kvalifitseeritud usaldusteenuste kasutamist, võrreldes teiste kaugtuvastamise viisidega.

Vastavalt RahaPTS § 31 lõike 6 muudetud sõnastusele on eelduslikult turvaline protseduur Euroopa Pangandusjärelevalve (EBA) kaugtuvastamise lahenduse suunistega kooskõlas olev protseduur. Viide ärisuhte loomisele kustutatakse, kuna ärisuhte loomine on liiga kitsas alus käesolevas paragrahvis sätestatud hoolsusmeetmete kohaldamise kohustuse tekkeks. Vastavalt RahaPTS §-le 19 võib hoolsusmeetmete kohaldamise kohustus tekkida ka ärisuhte väliselt tehingute juhuti tegemisel või tehingute vahendamisel ja ärisuhte kestel, kui tekib kahtlus seni kogutud andmete piisavuses või tõlevastavuses või kui tekib rahapesu või terrorismi rahastamise kahtlus. Vahetu kontaktita ärisuhte haavatavuse tase sõltub kontaktide iseloomust ja hulgast kogu ärisuhte kestel mitte ainult ärisuhte loomise viisist, seega pole asjakohane käesolevas sättes viidata ärisuhte loomisele. Ka isikusamasuse tuvastamise üldsätted ehk RahaPTS §-d 21 ja 22 ei viita ärisuhte loomisele, kuna isikusamasuse tuvastamise vajadus võib ilmneda ka ärisuhte käigus või ärisuhteväliselt.

Lõike 1 punktist 1 jäetakse välja § 31 kohaldamise alus, mis lähtub kliendi päritolust. Põhiseaduse ja Euroopa Liidu põhiõiguste harta kohaselt ei tohiks kohaldada põhjendamatu erisusi, mis põhinevad üksnes isiku päritolul või etnilisel kuuluvusel. Rahapesu ja terrorismi rahastamise tõkestamise praktikas on osutunud oluliseks faktoriks residentsus. Kui isik on näiteks pärit kõrge riskiga kolmandast riigist, kuid suurema osa oma elust resideerunud madala riskiga kolmandas riigis, EL-i liikmesriigis või Eestis, siis pole selle isikuga seonduv geograafilineriskitase sama kõrge nagu näiteks seda on isikul, kes hoolsusmeetmete kohaldamise ajahetkel resideerub kõrge riskiga kolmandas riigis.

Punktiga 21 sätestatakse, et peab kasutama e-IDAS vahendit, mis vastavad usaldusväärse tasemele „kõrge“ või „märkimisväärne“, või kvalifitseeritud usaldusteenust, kui isiku elu- või asukoht on suure riskiga kolmandas riigis või riigis või jurisdiktsioonis, mis rahastab või toetab terrorismi või mille territooriumil tegutsevad Euroopa Liidu või ÜRO poolt kindlaks määratud terroristlikud organisatsioonid².

Suure riskiga kolmas riik on defineeritud RahaPTS § 3 punktis 18, mille kohaselt suure riskiga kolmas riik on AMLD4 artikli 9 lõike 2 alusel vastu võetud delegeeritud aktis nimetatud riik³. Tegemist on olukordadega, kus esineb edastamiskanaliga seotud kõrgemale riskile viitav asjaolu ja samal ajal tavapärasest kõrgemale geograafilisele riskile viitav asjaolu ning seejuures on tuvastatud, et geograafiline risk on otseselt seotud tavapärasest kõrgema rahapesu ja/või terrorismi rahastamise riskiga. Kui muud kaugtuvastamise edastamiskanaliga seonduvad kõrgemale riskile viitavad asjaolud ja geograafilisele riskile viitavad asjaolud toovad endaga kaasa kohustuse võtta kasutusele tugevdatud hoolsusmeetmeid, siis antud juhul

¹ Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ (ELT L 141, 05.06.2015, lk 73–117), muudetud direktiividega (EL) 2018/843 (ELT L 156, 19.06.2018, lk 43–74) ja (EL) 2019/2177 (ELT L 334, 27.12.2019, lk 155–163)

² RAB peab kahtlaste tehingute tunnuste juhendi lisana kõrgema terrorismi rahastamise riskiga riikide nimekirja, mille koostamisel on arvesse võetud rahvusvaheliste organisatsioonide hinnanguid ja raporteid koos ametiasutuste ohuhinnangutega. Nimekirja vaadatakse üle vähemalt kord aastas ja viimati uuendati 2023. aasta 6. septembril. Juhendid on kättesaadavad RAB-i kodulehel: <https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh>

³ Täiendav informatsioon suure riskiga kolmandate riikide kohta, koos lingiga delegeeritud aktile: https://finance.ec.europa.eu/financial-crime/high-risk-third-countries-and-international-context-content-anti-money-laundering-and-countering_en

ettepaneku koostajate hinnangul tugevdatud hoolsusmeetmetega pole võimalik piisavalt riski maandada ning seetõttu ei tohiks ärisuhet luua ega tehingut teha.

