

## Suunised, millega muudetakse suuniseid EBA/GL/2021/02,

---

milles käsitletakse kliendi suhtes rakendatavaid hoolsusmeetmeid ning tegureid, mida krediidi- ja finantseerimisasutused peaksid arvestama, kui hindavad üksikute ärisuhete ja juhutehingute rahapesu ja terrorismi rahastamise riski (edaspidi „rahapesu ja terrorismi rahastamise riskitegurite suunised“), ja mis on koostatud direktiivi (EL) 2015/849 artikli 17 ja artikli 18 lõike 4 alusel

# 1. Järgimis- ja teatamiskohustused

---

## Suuniste staatus

1. Käesolev dokument sisaldab määruse (EL) nr 1093/2010<sup>1</sup> artikli 16 kohaselt väljastatud suuniseid. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 alusel peavad pädevad asutused ja finantseerimisasutused võtma mis tahes meetmeid, et suuniseid järgida.
2. Suunistes esitatakse EBA seisukoht nõuetekohase järelevalvetava kohta Euroopa Finantsjärelevalve Süsteemis ehk kuidas tuleks ELi õigust konkreetses valdkonnas kohaldada. Suuniste adressaadiks olevad määruse (EL) nr 1093/2010 artikli 4 punktis 2 määratletud pädevad asutused peaksid suuniseid järgima, kaasates need sobival viisil oma tavadesse (nt muutes oma õigusraamistikku või järelevalveprotsesse) ka siis, kui suunised on ette nähtud eelkõige finantseerimisasutustele.

## Teatamiskohustus

3. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused teatama EBA-le hiljemalt 28.08.2024, kas nad järgivad või kavatsevad järgida käesolevaid suuniseid, või vastasel juhul mittejärgimise põhjused. Kui selleks tähtajaks teadet ei saada, peab EBA pädevat asutust nõudeid mitte täitvaks. Teated tuleb saata EBA veebilehel avaldatud vormil, märkides viite EBA/GL/2024/01. Teate peaksid saatma isikud, kes on asjakohaselt volitatud esitama oma pädeva asutuse nimel nõuete järgimise teateid. Nõuete järgimise staatuse mis tahes muutusest tuleb EBA-le teada anda.
4. Kooskõlas EBA määruse artikli 16 lõikega 3 avaldatakse teated EBA veebilehel.

---

<sup>1</sup> Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12).

## 2. Sisu, kohaldamisala ja mõisted

---

### Adressaadid

5. Käesolevad suunised on adresseeritud direktiivi (EL) 2015/849<sup>2</sup> artikli 3 punktides 1 ja 2 määratletud krediidi- ja finantseerimisasutustele ning määruse (EL) nr 1093/2010 artikli 4 punkti 2 alapunktis iii määratletud pädevatele asutustele.

---

<sup>2</sup> Euroopa Parlamendi ja nõukogu 20. mai 2015. aasta direktiiv (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist (ELT L 141, 5.6.2015, lk 73).

## 3. Rakendamine

---

### Kohaldamiskuupäev

6. Käesolevaid suuniseid kohaldatakse alates 30. detsembrist 2024.

## 4. Muudatused

---

### (i) Suuniste pealkirja muudatus

7. Suuniste pealkiri asendatakse järgmise tekstiga:

„Suunised EBA/GL/2021/02, milles käsitletakse kliendi suhtes rakendatavaid hoolsusmeetmeid ning tegureid, mida krediidi- ja finantseerimisasutused peaksid arvestama, kui hindavad üksikute ärisuhete ja juhutehingute rahapesu ja terrorismi rahastamise riski (edaspidi „rahapesu ja terrorismi rahastamise riskitegurite suunised“), ja mis on koostatud direktiivi (EL) 2015/849 alusel“

### (ii) Sisu, reguleerimisala ja mõistete muudatused

8. Punkti 12 sissejuhatav lause asendatakse järgmisega:

„Kui ei ole sätestatud teisiti, on direktiivis (EL) nr 2015/849 ja määruses (EL) 2023/1113 kasutatud ning määratletud mõistetel sama tähendus ka käesolevates suunistes. Lisaks kasutatakse suunistes järgmisi mõisteid.“

9. Punkti 12 alapunktid f ja m jäetakse välja.

### (iii) Muudatused: 1. suunis. Riskihinnangud: kõigi äriühingute peamised põhimõtted

10. Suunisesse 1.7 lisatakse järgmine punkt:

„d) kui äriühing toob turule uued tooted, teenused või äritavad või muudab neid oluliselt, sealhulgas kui ta võtab oma rahapesu ja terrorismi rahastamise tõkestamise süsteemide ja kontrollide raamistikus kasutusele uue tarnekanali või uuendusliku tehnoloogia, tuleks hinnata enne nende toodete, teenuste või äritavade turuletoomist rahapesu ja terrorismi rahastamise riskipositsiooni. Kui need tooted, teenused või äritavad mõjutavad äriühingu rahapesu ja terrorismi rahastamise riskipositsiooni oluliselt, peaks äriühing kajastama seda hinnangut kogu tegevuse riskihindamises, mis viiakse läbi kooskõlas direktiivi (EL) 2015/849 artikli 8 lõikega 2, ning oma poliitikates ja menetlustes.“

### (iv) Muudatused: 2. suunis. Rahapesu ja terrorismi rahastamise riskitegurite tuvastamine

11. Suunises 2.4 asendatakse punkt b järgmisega:

„b) Kas kliendil või tegelikult kasu saaval omanikul on sidemeid sektoritega, mis on seotud suurema rahapesu ja terrorismi rahastamise riskiga, näiteks teatud rahateenuste osutajate, suunises 9.20 ja 9.21 kirjeldatud krüptorahateenuse osutajate, kasiinode või väärismetallikauplejatega?“

## **(v) Muudatused: 4. suunis. Kliendi suhtes rakendatavad hoolsusmeetmed, mida peaksid kohaldama kõik äriühingud**

12. Suunises 4.29 asendatakse sissejuhatav lause järgmisega:

„4.29 Et täita oma direktiivi (EL) 2015/849 artikli 13 lõikest 1 tulenevaid kohustusi olukordades, kus ärisuhe algatatakse, luuakse või toimub vahetu kontaktita või kui juhutehingu tegemise ajal ei viibita samas kohas vastavalt EBA suunistele (EBA/GL/2022/15) klientide kaugtuvastamise lahenduste kohta kooskõlas direktiivi (EL) 2015/849 artikli 13 lõikega 1, peaksid äriühingud tegema järgmist:“

13. Suunis 4.35 asendatakse järgmisega:

„4.35 Kui väline teenuseosutaja on ELi-välises riigis asutatud äriühing, peaks äriühing tagama, et mõistab sellega seotud õiguslikke riske ja operatsiooniriski ning andmekaitse nõudeid ja maandab neid riske tõhusalt. Äriühing peaks samuti tagama, et tal on vajaduse korral viivitamata juurdepääs asjakohastele kliendiandmetele ja teabele, sealhulgas tegevuse edasiandmise lepingu lõpetamise korral.“

