Mainston International OÜ

Registrinumber 14763925

Aadress: Harju maakond, Tallinn, Kesklinna linnaosa, Viru väljak 2, 10111

Rahapesu ja terrorismi rahastamise tõkestamise töökord

Sisu

Heaks kiidetud juhatuse otsusega 01.06.2022

1. Üldsätted

1.1. Käesolevas töökorras sätestatakse sisemised turvameetmed hoolsuskohustuse täitmiseks ning kahtlaste ja ebatavaliste tehingute avastamiseks kõigis Mainston International OÜ (edaspidi Mainston) tegevusvaldkondades.

1.2. Kõik asjaomased töötajad peaksid tundma ja järgima rahapesu ja terrorismi rahastamise tõkestamise seaduses (RTRTS) sätestatud nõudeid, suuniseid rahapesu ja terrorismi rahastamisega seotud võimalike kahtlaste tehingute tunnuste kohta, muid Mainstoni tegevusega seotud RTRTS-i järgimise suuniseid ning käesolevat töökorda.

1.3. Kõik asjaomased töötajad peaksid end kursis hoidma õigusaktide muudatustega ja muude õigusaktidega, mis on avaldatud rahapesu andmebüroo veebilehel https://fiu.ee.

1.4. Käesoleva töökorra koopia peab olema kättesaadav kõigile asjaomastele töötajatele.

2. Mõisted

2.1. Mis on rahapesu?

2.1.1. Kuritegelikust tegevusest saadud vara või sellie asemel saadud vara muundamine või üleandmine, kui on teada, et see vara on saadud kuritegelikust tegevusest või sellises tegevuses osalemisest, eesmärgiga varjata vara ebaseaduslikku päritolu või abistada kuritegelikus tegevuses osalenud isikut, et ta saaks hoiduda oma tegude õiguslikest tagajärgedest.

2.1.2. Kuritegelikust tegevusest saadud vara või selle asemel saadud vara omandamine, valdamine või kasutamine, kui selle saamisel on teada, et see vara on saadud kuritegelikust tegevusest või selles osalemisest.

2.1.3. Kuritegelikust tegevusest saadud vara või selle asemel saadud vara tõelise olemuse, päritolu, asukoha, käsutamisviisi, ümberpaigutamise, sellega seotud õiguste või omandiõiguse varjamine, kui on teada, et see vara on saadud kuritegelikust tegevusest või sellises tegevuses osalemisest.

2.1.4. Kuritegelikust tegevusest saadud vara või selle asemel saadyd vara tõelise olemuse, päritolu, asukoha, käsutamisviisi, ümberpaigutamise või omandiõiguse varjamine või varaga seotud muude õiguste varjamine.

2.2. Mis on terrorismi rahastamine?

Rahaliste vahendite eraldamine või kogumine selliste tegude kavandamiseks või sooritamiseks, mida peetakse terroriaktideks, või terroristlike organisatsioonide tegevuse rahastamiseks või teadmises, et eraldatud või kogutud vahendeid kasutatakse eespool nimetatud eesmärkidel.

2.3. Mis on riskiriik?

Huvipakkuvad riigid või piirkonnad, kus rahapesu või terrorismi oht on suur. Riskiriik on riik või jurisdiktsioon, mis

2.3.1. usaldusväärsete allikate, näiteks vastastikuste hindamiste, üksikasjaliku hindamise aruannete või avaldatud järelaruannete kohaselt ei ole kehtestanud rahapesu ja terrorismi rahastamise tõkestamise tõhusaid süsteeme;

2.3.2. usaldusväärsete allikate kohaselt on märkimisväärse korruptsiooni või muu kuritegeliku tegevuse tasemega;

2.3.3. on näiteks Euroopa Liidu või ÜRO sanktsioonide, embargode või muude sarnaste meetmete all;

2.3.4. rahastab või toetab terroristlikku tegevust või kus tegutsevad Euroopa Liidu või ÜRO poolt kindlaks määratud terroristlikud organisatsioonid.

2.4. Mis on kõrge riskiga riik?

Euroopa Parlamendi ja nõukogu direktiivi (EIJ) 2015/849 (mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist) artikli 9 lõike 2 alusel vastu võetud delegeeritud õigusaktis nimetatud riik. Praegune loetelu põhineb Euroopa Komisjoni delegeeritud määrusel (EL) 2016/1675, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849, määrates kindlaks suure riskiga kolmandad riigid, kus esineb strateegilisi puudusi (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R1675-20210207).