Punktidega 22 ja 23 muudetakse RahaPTS § 31 lõiget 3 ja lisatakse lõige 3¹. Lõikes 3 nimetatakse isikusamasuse kaugtuvastamiseks sobivad vahendid ja teenused ning lõikes 3¹ sätestatakse nõuded teistele isikusamasuse kaugtuvastamiseks ja andmete kontrollimiseks kasutatavale vahenditele või teenustele. Lõige 3¹ kohaldub juhul, kui ei kasutata lõikes 3 nimetatud vahendit või teenust. Lõigete sõnastus lähtub EBA kaugtuvastamise lahenduse suunistest. Muudatusega vähendatakse tehnoloogilist barjääri, arvestades võimalustega maandada riske teiste protseduuridega, võttes arvesse, et tehnilistele vahenditele kohalduvate nõuete täitmine ei tähenda tingimata, et riskid on asjakohaselt maandatud ega seda, et võiks seda vahendit kasutades luua või jätkata igat ärisuhet või teostada igat tehingut. Erinevate kaugtuvastamisvahendite kasutamise mõju riskitasemele on täpsemalt sätestatud §-des 36 ja 42.

RahaPTS § 31 lõikega 3 sätestatakse lahendused, mida võib kasutada isikusamasuse kaugtuvastamiseks. Eeskujuna on kasutatud EBA kaugtuvastamise lahenduse juhendit.

Punktis 1 on viidatud e-IDAS vahenditele, mis vastavad usaldusväärse tasemetele „kõrge“ või „märkimisväärne“. Kehtiva Rahandusministri 23. mai 2018. aasta määruse number 25 „Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise tehnilised nõuded ja kord“ (edaspidi kaugtuvastamise määrus) kohaselt peab olema kaugtuvastamiseks kasutatava vahendi usaldusväärse tase vähemalt kõrge, kuid EBA juhise kohaselt on piisavaks tasemeks ka märkimisväärne tase. Siiski pole märkimisväärse usaldusväärse tasemega vahendi kasutamine alati piisav ja seda peab kohustatud isik riske juhtides arvesse võtma.

Lisaks e-IDAS vahendile sobib kaugtuvastamisel kasutamiseks ka kvalifitseeritud usaldusteenus. Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 lõike 3 punktile 16 on usaldusteenus elektrooniline teenus, mida tavaliselt osutatakse tasu eest ja mis seisneb:

- a) e-allkirjade, e-templite või e-ajatemplite, registreeritud e-andmevahetusteenuste ning nende teenustega seotud sertifikaatide loomises, kontrollimises ja valideerimises; või
- b) veebisaidi autentimise sertifikaatide loomises, kontrollimises ja valideerimises; või
- c) e-allkirjade, e-templite või nende teenustega seotud sertifikaatide säilitamises.

Kvalifitseeritud usaldusteenus on teenus, mis vastab viidatud EL määruses sätestatud turvalisust ja kvaliteeti tagavatele nõuetele. Kvalifitseeritud usaldusteenuse osutajate üle teostatakse järelevalvet. Kaugtuvastamise määruse § 5 lõikes 1 on sätestatud, et teenusepakkuja infosüsteem peab võimaldama digitaalset allkirjastamist. Seega ka kehtiva õiguse kohaselt võib digitaalset allkirjastamist kasutada isikusamasuse tuvastamise protsessis, kuid sellel on üksnes toetav roll ning säte on sõnastatud nõudena kasutatavale infosüsteemile, kuid on jäetud täpsustamata, millal sellist võimalust võib või peab kasutama.

RahaPTS § 31 lõikes 3¹ on sätestatud alternatiivne võimalus teostada isikusamasuse kaugtuvastamist. Lõige sätestab kvalitatiivsed nõuded kasutatavale vahendile või teenusele, mida kasutatakse kaugtuvastamiseks. Kõik kolmes punktis sätestatud nõuded peavad olema üheaegselt täidetud, et saaks toimuda edukas seaduse nõuetele vastav isikusamasuse kaugtuvastamine ja andmete kontrollimine. Lõike 3¹ rakendamisel peab kohustatud isik ise hindama kasutatava teenuse või vahendi vastavust käesolevas lõikes sätestatud nõuetele või tuginema asjakohasele välisele ekspertarvamusele.

Punktis 1 sätestatu kohaselt peab vahend või teenus tagama hoolsusmeetmete kohaldamisel kogutud andmete ja dokumentide õigsuse ja ajakohasuse. See tähendab, et kasutatav vahend

või teenus integreerituna kohustatud isiku hoolsusmeetmete raamistikku tagab piisava kindlusega, et esitatud andmed ja dokumendid on õiged (sh ka piisavad) ja ajakohased ning hoolsusmeetmeid on võimalik sooritada. Vahendi või teenuse nõuetelevastavus sõltub ka riskidest, millega kohustatud isik kokku puutub ja protseduurireeglitest, mida ta rakendab. Muu hulgas peab vahend või teenus võimaldama tuvastada, kas klient või juhuti tehingut teostav isik osaleb hoolsusmeetmetes isiklikult ja et ei kasutataks kolmanda isiku lubamatut abi, ning kontrollida, kas esitatud andmed ja dokumendid on kooskõlas teisest allikast saadud informatsiooni või andmetega. Osaliselt kattub kõnealuses punktis olev nõue kaugtuvastamise määruse § 2 lõike 5 punktis 1 ning § 3 lõike 1 punktides 1, 3 ja 4 sätestatuga.