14. Suunise 4.60 punkt a asendatakse järgmisega:

„a) need erinevad tehingutest, mida äriühing tavaliselt eeldab selle alusel, mida ta teab kliendi, ärisuhte või kliendi kategooria kohta, kas summa, sageduse, keerukuse või muu sarnase teguri poolest, sealhulgas kui tehingud on tavapärasest suuremad või sagedamad või kui väikesi summasid hõlmavad tehingud on ebatavaliselt sagedad või kui tehakse järjest tehinguid, millel puudub ilmne majanduslik põhjendus, nt tehingud, mis on jagatud osadeks aruandluspiirangutest kõrvalehoidmiseks või mis kombineerivad ebatavalisi tehinguid tavapäraselt eeldatava käitumise ja muustriga, mida tõendavad kliendi tuvastamise menetluse käigus kogutud teave ja ärisuhte pidev jälgimine;“

15. Suunise 4.61 punkt a asendatakse järgmisega:

„a) mõistlike ja piisavate meetmete võtmine, et mõista tehingu tausta ja eesmärki, näiteks leides rahaliste vahendite või krüptovarade allika ja sihtkoha või otsides rohkem teavet kliendi tegevuse kohta, et leida tema sellise tehingu tegemise tõenäosus, ning“

16. Suunise 4.74 punkt b asendatakse järgmisega:

„b) kas tehinguid jälgitakse käsitsi või kasutatakse automaatset tehinguseiresüsteemi; suurt tehingumahtu või vältktehinguid töötlevad äriühingud peaksid kaalutlema automaatse tehinguseiresüsteemi kasutuselevõttu; ning“

17. Suunisesse 4.74 lisatakse järgmine punkt:

„d) kas on vaja kasutada täiustatud analüüsivahendeid, näiteks hajusraamatu või plokiahela analüüsivahendeid, võttes arvesse äriühingu tegevuse ning selle klientide individuaalsete tehingutega seotud rahapesu ja terrorismi rahastamise riski.“

## **(vi) Muudatused: 6. suunis. Koolitus**

18. Suunise 6.2 punkt c asendatakse järgmisega:

„c) kuidas tunda ära kahtlasi või ebatavalisi tehinguid ja tegevusi, võttes arvesse nende toodete ja teenuste eripära, ning mida sel juhul teha;“

19. Suunisesse 6.2 lisatakse järgmine punkt:

„d) kuidas kasutada tehingute ja ärisuhete seireks automaatsüsteeme, sealhulgas täiustatud analüüsivahendeid, ning kuidas tõlgendada nende süsteemide ja vahendite tulemusi.“

## **(vii) Muudatused: 8. suunis. Valdkondlik suunis seoses korrespondentsuhetega**

20. Suunise 8.6 punkt d asendatakse järgmisega:

„d) Respondentasutusel on oluline tegevus sektorites, mida seostatakse rahapesu ja terrorismi rahastamise suurema riskiga; näiteks tegeleb respondentasutus järgmisega:

- i. osutab olulises mahus rahasiirdeteenuseid;
- ii. tegeleb teatud rahasiirdeteenuse pakkujate või rahavahetuspunktide nimel;
- iii. tegeleb krüptovarateenuse osutajate nimel või koos nendega, v.a määrusega (EL) 2023/1114<sup>3</sup> reguleeritud krüptovarateenuse osutajad, kellele kohaldatakse direktiivis (EL) 2015/849 ettenähtud korrast leebemat rahapesu ja terrorismi rahastamise tõkestamise ja järelevalve korda või kellele ei kohaldata mingeid rahapesu ja terrorismi rahastamise tõkestamise kohustusi;
- iv. tegeleb olulise äritegevusega selliste krüptovarateenuse osutajate nimel, kelle ärimudel keskendub suunise 21.3 punktis d kirjeldatud toodete ja teenuste pakkumisele;
- v. tegeleb mitteresidente hõlmava äritegevusega või
- vi. tegeleb äritegevusega valuutas, mis ei ole tema asukohariigi valuuta.“

21. Suunisesse 8.6 lisatakse järgmine punkt:

„h) Krüptovarateenust pakkuva respondentasutuse IBAN-konto, kuhu laekub klientidelt raha ametlikus väärings<sup>4</sup>, on sellise äriühingu nimel ja omandis, kes ei ole krüptovarateenust pakkuva respondentasutus või ei ole teadaolevalt mingil viisil krüptovarateenust pakkuva respondentasutusega seotud.“

---

<sup>3</sup> Määrus (EL) 2023/1114, mis käsitleb krüptovaraturge ning millega muudetakse määrusi (EL) nr 1093/2010 ja (EL) nr 1095/2010 ning direktiive 2013/36/EL ja (EL) 2019/1937.

<sup>4</sup> Määruse (EL) 2023/1114 artikli 3 punktis 8 on ametlik vääring määratletud kui riigi ametlik vääring, mida emiteerib keskpank või muu rahaasutus.

22. Suunisesse 8.8 lisatakse järgmine punkt:

„d) Respondentasutus ei saa piisava kindlusega kontrollida, et tema kliendid ei asu suunise 8.8 punktis a nimetatud jurisdiktsioonides, sealhulgas oma klientide internetiprotokolli (IP) aadresside kontrollimise kaudu või muul viisil, kui seda nõuavad respondentasutuse poliitikad ja menetlused.“

23. Suunise 8.17 punktid a ja c asendatakse järgmiste punktidega:

„a) Koguda piisavat teavet respondentasutuse kohta, et mõista täielikult respondentasutuse tegevuse olemust, et leida, kui palju tekitab respondentasutuse tegevus korrespondentasutusele rahapesu suuremat riski. See peaks hõlmama meetmeid, et mõista ja hinnata respondentasutuse kliendibaasi olemust ning sellega kaasnevat riski, küsides vajaduse korral respondentasutuselt teavet tema klientide ja tegevuste kohta, mida respondentasutus teeb korrespondentkontolt, või asjakohasel juhul krüptovara liigi kohta, millega krüptovarateenust pakkuv respondentasutus teeb korrespondentkontolt tehinguid.“