Punktis 2 on sätestatud, et kujutis, heli, video ja andmed peavad olema kogutud turvaliselt, arusaadavas vormis ja piisava kvaliteediga, mis tagab isiku üheselt äratuntavuse, ning neid tuleb ka selliselt säilitada. Andmete säilitamise nõuded tulevad RahaPTS-i §-st 47. Siinkohal ei reguleerita andmete säilitamist vaid vahendit või teenust, mida võib kasutada. Sarnased nõuded on sätestatud praegu kaugtuvastamise määruse paragrahvides 5–7.

Punktis 3 on sätestatud, et ühenduse ootamatul katkemisel või muude tehniliste puuduste ilmnemisel loetakse isikusamasuse tuvastamine ebaõnnestunuks. Infotehnoloogilise lahenduse puhul, eriti automatiseeritud lahenduse puhul, peaks tehniline lahendus seirama ühenduse kvaliteeti ja tunda ära, kui kvaliteet langeb liiga madalaks. Alternatiivselt peaks toimuma isiku poolt teostatuna samasisuline hindamine hoolsusmeetme teostamise ajal või vahetult pärast hoolsusmeetet. Samasisuline nõue on praegu kehtestatud kaugtuvastamise määruse § 3 lõike 1 punktis 2.

Punktiga 24 muudetakse RahaPTS § 31 lõiget 4. Kehtiv lõige 4 on sisuliselt üle kantud eelmisest RahaPTS-i terviktekstist. 2016. aastal kehtestatud sõnastuse kohaselt pidi välisriigi kodanik kasutama Eesti Vabariigi väljaantud digitaalseks isiku tõendamiseks ettenähtud dokumendi kõrval välisriigi pädeva asutuse väljaantud isikut tõendavat dokumenti. Muudatuste eesmärk oli luua isikusamasuse kaugtuvastamise võimalus Eestis, kuid selline võimalus loodi üksnes Eesti väljastatud digitaalse isikutunnistuse kasutamisel. Karmi regulatsiooni, sh kahe dokumendi esitamise nõude kehtestamist seaduses põhjendati eelnõu koostajate seisukohaga, et digi-ID-ga tuvastamine on FATF soovitus number 15 tähenduses uus tehnoloogia. Täpsemalt ei selgitatud, mis aspekt digi-ID tuvastamises uut tehnoloogiat hõlmas, kuid kõige uuem aspekt eelnõu koostamise ajal oli e-residentsus ja sellega seonduvad lahendused. Kaugtuvastamist ennast oli rahvusvaheline standardiseadja FATF pidanud oma 2003. aasta soovitusel uueks tehnoloogiaks. Samas seletuskirjas viidati 2012. aastal välja antud FATF-i soovitustele, mis asendasid eelmiseid ja mille kohaselt kaugteel teenuste pakkumine ei kvalifitseerunud enam uueks tehnoloogiaks. Digitaalne identiteet ja digitaalne isikutunnistus pole enam uued tehnoloogiad, kuid mitteresidentide äri, nõrgem kindlusastmega kaugtuvastamine ja teenuse pakkumine kliendiga samas kohas viibimata kätkevad endas jätkuvalt riske. 2017. aastal lubati kõigi e-IDAS vahendite kasutust kaugtuvastamiseks, kuid säilitati reegel, et välisriigi kodanik peab kasutama samaaegselt ka välisriigi pädeva asutuse väljaantud dokumenti. Selline üldistatud kodumaise e-IDAS vahendi eelistamine välismaistele pole põhjendatud. Samas e-residendi digitaalse isikutunnistuse kasutamise puhul saab kindlalt pidada isikusamasuse tuvastamist automaatselt tugevaks, kui kasutatakse ka mõnda teist dokumenti. Nimelt e-residentsuse eripäraks on see, et Eesti väljastab isikutunnistusi isikutele, kes pole Eesti kodanikud ega residentid. E-residendi kohta käivate andmete uuendamine on suures osas e-residendi enda vastutus ja riigil on, võrreldes oma kodanike ja residentide kohta käivate andmetega, piiratumad võimalused saada informatsiooni teistest allikatest. Seetõttu on jätkuvalt asjakohane tugeva isikusamasuse tuvastamisel kasutada samaaegselt teist dokumenti. E-residendi digitaalne isikutunnistus ilma täiendava dokumendita on jätkuvalt kasutatav üldregulatsiooni järgides, kui ei kohaldu RahaPTS § 31.

Kehtiv lõige 4 nõuab, et kasutataks isikut tõendavat dokumenti, kuid selline lahendus piirab

põhjendamatult kasutatavate dokumentide ringi. Mõnes riigis puudub universaalne isikut tõendav dokument ja paljudes riikides pole sellise dokumendi omamine kohustuslik. Seetõttu kasutatakse neis riikides teisi pädevate asutuste välja antud dokumente nagu näiteks reisidokumendid või sõiduki juhtimise luba. Isikusamasuse tuvastamist reguleeriv RahaPTS § 21 arvestab selliste eripäradega ja muudatusega ühtlustatakse kasutatavate dokumentide loetelu e-residentide kaugtuvastamisel kõigi teiste isikute isikusamasuse tuvastamiseks kasutatavate dokumentide loeteluga.

Punktiga 25 tunnistatakse kehtetuks RahaPTS § 31 lõike 5 esimene lause, mille kohaselt isikusamasuse tuvastamiseks ja andmete kontrollimiseks kasutatakse lisaks usaldusväärsest ja sõltumatust allikast pärit teavet. RahaPTS § 21 lõike 2 ja § 22 lõike 2 kohaselt kohustatud isik veendub isikusamasuse tuvastamiseks kogutud andmete õigsuses, kasutades selleks usaldusväärsest ja sõltumatust allikast pärit teavet. RahaPTS § 31 lõikes 1 olev RahaPTS § 21 lõiget 1 ja § 22 lõike 1 esimest lauset dubleeriv lause võib anda aluse tõlgendusele, mille kohaselt RahaPTS § 31 on terviklik eriregulatsiooni isikusamasuse tuvastamiseks juhul, kui seda tehakse samas kliendi või isikuga samas kohas viibimata. Selline tõlgendus on väär. RahaPTS § 31 ei ole terviklik eriregulatsioon, vaid tegemist on erisusega RahaPTS §-des 21 ja 22 sätestatud isikusamasuse tuvastamise üldregulatsioonist. Küsimustes, mida RahaPTS § 31 ei reguleeri, tuleb kohaldada §-des 21 ja 22 sätestatud.

Punktiga 26 asendatakse RahaPTS § 31 lõikes 6 olev volitusnorm viitega EBA asjakohastele juhenditele ja suunistele ning pädevate järelevalveasutuste juhenditele ja suunistele. Muudetud kujul lõige 6 kehtestab finantseerimisasutustele ja krediidasutustele kohustuse arvestada juhendites ja suunistes sätestatuga. Sarnased nõuded arvestada pädevate asutuste ja EBA juhendites ja suunistes tooduga on RahaPTS-is sätestatud ka § 14 lõigetes 4 ja 7, § 35 lõikes 1, § 37 lõikes 5 ning § 38 lõikes 4. Peaasjalikult on siinkohal peetud silmas EBA suunist: „Suunised klientide kaugtuvastamise lahenduste kohta kooskõlas direktiivi (EL) 2015/849 artikli 13 lõikega 1“, mis jõustus Eestis 29. mail 2023 Finantsinspektsiooni juhatuse otsusega⁴. Kuna EBA juhised ei ole mõeldud kohaldama kõigile finantsteenustele ja võib olla vajalik Eestis täiendavalt arvestada mõne siinse eripäraga, näiteks e-residentsusega, siis jäetakse võimalus RAB-ile ja FI-le kehtestada täiendavaid suuniseid ja juhendeid, millega turuosalisel peavad arvestama. Lõike 6 alusel kehtestatud määrus tunnistatakse kehtetuks.

Punktiga 26 tunnistatakse kehtetuks RahaPTS § 31 lõige 7, kuna muudetakse lõiget 6 ja senise määruse asemel reguleeritakse kaugtuvastamist täpsemalt seaduse tasandil koostöös pädevate asutuste ja EBA suuniste ja juhenditega.

1.4. Täiendada § 55 pärast punkti 15 (uue numeratsiooni järgi 28) uute punktidega, muutes järgmiste punktide numbreid, järgmises sõnastuses:

„**29)** paragrahvi 36 lõiget 2 täiendatakse punktiga 6 järgmises sõnastuses:

6) klient või tehingus osalev isik või tehing ise on seotud riigiga või jurisdiktsiooniga, kus usaldusväärsete allikate kohaselt on korruptsiooni või muu kuritegeliku tegevuse tase märkimisväärne või mille suhtes on kehtestatud sanktsioonid, embargo või nendega sarnased meetmed ja käesoleva seaduse §-s 31 sätestatud hooldusmeetmete erisuste rakendamisel ei kasutata § 31 lõikes 3 nimetatud vahendit või teenust.“;

30) paragrahvi 37 lõike 3 punktis 4 asendatakse sõna „rakendamist“ tekstiosaga „lõikes 3 nimetatud vahendit või teenust või muud Eesti või Euroopa Majanduspiirkonna lepinguriigi valitsusasutuse või muid avalikke ülesandeid täitva asutuse reguleeritud, tunnustatud, heakskiidetud või aktsepteeritud turvalist vahendit“;“.

⁴ Kättesaadav eesti ja inglise keeles Finantsinspektsiooni kodulehelt: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/suunised-klientide-kaugtuvastamise-lahenduste-kohta-kooskõlas-direktiivi-el-2015849-artikli-13>

Selgitus: Punktiga 29 täiendatakse eelnõud, lisades sinna RahaPTS § 36 lõike 2 täiendamine punktiga 6, mille kohaselt on tavapärasest kõrgem risk, kui on üheaegselt täidetud järgmised asjaolud:

- klient või tehingus osalev isik või tehing ise on seotud riigi või jurisdiktsiooniga, kus usaldusväärsete allikate kohaselt on korrupsiooni või muu kuritegeliku tegevuse tase märkimisväärne (RahaPTS § 37 lõike 4 punktis 2 sätestatud asjaolu) või mille suhtes on kehtestatud sanktsioonid, embargo või nendega sarnased meetmed (RahaPTS § 37 lõike 4 punktis 3 sätestatud asjaolu)⁵ ja;
- kaugtuvastamiseks pole kasutatud märkimisväärse või kõrge usaldusväärse tasemega e-IDAS vahendit või kvalifitseeritud usaldusteenust (RahaPTS § 37 lõike 3 punktis 4 sätestatud asjaolu).