„c) Hinnata respondentasutuste rahapesu ja terrorismi rahastamise tõkestamise kontrollid. See tähendab, et korrespondentasutus peaks hindama kvalitatiivselt respondentasutuse rahapesu ja terrorismi rahastamise tõkestamise kontrolliraamistikku, mitte lihtsalt hankima koopia respondentasutuse rahapesu ja terrorismi rahastamise tõkestamise poliitikest ja menetlustest. See hinnang peaks hõlmama ka olemasolevaid tehingute seirevahendeid, et tagada, et need vastaks respondentasutuse äritegevuse tüübile. See hinnang tuleks nõuetekohaselt dokumenteerida. Kooskõlas riskipõhise lähenemisviisiga peaks korrespondentasutus kaalutlema kohapealseid külastusi ja/või pistelist kontrolli, kui risk on eriti suur ja eelkõige kui korrespondentpanganduse tehingute maht on oluline, tagamaks, et respondentasutuse rahapesuvastaseid poliitikaid ja menetlusi rakendatakse tulemuslikult.“

## **(viii) Muudatused: 9. suunis. Valdkondlik suunis jaepankadele**

24. Suunis 9.3 asendatakse järgmisega:

„9.3. Lisaks käesolevate suuniste I jaotises esitatud riskiteguritele ja meetmetele peaksid pangad kaalutlema järgmisi riskitegureid ja meetmeid. Varahaldusteenuseid pakkuvad pangad peaksid lugema ka valdkondlikku 12. suunist, makse algatamise teenuseid või kontoteabe teenuseid pakkuvad pangad peaksid lugema ka valdkondlikku 18. suunist ja krüptovarateenust pakkuvad pangad peaksid lugema valdkondlikku 21. suunist.“

25. Suunis 9.16 asendatakse järgmisega:

„9.16 Kui panga klient avab ühiskonto või omnibus-konto, et hallata kliendi klientidele kuuluvaid rahalisi vahendeid või krüptovarasid, peaks pank rakendama täielikke hooldusmeetmeid, sealhulgas kohtlema oma kliendi kliente ühiskontol hoitavate rahaliste vahendite tegelikult kasu saavate omanikena ning kontrollima nende isikusamasust.“



26. Suunis 9.17 asendatakse järgmisega:

„9.17 Kui pank on kooskõlas käesolevate suunistega läbiviidud rahapesu ja terrorismi rahastamise riskihindamise põhjal kindlaks teinud, et ärisuhtega seotud rahapesu ja terrorismi rahastamise risk on suur, peaks ta rakendama direktiivi (EL) 2015/849 artiklis 18 sätestatud tugevdatud hoolsusmeetmeid, kui asjakohane.“

27. Suunises 9.18 asendatakse sissejuhatav lause järgmisega:

„9.18 Kui kliendi rahapesu ja terrorismi rahastamise üksiku riskihindamise alusel on ärisuhtega seotud risk siiski väike, võib pank riiklike õigusaktidega lubatud ulatuses rakendada lihtsustatud hoolsusmeetmeid, kui“

28. Suuniste 9.20–9.24 pealkiri asendatakse järgmisega:

„Krüptovaradega seotud teenuseid osutavad kliendid“

29. Suunised 9.20–9.23 jäetakse välja.

30. Lisatakse järgmised suunised 9.20 ja 9.21:

„9.20 Ärisuhete loomisel krüptovarateenust osutava kliendiga, kes ei ole määrusega (EL) 2023/1114<sup>5</sup> reguleeritud krüptovarateenuse osutaja, võib panku ohustada suurem rahapesu ja terrorismi rahastamise risk. Risk võib olla väiksem olukorras, kus selline teenuseosutaja on reguleeritud ja tema üle tehakse järelevalvet õigusraamistiku alusel, mis sarnaneb määruses (EL) 2023/1114 või direktiivis (EL) 2015/849 sätestatuga. Pangad peaksid enne nende klientidega ärisuhte loomist tegema seonduva rahapesu ja terrorismi rahastamise riskihindamise. Pangad peaksid selles arvesse võtma ka rahapesu ja terrorismi rahastamise riski, mis on seotud nende teenuseosutajate pakutavate või teenindatavate krüptovarade konkreetse liigiga.“

9.21 Suunises 9.20 kirjeldatud klientidega seotud rahapesu ja terrorismi rahastamise riski maandamiseks peaksid pangad kliendi suhtes rakendatavate hoolsusmeetmete osana tegema vähemalt järgmist:

- a) alustama kliendiga dialoogi, et mõista äritegevuse olemust ja selle tekitatavaid rahapesu ja terrorismi riske;
- b) lisaks kliendi tegelikult kasu saavate omanike tuvastamisele rakendama hoolsusmeetmeid ka kõrgemale juhtkonnale, kui need on muud isikud, sealhulgas võtma arvesse mis tahes negatiivset teavet;
- c) mõistma, kui palju rakendavad need kliendid oma klientide suhtes hoolsusmeetmeid kas juriidilise kohustuse tõttu või vabatahtlikult;
- d) leidma, kas klient on registreeritud või litsentsitud ELi/EMP liikmesriigis või ELi-välises riigis ning viimasel juhul võtma seisukoha selle ELi-välise riigi rahapesu ja

---

<sup>5</sup> Määrus (EL) 2023/1114, mis käsitleb krüptovaraturge ning millega muudetakse määrusi (EL) nr 1093/2010 ja (EL) nr 1095/2010 ning direktiive 2013/36/EL ja (EL) 2019/1937.

terrorismi rahastamise tõkestamise ja järelevalve korra piisavuse kohta vastavalt suunisele 2.11;

- e) leidma, kas kliendi pakutavad teenused kuuluvad kliendi registreerimis- või litsentsimisalasse;
- f) leidma, kas klient osutab muid teenuseid kui need, mille jaoks ta on krediidi- või finantseerimisasutusena registreeritud või litsentsitud;
- g) kui kliendi äritegevus hõlmab krüptovara väljastamist raha kogumise eesmärgil, näiteks tokenite esmapakkumisi, peaksid pangad kindlaks tegema, kas selline tegevus toimub kooskõlas kehtivate õiguslike nõuetega, ning kui asjakohane, kas seda reguleeritakse rahapesu ja terrorismi rahastamise tõkestamise eesmärgil vastavalt rahvusvaheliselt kokkulepitud standarditele, nt FATFi avaldatud standarditele.“

### **(ix) Muudatused: 10. suunis. Valdkondlik suunis e-raha väljastajatele**

31. Suunis 10.2 asendatakse järgmisega:

„10.2 Lisaks käesolevate suuniste I jaotises esitatud riskiteguritele ja meetmetele peaksid e-raha väljastavad äriühingud kaalutlema järgmisi riskitegureid ja meetmeid. Äriühingud, kelle volitus hõlmab äritoimingute osutamist makse algatamise teenusena ja kontoteabe teenusena, peaksid lugema ka valdkondlikku 18. suunist. Selles kontekstis võib asjakohane olla ka valdkondlik 11. suunis rahasiirdeteenuse pakujatele. Krüptovarateenust osutavad äriühingud peaksid lugema ka valdkondlikku suunist 21.“