Sellises olukorras esinevad üheaegselt kaks RahaPTS §-s 37 sätestatud riski suurendavat asjaolu: geograafilist riski suurendav asjaolu ja edastamiskanali seotud riski suurendav asjaolu. Rahapesu ja terrorismi rahastamine toimub tihti piiriülel ja on tuvastatud, et kõrgema tõenäosusega kasutatakse selles tegevuses jurisdiktsioon ja riike, mille institutsioonide võimekus võidelda korrupsiooni ja organiseeritud kuritegevusega on madal, Tihti on Eesti teenuspakkujatel piiratumad teadmised selliste riikide ja jurisdiktsioonide oludest ja tavadest, mis võib omakorda muuta keerulisemaks hoolsusmeetmete kohaldamise (ärisuhte eesmärgi mõistmine, keelebarjäär, teadmised riigi õigussüsteemist jne). Teiseks riskiteguriks on sanktsioonide ja nendega sarnaste meetmete vältimine, mille akuutsus on alates 2022. aastast kasvanud märkimisväärselt seoses sanktsioonirežiimide mahu kiire kasvuga. Sellised riigid ja jurisdiktsioonid teevad enamasti puudulikku koostööd Eesti pädevate asutustega kriminaalmenetlustes ja muudes menetlustes või ei tee üldse koostööd. Madal kuritegevusega võitlemise tase, piiratud asutustevaheline piiriülene koostöö ja soov vältida sanktsioonide tõstak selliste piiriüleste ärisuhte ja tehingute atraktiivsust kurjategijate silmis. Võimalusel peaksid kohustatud isikud kasutama tõsikindla isikusamasuse kaugtuvastamise teostamiseks e-IDAS vahendit või kvalifitseeritud usaldusteenust, kuid enamasti nende riikides ja jurisdiktsioonides resideeruvatel isikutel pole ligipääsu nendele teenustele ja vahenditele. Olukordades, kus kasutatakse mõnda muud vahendit või teenust, on vajalik tagada, et kohustatud isikud koguksid täiendavalt informatsiooni, analüüsiks seda ja vajadusel teavitaksid operatiivselt RAB-i, et RahaPTS §-s 38 sätestatud täiendavate hoolsusmeetmete rakendamiseks aidata kaasa rahapesu ja terrorismi rahastamise juhtumite ennetusele ja uurimisele.

Punktiga 30 muudetakse RahaPTS § 37 lõike 3 punkti 4 sõnastust. Sõnastus viiakse paremini kooskõlla AMLD4 lisa III punktis 2) alampunktis c) sätestatuga. Kehtiv RahaPTS § 37 lõike 3 punkt 4 viitab tervikuna RahaPTS §-s 31 sätestatud protseduurile, kuid direktiivi kohaselt on kindlalt kõrgemale riskile viitav asjaolu üksnes see, kui ärisuhte või tehingu puhul samas kohas viibimata ei võeta kaitseabinõuna kasutusele e-IDAS vahendit, kvalifitseeritud usaldusteenust või mõnda muud Eesti või Euroopa Majanduspiirkonna lepinguriigi valitsusasutuse või muid avalikke ülesandeid täitva asutuse reguleeritud, tunnustatud, heakskiidetud või aktsepteeritud turvalist, kaug- või elektroonilist identifitseerimismenetlust. Kehtiv viide tervele kaugtuvastamise protseduurile asendatakse konkreetsema viitega e-IDAS vahendile, mille usalsuväärsuse tase on „märkimisväärne“ või „kõrge“, kvalifitseeritud usaldusteenusele ja muule Euroopa Majanduspiirkonna lepinguriigi valitsusasutuse või muid avalikke ülesandeid täitva asutuse reguleeritud, tunnustatud, heakskiidetud või aktsepteeritud turvalisele vahendile või teenusele. Kui kasutatakse kaugtuvastamisel mõnda muud vahendit või teenust, siis on täidetud üks kõrgemale riskile viitav asjaolu. See tähendab, et mõne teise kõrgemale riskile viitava asjaolu esinemisel peab kohustatud isik kasutusele võtma täiendavad hoolsusmeetmed, et maandada tavapärasest kõrgemat riski ehk teisisõnu muudatuse kohaselt üksnes RahaPTS § 31 rakendamisest enam ei piisa, et tagada, et hoolsusmeetmete kohaldamisega samas kohas viibimata seonduvad tavapärarast tasemest kõrgemad riskid oleksid tõhusalt maandatud.

1.5. Täiendada § 55 pärast punkti 22 (uues numeratsioonis punkt 37) uue punktiga, muutes järgmiste punktide numbreid, järgmises sõnastuses:

⁵ Sanktsioonide osas on ülevaatlilik „EU Sanctions Map“. Kättesaadav: <https://www.sanctionsmap.eu/#/main>

„38) paragrahvi 46 lõike 2 punkti 3 muudetakse ja sõnastatakse järgmiselt:

„3) teabe, kui käesoleva seaduse § 31 rakendamisel ei ole võimalik § 20 lõikes 1 nimetatud hoolsusmeetmeid kohaldada;“.

***Selgitus:** Punktiga muudetakse RahaPTS § 46 lõike 2 punkti 3 sõnastust, asendades viite infotehnoloogilistele vahenditele viitega §-s 31 sätestatud, et arvestada RahaPTS §-s 31 tehtud muudatustega, mille tulemusel kasutatava vahendi asemel reguleeritakse isikusamasuse kaugtuvastamise protseduuri tervikuna.*

1.6. Täiendada § 55 pärast punkti 23 (uues numeratsioonis punkt 39) uue punktiga, muutes järgmiste punktide numbreid, järgmises sõnastuses:

„40) paragrahvi 47 lõiget 6 täiendatakse pärast sõna „videosalvestist“ sõnadega „koos ajatempliga“;“.

***Selgitus:** Punktiga täiendatakse RahaPTS § 47 lõiget 6 sõnadega „koos ajatempliga“ seoses kaugtuvastamise määruse kehtetuks tunnistamisega, kus see nõue oli senini sätestatud. Kehtivas määruuses on koos ajatempliga salvestamise nõue sätestatud § 6 lõikes 2. Ajatemplite salvestamise eesmärk on võimaldada tagantjärele kõiki protseduure taasesitada viisil, mis tagaks nende alusel õiguskaitseasutuste võimalikult kiire informeerimise ja ka informatsiooni sisulise asjakohasuse. Ajatempel tagab, et andmeid ei saa hiljem muuta ilma, et tuvastamise ajatempel ei muutuks.*

1.7. Muuta § 55 punkti 36 (uue numeratsiooni järgi 53) ja sõnastada järgmiselt:

„53) seadust täiendatakse §-dega 118⁴ ja 118⁵ järgmises sõnastuses:

„§ 118⁴. **Virtuaalvääringu teenuse pakkuja tegevusluba**

(1) Ettevõtja ei saa taotleda käesoleva seaduse alusel virtuaalvääringu teenuse pakkujateks tegevusluba alates 2024. aasta 30. detsembrist ja tegevusloa muutmist alates 2026. aasta 1. jaanuarist.

(2) Kui virtuaalvääringu teenuse pakkuja tegevusloa taotlus on Rahapesu Andmebüroole esitatud enne 2024. aasta 30. detsembrist ja Rahapesu Andmebüroo ei ole tegevusloa taotlust nimetatud kuupäevaks lahendanud, jätab Rahapesu Andmebüroo taotluse läbi vaatamata. Taotluse läbi vaatamata jätmise korral tagastab Rahapesu Andmebüroo esitatud dokumendid.

(3) Käesoleva seaduse alusel antud virtuaalvääringu teenuse pakkuja tegevusluba muutub kehtetuks käesoleva seaduse § 75 lõike 1 punkti 1 alusel, kui ettevõtja on saanud Finantsinspeksioonilt Euroopa Parlamendi ja nõukogu määruse (EL) 2023/1114 alusel krüptovarateenuse osutaja tegevusloa, või hiljemalt 2026. aasta 1. jaanuarist.

§ 118⁵. Virtuaalvääringu teenuse pakkuja omavahendite aruande audiitorkontrolli erisus

(1) Käesoleva seaduse § 72³ lõiget 4 ei rakendata, kui virtuaalvääringu teenuse pakkuja tegevusluba on muutunud kehtetuks § 118⁴ lõikes 3 sätestatud tingimustel.“;“.

***Selgitus:** Eelnõust jäävad välja § 118⁵ lõiked, mis käsitlevad virtuaalvääringu teenuse pakkuja dokumentide hoidja määramist, selleks läbi viidavat menetlust ning dokumentide säilitamist ja Rahapesu Andmebüroole väljastamist. Välja jäetav regulatsioon lisati kooskõlastusringis saadud RAB-i ettepanekuga seoses, mille kohaselt RAB-i hinnangul oli vaja muuta RahaPTS-i sätestades, et kõigil virtuaalvääringu teenuse pakkujatel, kelle tegevusluba muutub kehtetuks FI-le loa saamisega või tähtaja saabumisega, peavad andmeid säilitama 5 aastat pärast tegevusloa lõppemist. Rahandusministeerium sai pärast sätte lisamist RAB-ilt tagasiside, mille*

kohaselt RAB-ile tekitab dokumendihoidjate suhtes sobivusmenetluse teostamine liiga suure töökoormuse. Rahandusministeeriumi hinnangul ilma asjakohaste kontrollmeetmeteta pole mõistlik kehtestada teenuspakkujatele täiendavaid kohustusi, kuna sellisel juhul tõuseks seaduskuulekate teenuspakkujate halduskoormus, kuid need teenuspakkujad, kelle tõttu peaaesjalikult on vaja selliste nõuete kehtestamist seaduse tasandil, saaksid vältida nõuete täitmist.

1.8. Muuta eelnõu §-i 60 ja sõnastada see järgmiselt:

„(1) Käesoleva seaduse § 55 punktid 1, 4, 11, 13, 15, 17, 37, 42, 43, 46–48 ning § 56 jõustuvad 2026. aasta 1. juulil.

(2) Käesoleva seaduse § 55 punktid 2, 3, 5, 6, 9, 12, 14, 16, 28, 31–36, 39, 41, 45, 49–52 ja 54 ning § 57 jõustuvad 2024. aasta 30. detsembril.