### **(x) Muudatused: 15. suunis. Valdkondlik suunis investeerimisühingutele**

32. Suunis 15.1 asendatakse järgmisega:

„15.1 Direktiivi 2014/65/EL artikli 4 lõike 1 punktis 1 määratletud investeerimisühingud peaksid direktiivi 2014/65/EL artikli 4 lõike 1 punktis 2 määratletud investeerimisteenuste osutamisel või toimingute tegemisel lisaks käesolevate suuniste I jaotises sätestatule arvestama ka järgmisi riskitegureid ja meetmeid. Selles kontekstis võivad asjakohased olla ka valdkondlikud suunised 12 ja 21.“

### **(xi) Muudatused: 17. suunis. Valdkondlik suunis reguleeritud ühisrahastusplatvormidele**

33. Suunise 17.4 punkt i asendatakse järgmisega:

„i) Ühisrahastusteenuse osutaja võimaldab investoritel ja projekti haldajatel kasutada krüptovarasid oma maksetehingute arveldamiseks ühisrahastusplatvormi kaudu, kus selliste ülekannetega võib olla seotud rahapesu ja terrorismi rahastamise suurem risk suunise 21.3 punktis d kirjeldatud tegurite tõttu.“

34. Suunise 17.6 punkt b asendatakse järgmisega:

„b) investor või projekti haldaja kannab üle krüptovarasid, kusjuures selline ülekanne võib olla seotud rahapesu ja terrorismi rahastamise suurema riskiga suunise 21.3 punktis d kirjeldatud tegurite tõttu.“

35. Lisatakse järgmine 21. suunis:

## **(xii) „21. suunis. Valdkondlik suunis krüptovaratteenuse osutajatele**

21.1. Krüptovaratteenuse osutajad peaksid meeles pidama, et nad on haavatavad rahapesu ja terrorismi rahastamise riskide suhtes oma ärimudeli ja nende äritegevuses kasutatava tehnoloogia eriomaduste tõttu, mis võimaldavad neil krüptovarasid otsekohe kogu maailmas üle kanda ja teenindada kliente eri jurisdiktsioonides. See risk suureneb veelgi, kui nad töötlevad või hõlbustavad tehinguid või pakuvad tooteid või teenuseid, mis pakuvad suuremat anonüümsust.

21.2. Krüptovaratteenuse pakkumisel peaksid krüptovaratteenuse osutajad järgima I jaotise sätteid ja II jaotise sektoripõhiseid sätteid, kui need on krüptovaratteenuse osutaja tootevaliku seisukohast asjakohased.

## **Riskitegurid**

### **Toodete, teenuste ja tehingute riskitegurid**

21.3. Järgmised tegurid võivad **riski suurendada**.

- a) Krüptovaratteenuse osutaja tooted või teenused pakuvad suuremat anonüümsust.
- b) Toode võimaldab makseid kolmandatelt isikutelt, kes ei ole tootega seotud ja keda ei ole eelnevalt tuvastatud ega kontrollitud, kusjuures sellistel maksetel puudub ilmne majanduslik põhjendus.
- c) Toode ei sea otseseid piiranguid tehingute kogumahule või -väärtusele.
- d) Toode võimaldab teha tehinguid kliendi konto ja järgmiste vahel:
  - i. isehostitud aadressid;
  - ii. krüptovarakontod või hajusraamatu aadressid, mida haldab krüptovaratteenuste osutaja, nagu on määratletud suunises 9.20 või kelle suhtes kohaldatakse direktiiviga (EL) 2015/849 ettenähtud korrast leebemat rahapesu ja terrorismi rahastamise regulatiivset ja järelevalvekorda;
  - iii. vastastikune krüptoraha vahetusplatvorm või muud liiki detsentraliseeritud või hajutatud krüptovararakendus, mida ei kontrolli ega mõjuta juriidilised või füüsilised isikud (nimetatakse sageli detsentraliseeritud rahanduseks (DeFi));
  - iv. platvormid, mille eesmärk on varjata tehinguid ja hõlbustada anonüümsust, näiteks segamis- või trummelplatvormid;

- v. riistvara, mida kasutatakse krüptovarade vahetamiseks ametlike vääringute vastu või vastupidi (nt krüptorahaautomaadid) ja mis hõlmab sularaha või e- raha kasutamist, mille suhtes kohaldatakse direktiivi (EL) 2015/849 artikli 12 kohaseid erandeid või mis ei kuulu ELi regulatiivse ja järelevalvekorra alla.
- e) Tooted, mis hõlmavad uusi äritavasid, sealhulgas uusi edastuskanaleid, ja tehnoloogiaid, mille puhul krüptovarateenuse osutaja ei saa teabe puudumise tõttu usaldusväärselt hinnata rahapesu ja terrorismi rahastamise riski kooskõlas suunise 1.7 punktiga d.
- f) Kui krüptovara hulgiteenuse osutajal on nõrk kontroll teise krüptovarateenuse osutaja pakutava vahendusteenuse üle.
- g) Täiustatud analüüsivahenditega tehtud analüüsi tulemused näitavad, et riskitase on suurenenud.

#### 21.4. Järgmised tegurid võivad **riski vähendada**.

- a) Vähendatud funktsionaalsusega tooted, näiteks väikesed tehingumahud või -väärtused.
- b) Toode võimaldab tehinguid kliendi konto ja järgmiste vahel:
  - i. kliendi nimel olevad krüptovarakontod või hajusraamatu aadressid, mida haldab krüptovarateenuse osutaja;
  - ii. kliendi nimel olev krüptovarakonto või hajusraamatu aadress, mida haldab muu kui määrusega (EL) 2023/1114<sup>6</sup> reguleeritud krüptovarateenuse osutaja, kelle tegevus on reguleeritud väljaspool ELi õigusraamistiku alusel, mis on sama range kui määruses (EL) 2023/1114 sätestatu, ning kelle suhtes kohaldatakse rahapesu ja terrorismi rahastamise tõkestamise regulatiivset ja järelevalveraamistikku, mis on sama range kui direktiivis (EL) 2015/849 sätestatu;
  - iii. kliendi nimel olev pangakonto krediidasutuses, mille suhtes kohaldatakse rahapesu ja terrorismi rahastamise tõkestamise regulatiivset ja järelevalveraamistikku, mis on sätestatud direktiivis (EL) 2015/849, või muud ELi-välist õigusraamistikku, mis on sama range kui direktiivis (EL) 2015/849 sätestatu, või
- c) krüptovarateenuse osutaja kasutatavate maksekanalite või -süsteemide olemus ja ulatus on piiratud kinniste süsteemidega või süsteemidega, mille eesmärk on hõlbustada mikromakseid või valitsuselt isikule või isikult valitsusele tehtavaid makseid.
- d) Toode on kättesaadav üksnes piiratud ja määratletud kliendirühmale, näiteks krüptovara väljastanud ettevõtte töötajatele.