Selgitus: Tulenevalt RahaPTS muudatusettepanekutest muutub eelnõu numeratsioon ning seoses sellega ka viited eelnõu § 55 vastavatele punktidele. Lisaks on sõnastuses muudetud lõikes I sätestatud jõustumiskuupäeva tulenevalt üleminekuperioodi pikendamisest 2026. aasta 1. juulini.

II Üleminekuperioodi pikendamine

Turuosalised on teinud ettepaneku pikendada EL määruse nõuetele üleminekuperioodi kuue kuu võrra ehk senise 12 kuu asemel tuleks ette näha 18-kuuline üleminekuperiood. Kuigi Rahandusministeerium lähtus eelnõu koostamisel 12-kuulise üleminekuperioodi sätestamisel Euroopa Väärtpaberijärelevalve Asutuse soovitusel rahandusministritele, leiame, et on põhjendatud pikema üleminekuperioodi rakendamine.

Ühtlasi juhime tähelepanu rahanduskomisjonile esitatud muudatusettepanekule nr 1. Esitatud muudatusettepanekust saame nõustuda „2026. aasta 1. jaanuari“ asendamisega „2026. aasta 1. juuliga“. Muudel juhtudel ei ole tähtaegade asendamine kooskõlas EL õigusega, kuna:

- liikmesriikidel ei ole võimalik edasi lükata krüptovaraturu EL määruse rakendamise tähtaega (kuna see ei ole seotud üleminekuperioodi pikendamisega). EL määrus rakendub vastavalt 2024. aasta 30. juunist või 2024. aasta 30. detsembris, sõltuvalt, kas tegemist on krüptovara emitendi või krüptovara teenuse osutajaga;
- eeltoodust tulenevalt ei ole asjakohane lükata edasi ka 2024. aasta 1. septembri tähtaega;
- liikmesriikidel ei ole võimalik edasi lükata küberturvalisuse EL määruse nõuete rakendamist. EL määrust tuleb rakendada hakata 2025. aasta 17. jaanuarist, kuid see kohaldub ainult sellistele krüptovaraturu osalistele, kes on saanud tegevusloa käesoleva seaduse (st EL määruse) alusel.

Kuna EL määrus lubab liikmesriikidel rakendada maksimaalselt 18-kuulist üleminekut, teeme ettepaneku muuta:

2. Asendada eelnõus läbivalt tekstiosa „2026. aasta 1. jaanuar“ tekstiosaga „2026. aasta 1. juuli“ vastavas käändes.

Selgitus: Muudatusettepanekuga pikendatakse uutele nõuetele üleminekuperioodi kuus kuud ehk turuosalised peavad hiljemalt 2026. aasta 1. juuliks minema üle EL määruse nõuetele või lõpetama tegevuse.

III Nõuded krüptovaraturu osalise nõukogule

Lähtuvalt turuosaliste ettepanekutest muuta krüptovarateenuse osutaja nõukogu moodustamise kohustus paindlikumaks, teeme ettepaneku:

3. Muuta § 7 lõike 2 teist lauset ja sõnastada see järgmiselt:

„Osaühingust krüptovarateenuse osutajal ei pea olema nõukogu, kui ta ei osuta Euroopa Parlamendi ja nõukogu määruse (EL) 2023/1114 artikli 3 lõike 1 punkti 16 alapunktis a või b nimetatud teenust.

***Selgitus:** Muudatusettepaneku kohaselt on osaühingust krüptovarateenuse osutaja nõukogu moodustamine kohustuslik vaid sellisel juhul, kui ta osutab EL määruse 2023/1114 artikli 3 lõike 1 punkti 16 alapunktis a või b nimetatud teenust. Alapunkt a puudutab seda teenust kui krüptovarateenuse osutaja hoiab ja haldab krüptovara kliendi nimel. Alapunkt b teenuse sisuks on see kui korraldatakse krüptovara kauplemisplatvormi (lihtsustatult krüptovara börsi). Ehk sel juhul võiks vastav hoolsuse määr kõrgem olla s.t. nõutav on alati nõukogu olemasolu.*

IV Finantsinspeksiooni ettepanekud

Lähtuvalt Finantsinspeksiooni esitatud arvamusest teeme ettepaneku:

4. Teha eelnõus järgmised muudatused:

4.1. Täiendada eelnõu § 10 lõiget 2 punktiga 4 ja sõnastada see järgmiselt:

„4) kinnituse, et krüptovaraturu osaline on analüüsinud talle sihtriigi õigusaktides kohalduvaid nõudeid ning ta on võimeline neid täitma.“.