---

<sup>6</sup> Määrus (EL) 2023/1114, mis käsitleb krüptovaraturge ning millega muudetakse määrusi (EL) nr 1093/2010 ja (EL) nr 1095/2010 ning direktiive 2013/36/EL ja (EL) 2019/1937

## Kliendi isiku riskitegurid

### 21.5. Järgmised tegurid võivad riski suurendada.

#### a) Eelkõige seoses **kliendi olemusega**:

- i. mittetulundusühendus, mis on usaldusväärsete ja sõltumatute allikate põhjal seotud äärmusluse, äärmusliku propaganda või terroristide toetamise ja terroristliku tegevusega või on osalenud väärkäitumises või kriminaalses tegevuses, sealhulgas rahapesu või terrorismi rahastamise või korruptsiooniga seotud juhtumites;
- ii. ettevõtte, mis on direktiivi (EL) 2015/849 artikli 3 punktis 17 määratletud varipank või muud liiki varifirma;
- iii. hiljuti asutatud ettevõtte, mis töötleb suures mahus tehinguid;
- iv. seaduslikult registreeritud ettevõtte, mis töötleb suures mahus tehinguid pärast asutamisele järgnenud tegevusetuse perioodi;
- v. ettevõtte, millel on ärisuhe direktiivi (EL) 2015/849 artikli 3 punktis 15 määratletud kontserni muu(de) ettevõtte(te)ga, mis pakub (pakuvad) krüptovaradega seotud tooteid ja teenuseid;
- vi. ettevõtte või isik, kes kasutab IP-aadressi, mis on seotud pimevõrguga või anonüümset suhtlust võimaldava tarkvaraga, sealhulgas krüptitud e-kirjad, anonüümised või ajutised e-posti teenused ja VPNid;
- vii. haavatav isik, st isik, kes tõenäoliselt ei ole krüptovarateenuse osutaja tüüpiline klient, või isik, kellel on väga vähe teadmisi ja arusaamist krüptovaradest või seonduvast tehnoloogiast, mida tõendavad sobivuse/teadmiste testi tulemused või muu kliendiga seotud suhtlus, ning kes siiski otsustab teha sagedaid või suure väärtusega tehinguid, võib suurendada riski, et klienti kasutatakse rahamuulana.

#### b) Seoses **kliendi käitumisega**, olukorrad, kus klient:

- i. püüab avada krüptovarateenuse osutaja juures mitut krüptovarakontot ilma ilmse majandusliku põhjenduse või ärieesmärgita,
- ii. või kliendi tegelikult kasu saav omanik ei suuda või ei soovi esitada krüptovarateenuse osutaja nõudel vajalikku kliendi suhtes rakendatavate hoolsusmeetmete teavet, ilma et selleks oleks õiguspärast põhjust, kusjuures ta:
  - a) väldib teadlikult otsest kokkupuudet krüptovarateenuse osutajaga kas isiklikult või kaugsuhtluse teel;
  - b) püüab varjata vahendite tegelikku kasusaajat vahendajate või sidusettevõtjate, nt usaldus- või korporatiivteenuste pakkujate ärisuhtesse või tehingutesse kaasamise kaudu;

- c) ei anna krüptovarateenuse osutajale teavet või püüab teda eksitada krüptovarade kogumiseks kasutatud vahendite või krüptovarade päritolu või tehingute eesmärgi kohta;
- iii. kasutab ilmse majandusliku põhjendusega IP-aadressi või mobiilseadet, mis on seotud mitme kliendiga või on teadaolevalt seotud potentsiaalselt ebaseadusliku või kuritegeliku tegevusega; või kliendi krüptovarakontole on juurdepääs mitmelt IP-aadressilt, millel puudub kliendiga ilmne seos;
- iv. annab vastuolulist teavet, sealhulgas kui kliendi IP-aadress ei ole kooskõlas muu klienditeabega, nt teabega, mis on määruse (EL) 2023/1113 artikli 14 lõigete 1 ja 2 alusel vajalik ülekande tegemiseks, või kliendi alalise elukoha, registreeringu või äritegevuse teabega (nii ärisuhte loomise kui ka tehingu tegemise ajal), ning vahendite allikate või krüptovarade allika teave ei ole kooskõlas muu kliendi suhtes hoolsusmeetmete rakendamise käigus kogutud teabe või kliendi üldprofiilliga;
- v. kasutab aadressi, asukohta või IP-aadressi, mis on seotud krüptovarakontodega, mis on registreeritud eri kasutajatele ühe või mitme krüptovarateenuse osutaja juures;
- vi. muudab oma isikuandmeid või maksevahendeid sageli ilma ilmse põhjusega;
- vii. saab sageli isehallatavatele aadressidele või kannab neilt üle krüptovarasid summas, mis on veidi alla määruse (EL) 2023/1113 artikli 14 lõikes 5 ja artikli 16 lõikes 2 määratletud 1000 euro künnise, mis tingiks tehingust kasusaaja või selle algataja kontrolli;
- viii. märgib, et tema eesmärk on investeerida tokenite või krüptovarade või muu sellise toote esmapakkumisse, mis pakub ebaproportsionaalselt suurt tulu ja asub suure riskiga jurisdiktsioonis või millel on ilmsed pettustunnused või mida ei toeta määruse (EL) 2023/1114<sup>7</sup> kohaselt nõutav valge raamat;
- ix. tema käitumis- või tehingumustrid ei ole kooskõlas kliendi tüübi või riskikategooriaga või ei ole ootuspärased kliendi poolt krüptovarateenuse osutajale kas ärisuhte algul või selle vältel esitatud teabe põhjal. Sellised olukorrad hõlmavad klienti, kes
  - a) suurendab ootamatult ja ilmselge põhjusega krüptovarade ülekande või kombineeritud ülekannete mahtu või väärtust pärast vaiksemat perioodi;
  - b) teeb ebatavaliselt suure sageduse ja mahuga krüptovaratehinguid, mis ei ole kooskõlas ärisuhte eesmärgi ja olemusega ning millel puudub ilmne majanduslik eesmärk;

---

<sup>7</sup> Määrus (EL) 2023/1114, mis käsitleb krüptovaraturge ning millega muudetakse määrusi (EL) nr 1093/2010 ja (EL) nr 1095/2010 ning direktiive 2013/36/EL ja (EL) 2019/1937.