4.2. Täiendada eelnõu § 10 lõike 5 punkti 2 pärast sõna „ülesehitus“ sõnadega „või muud võimalused“.

***Selgitus:** Eelnõu § 10 reguleerib krüptovaraturu osalise tegutsemist kolmandas riigis. Selleks on vaja Finantsinspeksiooni luba. Lõikes 2 on sätestatud, millised andmed ja dokumendid tuleb Finantsinspeksioonile loa saamiseks esitada. Muudatusettepaneku eesmärk on täpsustada, et esitada tuleb kinnitus selle kohta, et taotleja on analüüsinud talle vastava kolmanda riigi õigusaktides kohalduvaid nõudeid ning ta on võimeline neid täitma. Vastav kinnitus peab olema allkirjastatud taotleja esindaja poolt.*

Eelnõu § 10 lõikes 5 on sätestatud alused, mil Finantsinspeksioon võib keelduda kolmandas riigis tegutsemise loa andmisest. Sõnastusse on lisatud täpsustus, et lisaks sellele, et krüptovaraturu osalise finantsseisund või organisatsiooniline ülesehitus ei ole piisavad tegevuskavas nimetatud teenuste osutamiseks, ei pruugi ka muud võimalused olla piisavad teenuse osutamiseks kolmandas riigis. Arvestades, et alati ei ole võimalik kõiki olukordi ja situatsioone ette näha, siis vastav laiendus annab Finantsinspeksioonile laiemad alused loa andmisest keeldumiseks. Tuleb arvestada, et loa andmisest keeldumine on diskretsiooniotsustus, mis peab olema põhjalikult kaalutud ning põhjendatud.

4.3. Asendada eelnõu § 49 punktis 7 läbivalt tekstiosa „0,005–1 protsendiga“ tekstiosaga „0,005–2 protsendiga“.

***Selgitus:** Selleks, et tagada suurem paindlikkus järelevalvetasude määramisel seaduse rakendamise käivitusfaasis, on eelnõus (Finantsinspeksiooni seaduse muudatused) järelevalvetasu määramise protsendivahemikku muudetud.*

4.4. Asendada eelnõu § 49 punktis 8 esitatud lõikes 5⁵ tekstiosa „mis on arvatud Inspeksioonile“ tekstiosaga „mis on arvatud tema Inspeksioonile esitatud aruannete

andmetel“

Selgitus: Eelnõu sõnastusest on ekslikult välja jäänud täpsustus, et krüptovarateenuse osutaja klientide jaoks hoitavate vahendite summa aritmeetiline keskmine on arvatatud teenuseosutaja poolt Inspektsioonile esitatud aruannete andmetel.

4.5. Asendada eelnõu § 50 punktis 5 esitatud investeerimisfondide seaduse § 543² lõikes 2 sõna „juhtudel“ tekstiosaga „juhtudel, sealhulgas juhul, kui väikefondi valitseja jätab samas lõikes sätestatud kohustuse täitmata,“.

Selgitus: Väikefondi valitsejal on eelnõus esitatud IFS § 543² lõikes 1 sätestatu kohaselt kohustus teavitada Finantsinspektsiooni, kui ta ei ole kuue kuu jooksul pärast registreerimist fondi valitsemist alustanud (samuti sellest, kui ta oma tegevuse lõpetab). Sama paragrahvi lõike 2 kohaselt kustutab Finantsinspektsioon lõikes 1 nimetatud juhtudel ehk olukordades, kus väikefondi valitseja tegevust lõpetatakse või tegevusega ei ole alustatud, väikefondi valitseja registrist. Finantsinspektsioon on osundanud, et lisaks registrist kustutamisele väikefondi valitsejalt vastava teavituse saamisel, on oluline, et oleks ka selge norm väikefondi valitseja registrist kustutamiseks, kui viimane on lõikes 1 sätestatud kohustuse jätnud täitmata, kuid vastav asjaolu on ilmnenu järelevalve teostamisel. Et oleks üheselt selge, et Finantsinspektsioon kustutab väikefondi valitseja registrist, kui viimane ei ole kuue kuu jooksul registreerimisest arvates fondi valitsema asunud, vaatamata asjaolule, kas väikefondi valitseja on talle pandud teavitamiskohustust täitnud või mitte, tehakse IFS § 543² lõike 2 sõnastuses vastav täpsustus. Sama kehtib ka tegevuse lõpetamisel (kui teavitus on jäetud tegemata, kuid Finantsinspektsioon tuvastab väikefondi valitseja lõppemise, kustutab ta viimase registrist). Lõikesse 3 jäävad alused, mille puhul jääb Finantsinspektsioonile registrist kustutamisel kaalutusõigus.

V Audiitorkogu täiendav ettepanek

Lähtuvalt Audiitorkogu ettepanekust täpsustada eelnõu § 18 lõiget 2, teeme ettepaneku:

5. Muuta eelnõu § 18 lõiget 2 ja sõnastada see järgmiselt:

„(2) Audiitorettevõtja on kohustatud krüptovaraturu osalisega märkimisväärses seoses oleva isiku audiitorkontrollis vandeaudiitori aruande väljastamisel või kliendilepingu ülesütlemise korral teavitama kirjalikult Finantsinspektsiooni asjaoludest, mille tulemuseks on või võib olla käesoleva paragrahvi lõikes 1 sätestatud asjaolu“.

Selgitus: Muudatusettepaneku eesmärk on täpsustada eelnõu § 18 lõike 2 sõnastust nii, et oleks selge, et: 1) nõue kehtib krüptovaraturu osalisega märkimisväärses seoses oleva isiku audiitorkontrolli kohta (ehk informeerimiskohustus laieneb ka ülevaatuse läbiviimise puhul); 2) Finantsinspektsiooni tuleb teavitada vandeaudiitori aruande väljastamisel või kliendilepingu ülesütlemise korral.