- c) suurendab tehingulimiiti määral, mis ei ole vastavuses kliendi deklareeritud sissetulekuga või ületab muul viisil eeldatavat tegevusmahtu;
- x. tal on ebatavalised käitumisviisid ja -mustrid, mida iseloomustavad seletamatud ülekanded hajusraamatu aadressidele/aadressidelt või krüptovarade kontodele/kontodelt mitmes jurisdiktsioonis ilma ilmse ärilise või õigusliku eesmärgita.
- xi. Krüptovarade ametlikeks väeringuteks ja vastupidi vahetamisel klient:
  - a) kasutab krüptovarakonto rahastamiseks mitmeid panga- või maksekontosid, krediitkaarte või ettemaksekaarte;
  - b) kasutab panga- või maksekontot või krediitkaarti, mis on kliendist erineva isiku nimel, kellega tal ei ole ilmselt seost;
  - c) kasutab teatud jurisdiktsioonis asuvat panga- või maksekontot, mis ei ole kooskõlas kliendi esitatud aadressi või asukohaga;
  - d) kasutab mitmeid makseteenuste pakkujaid;
  - e) taotleb korduvalt krüptovarade vahetamist sularaha või anonüümse e- raha vastu või vastupidi;
  - f) kasutab kahte plokiahelat ühendavaid protokolle, et vahetada krüptovarasid teiste krüptovarade vastu teises võrgus, näiteks Monero, Zcash jms;
  - g) kasutab eri asukohtades asuvaid krüptorahaautomaate vahendite korduvaks ülekandmiseks pangakontole;
  - h) kannab krüptovarateenuse osutaja juurest krüptovarad edasi isehallatavale aadressile kohe pärast krüptovarade deponeerimist või vahetamist erinevate krüptovarade vastu krüptovarateenuse osutaja juures;
- xii. investeerib või vahetab krüptovara, mille ta on laenanud vastastikuse või muu laenuplatvormi kaudu, mis ei kuulu määruse (EL) 2023/1114 või muu asjakohase õigusraamistiku kohaldamisalasse ELis või väljaspool ning on eelkõige detsentraliseeritud või hajus rakendus, mille üle puudub mis tahes juriidilisel või füüsilisel isikul kontroll või mõju;
- xiii. saab või saadab otseselt või kaudselt krüptovarasid, mis on seotud pimevõrgu või ebaseadusliku tegevusega;
- xiv. investeerib või vahetab krüptovarasid, mis pakuvad ise suuremat anonüümsust, või saab krüptovarasid, millega on tehtud anonüümsust suurendavaid toiminguid, eelkõige protsesse, mis varjavad tehingut hajusraamatu tehnoloogia abil, või millel on muid omadusi, mis sarnanevad suunise 21.5 punktis a nimetatud omadustega;

- xv. saab korduvalt krüptovarasid järgmistelt kontodelt/aadressidelt või saadab neid järgmistele kontodele/aadressidele:
- a) krüptovarakonto, mida haldab krüptovarateenuse osutaja, kes ei kuulu määruse (EL) 2023/1114 või muu asjakohase õigusraamistiku kohaldamisalasse ELis või väljaspool või kellele kohaldatakse rahapesu ja terrorismi rahastamise tõkestamise regulatiivset ja järelevalveraamistikku, mis on leebem kui direktiivis (EL) 2015/849 sätestatud raamistik;
  - b) mitu isehallatavat aadressi või mitu krüptovarakontot, mida haldavad samad või eri krüptovarateenuse osutajad, ilma ilmse majandusliku põhjendusega;
  - c) äsja loodud või varem mitteaktiivne krüptovarakonto või kolmanda isiku valduses olev hajasraamatu aadress;
  - d) isehallatavad aadressid detsentraliseeritud platvormidel, mis hõlmavad nn segistite (*mixers, tumblers*) ja muude privaatsust soodustavate tehnoloogiate kasutamist, mis võivad varjata hajasraamatu aadressi ja tehingu rahaliste vahendite allikaga seotud finantsajalugu, kahjustades seega krüptovarateenuse osutaja suutlikkust tunda oma kliente ning rakendada tõhusaid rahapesu ja terrorismi rahastamise tõkestamise süsteeme ja kontrole;
  - e) krüptovarakonto, millele järgneb lühikese aja jooksul pärast krüptovarateenuse osutajaga liitumist vara kontolt väljavõtmine või ülekandmine ilma ilmse majandusliku põhjendusega;
  - f) krüptovarakonto, mis on sageli alla määratletud künnise või isehallatavale aadressile suunatud ülekannete korral alla määruse (EL) 2023/1113 artikli 14 lõikes 5 ja artikli 16 lõikes 2 määratletud 1000 euro künnise;
  - g) krüptovarakonto, jagades tehingud mitmeks tehinguks, mis saadetakse smurfimistehnika abil mitmele hajasraamatu aadressile;
- xvi. klient näib kasutavat tehnoloogilisi probleeme või rikkeid enda kasuks;
- xvii. klient selgitab, et krüptovarateenuse osutajale ülekantud krüptovarad on saadud kaevandamise või preemiade kogunemise kaudu, kuid need preemiad ei näi olevat proportsionaalsed selliste tegevuste kaudu loodud krüptovaradega.

#### 21.6. Järgmised tegurid võivad **riski vähendada**.

- a) Klient on varasemate krüptovaradega tehtud tehingute korral täitnud määruses (EL) 2023/1113 sätestatud ning rahaliste vahendite ja teatavate krüptovarade



ülekannete kuritarvitamise vältimist käsitlevate EBA suuniste <sup>8</sup> punktis 4 täpsustatud teavitamisnõudeid ning on esitanud teavet, mis võimaldab klienti tuvastada või teda kahtluse korral kontrollida.

- b) Kliendi varasemad krüptovaratehingud ei ole olnud kahtlased ega problemaatilised ning soovitatav toode või teenus vastab kliendi riskiprofiilile.
- c) Klient taotleb vahetust ametlikku vääringsusse või ametlikust vääringust ning kas rahaliste vahendite allikas või sihtkoht on kliendi enda pangakonto krediidasutuses, mis asub krüptovaratteenuse osutaja hinnangul väikese riskiga jurisdiktsioonis.
- d) Klient taotleb vahetust ja krüptovara allikas või sihtkoht on kliendi enda krüptovarakonto või hajusraamatu aadress, mida haldab kas määrusega (EL) 2023/1114 reguleeritud krüptovaratteenuse osutaja või muu krüptovaratteenuse osutaja, kes ei ole määrusega (EU) 2023/1114 reguleeritud, kuid kes on reguleeritud ja kelle üle teostatakse järelevalvet väljaspool ELi õigusraamistiku alusel, mis on sama range kui määruses (EL) 2023/1114 sätestatu, ning kelle suhtes kohaldatakse sama rangeid rahapesu ja terrorismi rahastamise tõkestamise nõudeid kui direktiivis (EL) 2015/849 sätestatud ning kes on krüptovaratteenuse osutaja poolt valgesse nimekirja kantud või muul viisil hinnatud väikese riskiga teenuseosutajaks.
- e) Klient taotleb vahetust ja kas krüptovarade allikat või sihtkohta seostatakse väikese väärtusega maksetega kaupade ja teenuste eest krüptovarakontole/-kontolt või hajusraamatu aadressile/aadressilt, mille kohta ei ole negatiivset teavet.
- f) Klient teeb ülekandeid kahe krüptovaratteenuse osutaja vahel, kes on mõlemad reguleeritud määrusega (EL) 2023/1114 või kellest üks on määrusega (EL) 2023/1114 reguleeritud ja teine reguleerimata, kuid teise suhtes kohaldatakse kas ELi regulatiivset ja järelevalvekorda või muud õigusraamistikku, mis on sama range kui määruses (EL) 2023/1114 sätestatu, ja sama rangeid rahapesu ja terrorismi rahastamise tõkestamise nõudeid kui direktiivis (EL) 2015/849 sätestatud nõuded.

### Riiklikud või geograafilised riskitegurid

#### 21.7. Järgmised tegurid võivad riski suurendada.

- a) Kliendi rahalised vahendid, mida ta vahetab krüptovaradeks, tulenevad tema isiklikest või ärisidemetest jurisdiktsioonidega, mis on seotud rahapesu ja terrorismi rahastamise suurema riskiga.
- b) Krüptovarakonto või hajusraamatu aadress, kust varad pärinevad või kuhu need kantakse, on seotud jurisdiktsiooniga, mis on seotud suurema rahapesu ja

---

<sup>8</sup> Suunised rahaliste vahendite ja teatavate krüptovarade ülekannete kuritarvitamise vältimiseks rahapesu ja terrorismi rahastamise eesmärgil vastavalt määrusele (EL) 2023/1113, [... sisestada siia vastuvõetud suuniste number, praegu konsulteerimisel (EBA/CP/2023/35)]

terrorismi rahastamise riskiga, või jurisdiktsioonidega/piirkondadega, kus teadaolevalt rahastatakse või toetatakse terroristlikku tegevust või kus teadaolevalt tegutsevad terroriakte toimepanevad rühmitused, ning jurisdiktsioonidega, mille suhtes kohaldatakse finantssanktsioone, embargosid või meetmeid, mis on seotud terrorismi, terrorismi rahastamise või levikuga.

- c) Klient või kliendi tegelikult kasu saava omaniku elukoht, asukoht, tegevuskoht või isiklikud või ärisuhted on seotud jurisdiktsiooniga, millega kaasneb suurem rahapesu- või terrorismirisk.
- d) Ärisuhe luuakse krüptovarateenuse osutaja või krüptorahaautomaadi kaudu, mis asub piirkonnas või jurisdiktsioonis, mis on seotud rahapesu ja terrorismi rahastamise suure riskiga.
- e) Klient osaleb kas otseselt või kaudselt, st suhete kaudu kolmandate isikutega, krüptovarade kaevandamisel, mis toimub Euroopa Komisjoni poolt direktiivi (EL) 2015/849 artikli 9 alusel tuvastatud suure riskiga jurisdiktsioonis või jurisdiktsioonis, mille suhtes kohaldatakse piiravaid meetmeid või sihipäraseid finantssanktsioone.

#### 21.8. Järgmine tegur võib **riski vähendada**.

- a) Kui ülekanne pärineb krüptovarakontolt või hajusraamatu aadressilt, mida majutab määrusega (EL) 2023/1114 reguleeritud või reguleerimata krüptovarateenuse osutaja jurisdiktsioonis, mis on seotud rahapesu ja terrorismi rahastamise väikese riskiga.

### Turustuskanalite riskitegurid

#### 21.9. Järgmised tegurid võivad **riski suurendada**.

- a) Ärisuhte loomiseks kasutatakse klientide kaugtuvastamise lahendusi, mis ei ole kooskõlas EBA suunistega klientide kaugtuvastamise kohta<sup>9</sup>.
- b) Rahastamisvahendil puuduvad piirangud, näiteks sularaha või e-raha toodetega tehtavate maksete korral, millele kehtib direktiivi (EL) 2015/849 artikli 12 erand.
- c) Krüptovarateenuse osutaja ja kliendi vaheline ärisuhe luuakse eespool suunises 9.20 määratletud krüptovarateenuse vahendaja kaudu.
- d) Kliendi tuvastamine ja kontrollimine toimub suure riskiga jurisdiktsioonis asuva krüptovarateenuse osutaja poolt tegevuse edasiandmise lepingu alusel kooskõlas direktiivi (EL) 2015/849 artikliga 29.
- e) Krüptovarade turustamiseks kasutatakse uusi turustuskanaleid või uut tehnoloogiat, mida ei ole veel täielikult testitud või millega kaasneb rahapesu ja terrorismi rahastamise suurem risk.

---

<sup>9</sup> Suunised klientide kaugtuvastamise lahenduste kohta kooskõlas direktiivi (EL) 2015/849 artikli 13 lõikega 1.

- f) Ärisuhe luuakse krüptorahaautomaatide kaudu, mis suurendab sularaha kasutamisest tulenevat riski.

#### 21.10. Järgmised tegurid võivad **riski vähendada**.

- a) Kui krüptovarateenuse osutaja tugineb kliendi suhtes rakendatavatele hoolsusmeetmetele, mida kolmas isik kohaldab kooskõlas direktiivi (EL) 2015/849 artikliga 26, ja kui see kolmas isik asub ELis.

## Meetmed

21.11. Krüptovarateenuse osutajad peaksid tagama, et süsteemid, mida nad kasutavad rahapesu ja terrorismi rahastamise riskide tuvastamiseks ja maandamiseks, vastavad käesolevate suuniste I jaotises sätestatud kriteeriumidele. Eelkõige peaksid krüptovarateenuse osutajad oma ärimudelite tõttu tagama, et neil oleks olemas sobivad ja tõhusad järelevalvevahendid, sealhulgas tehingute jälgimise vahendid ja täiustatud analüüsivahendid. Selliste vahendite ulatus sõltub krüptovarateenuse osutaja tegevuse laadist ja mahust, sealhulgas kauplemiseks või vahetamiseks kättesaadavaks tehtud krüptovarade liigist. Krüptovarateenuse osutajad peaksid samuti tagama, et asjaomased töötajad saaksid erikoolituse, et neil oleks hea ülevaade krüptovaradest ning krüptovarateenuse osutajatele avalduvatest rahapesu ja terrorismi rahastamise riskidest.

### Kliendi suhtes rakendatavad tugevdatud hoolsusmeetmed

21.12. Kui ärisuhte või juhutehinguga seotud risk on suurem, peavad krüptovarateenuse osutajad kohaldama tugevdatud hoolsusmeetmeid vastavalt direktiivi (EL) 2015/849 artiklile 18 ja käesolevate suuniste I jaotises sätestatule. Lisaks peaksid krüptovarateenuse osutajad vajaduse korral kohaldama allpool loetelus loetletud asjakohaseid tugevdatud hoolsusmeetmeid, sõltuvalt ärisuhte riskipositsioonist:

- a) kliendi ja tegelikult kasu saava omaniku isikusamasuse kontroll mitme usaldusväärse ja sõltumatu allika põhjal;
- b) direktiivi (EL) 2015/849 artikli 3 kohasele tegelikult kasu saava omaniku määratlusele mittevastavate enamusaktsionäride või mis tahes füüsiliste isikute isikusamasuse tuvastamine ja kontroll, kui neil on volitus hallata kliendi nimel krüptovarakontot või hajusraamatu aadressi või anda juhiseid krüptovarade ülekandmiseks või vahetamiseks või muude nende krüptovaradega seotud teenuste osutamiseks;
- c) lisateabe hankimine kliendi ja ärisuhte olemuse ja eesmärgi kohta, et koostada kliendist terviklikum profiil, näiteks otsides teavet avalikest allikatest või negatiivsest meediakajastustest või tellides kolmandalt isikult uuriva aruande. Krüptovarateenuse osutaja otsitava teabe näited:

- i. kliendi tegevuse või tööhõive olemus;
  - ii. kliendi vara allikas ja kliendi krüptovaradeks vahetatavate rahaliste vahendite allikas, et mõistlikkuse piires veenduda nende seaduslikkuses;
  - iii. kliendi ametlike väeringute vastu vahetatavate krüptovarade allikas, sealhulgas nende ostmise aeg ja koht;
  - iv. tehingu eesmärk, sealhulgas asjakohasel juhul krüptovarade ülekande sihtkoht;
  - v. teave kliendi võimalike seoste kohta muude jurisdiktsioonidega (peakorter, tegevusrajatised, filiaalid jt) või isikutega, kellel on teadaolevalt oluline mõju kliendi tegevusele;
  - vi. teabepäringud, et saada teavet kliendi krüptovaratehingute kohta ja – kui klient on krüptovaratteenuse osutaja – tema kauplemisajaloo kohta krüptovaratteenuse osutaja süsteemist;
- d) tõendite hankimine rahaliste vahendite, varade või krüptovarade allika kohta suurema riskiga tehingute korral;
  - e) krüptovaratehingute sagedam jälgimine; kõiki tehinguid tuleks jälgida ootamatute käitumisviiside, mustrite ja kahtlase tegevuse tunnuste suhtes ning hõlmata tuleks ka pooled, kellega klient tehinguid teeb;
  - f) säilitatava teabe, andmete ja dokumentatsiooni sagedam läbivaatamine ja vajaduse korral ajakohastamine, eelkõige käivitava sündmuse korral;
  - g) kui ärisuhtega seotud risk on eriti suur, peaksid krüptovaratteenuse osutajad ärisuhte sagedamini üle vaatama;
  - h) kliendi krüptovarakontode kaudu tehtavate tegevuste sagedam või põhjalikum hindamine, kasutades krüptovarade analüüsivahendeid;
  - i) kui kliendil on mitu hajusraamatu aadressi või plokiahelavõrku, peaks krüptovaratteenuse osutaja seostama need aadressid kliendiga;
  - j) kliendi IP-aadresside jälgimise sageduse suurendamine ja kontrollimine, kas need vastavad teiste klientide kasutatavatele IP-aadressidele;
  - k) kinnituse hankimine kliendi krüptovarade alaste teadmiste ja arusaamise taseme kohta, et olla kindel, et klienti ei kasutata rahamuulana;
  - l) kui väljavõtmiste või tagasivõtmiste muster ei ole kooskõlas kliendiprofiiliga või ärisuhte olemuse ja eesmärgiga, peaks krüptovarateenuste osutaja võtma lisameetmeid tagamaks, et väljavõtmist või tagasivõtmist taotleb klient, mitte kolmas isik; see on eriti oluline suure riskiga või eakate või haavatavamate klientide puhul;
  - m) kinnituse hankimine, et isehallatav aadress, millelt ülekanne laekub, on krüptovarateenuste osutaja kliendi kontrolli all või valduses.

21.13. Krüptovarateenuse osutajad peaksid lisaks tavapärasele tehingute jälgimisvahenditele kasutama tehingute jälgimiseks riskitundlikkuse alusel täiustatud analüüsvahendeid. Krüptovarateenuse osutajad peaksid kasutama täiustatud analüüsvahendeid, et hinnata tehingutega, eelkõige isehallatavatelt aadressidelt tehtud tehingutega seotud riske, sest see võimaldab krüptovarateenuse osutajal jälgida tehingute ajalugu ja tuvastada võimalikke seoseid kuritegelike tegevuste, isikute või üksustega.

21.14. Suure riskiga ELi-väliseid riike hõlmavate ärisuhete või tehingute korral peaksid krüptovarateenuse osutajad järgima I jaotise suuniseid.

### **Kliendi suhtes rakendatavad lihtsustatud hoolsusmeetmed**

21.15. Krüptovarateenuse osutajad võivad väikse riskiga olukordades, mis on sellisteks liigitatud rahapesu ja terrorismi rahastamise riskihindamise tulemusena, mille krüptovarateenuse osutaja on teinud kooskõlas käesolevate suunistega, ja siseriiklike õigusaktidega lubatud ulatuses, kohaldada lihtsustatud hoolsusmeetmeid, mis võivad hõlmata järgmist:

- a) kui kliendi suhtes kohaldatakse ELis või ELi-välises riigis seadusest tulenevat litsentsimis- ja regulatiivkorda, isikusamasuse kontrollimine tõendite põhjal, mis näitavad, et kliendi suhtes kohaldatakse nimetatud korda, näiteks otsing reguleeriva asutuse avalikus registris;
- b) kliendi suhtes rakendatavate hoolsusmeetmete teabe, andmete ja dokumentide ajakohastamine ainult kindlate käivitavate sündmuste korral, näiteks kui klient soovib uut või suurema riskiga toodet või kui kliendi käitumise või tehinguprofiili muutused viitavad sellele, et ärisuhete seotud risk ei ole enam väike, järgides siseriiklikus õiguses sätestatud võimalikke ajakohastusperioode;
- c) tehingute järelevalve sageduse vähendamine korduvate tehingutega seotud toodete korral.

### **Dokumentide säilitamine**

21.16. Kui teave klientide ja tehingute kohta on hajusraamatus kättesaadav, ei tohiks krüptovarateenuse osutajad andmete säilitamisel tugineda hajusraamatule, vaid peaksid võtma meetmeid, et täita oma andmete säilitamise kohustusi vastavalt direktiivile (EL) 015/849 ning eespool esitatud suunistele 5.1 ja 5.2. Krüptovarateenuse osutajad peaksid kehtestama menetlused, mis võimaldavad neil seostada hajusraamatu aadressi füüsilise või juriidilise isiku kontrollitava privaativõtmega.“