2.5. Kes on riikliku taustaga isik?

Füüsiline isik, kes täidab või on täitnud avaliku võimu olulisi ülesandeid, samuti tema pereliikmed ja lähedased kaastöötajad. Isikuid, kes ei ole tehingu sõlmimise kuupäevaks vähemalt ühe aasta jooksul täitnud ühtegi avaliku võimu olulist ülesannet, samuti nende pereliikmeid või lähedasi isikuid ei käsitata riikliku taustaga isikutena,

2.5.1. Käesoleva töökorra tähenduses on <u>avaliku võimu oluliste ülesannete täitjad</u> järgmised isikud:

a) riigipea, valitsusjuht, minister ja ministri asetäitja või abiminister;
b) parlamendi või sarnase seadusandliku kogu liige, erakonna juhtorgani liige, kõrgeima kohtu kohtunik, riigikontrolör või keskpanga juhatuse liige;
c) suursaadik, asjur või kaitsejõudude kõrgem ohvitser;
d) riigiettevõtte haldus-, juhtimis- või järelevalveorgani liige;
e) rahvusvahelise organisatsiooni juht, juhi asetäitja või juhtorgani liige või samaväärne ametiisik, välja arvatud keskastme või madalama astme ametnikud.

f) õiguskantsler.

2.5.2. Järgmisi isikuid käsitatakse avaliku võimu olulisi ülesandeid täitva isiku <u>pereliikmetena:</u>

a) riigi või kohaliku tasandi riikliku taustaga isiku abikaasa või abikaasaga samaväärseks peetav isik;
b) riigi või kohaliku tasandi riikliku taustaga isiku laps, lapse abikaasa või abikaasaga samaväärseks peetav isik;
c) riigi või kohaliku tasandi riikliku taustaga isiku vanem.

2.5.3. Järgmisi isikuid käsitatakse avaliku võimu olulisi ülesandeid täitva isiku <u>lähedaste kaastöötajatena:</u>

a) füüsiline isik, kelle kohta on teada, et ta on juriidilise isiku või õigusliku üksuse tegelik tulusaaja või tegelikult tulu saav kaasomanik või kellel on muud lähedased ärisuhted riigi või kohaliku tasandi riikliku taustaga isikuga;
b) füüsiline isik, kes sellise juriidilise isiku või õigusliku üksuse ainus tulusaav omanik, mis on teadaolevalt tegelikult asutatud riigi või kohaliku tasandi riikliku taustaga isiku kasuks.

2.5.4. Järgmised isikud on <u>kohaliku tasandi riikliku taustaga isikud:</u>

isik, kes täidab või on täitnud avaliku võimu olulisi ülesandeid Eestis, mõnes teises Euroopa Majanduspiirkonna lepinguriigis või Euroopa Liidu institutsioonis.

2.5.5. <u>Kuidas asjaomane töötaja peaks kontrollima, kas klient on riikliku taustaga isik?</u>

Asjaomane töötaja peaks potentsiaalse kliendi täisnime kasutades uurima tema tausta. Juhul, kui leidub mitu sarnast vastet, peab asjaomane töötaja kasutama teist identifikaatorit (sünniaeg jne)kindle veendumaks, et leitud tulemus käib potentsiaalse kliendi kohta.

Asjaomase töötaja peaks kontrollimiseks kasutama üldtuntud internetipõhiseid otsingumootoreid ja andmebaase, millele Mainstonil on juurdepääs. Näiteks saab asjaomane töötaja kontrollida, kas potentsiaalne klient on riikliku taustaga isik, kasutades

andmebaasi, mis on kättesaadav aadressil: https://dilisense.com/en_US, või ettevõtte poolt pakutavat tarkvara.

2.6. Mis on RTRTS?

Õigusakt, mis reguleerib krediidi- ja finantseerimisasutuste, muude rahapesu ja terrorismi rahastamise tõkestamise seaduses nimetatud ettevõtjate ja asutuste ning rahapesu andmebüroo tegevust, mis on seotud rahapesu ja terrorismi rahastamise tõkestamisega. Eesti keeles rahapesu ja terrorismi rahastamise tõkestamise seadus (RT I, 12.03.2022, 19).

2.7. Mis on rahvusvahelise sanktsiooni seadus?

Õigusakt, reguleerib riigisiseselt rahvusvaheliste sanktsioonide kehtestamist, nende rakendamist ja järelevalvet, kui rahvusvaheliste sanktsioonide kehtestamise on otsustanud Euroopa Liit, ÜRO, muu rahvusvaheline organisatsioon või Eesti valitsus.

2.8. Kes on klient?

Isik või juriidiline isik, kes kasutab või on kasutanud ühte või mitut Mainstoni pakutavat teenust.

2.9. Kes on asjaomane töötaja?

Isik, kes viib Mainstonis läbi kliendiga seotud taustakontrolli / rahapesu tõkestamise meetmeid.

2.10. Mis on ärisuhe?

Käesoleva töökorra tähenduses on ärisuhe jätkuv lepinguline suhe kliendiga.

2.11. Mis on tehingu jälgimine?

Iga üksik uurimine, mille töötaja kliendi kohta läbi viib.

2.12. Kes on juriidilise isiku lõplik tegelik tulusaaja?

Lõplik tegelik tulusaaja on füüsiline isik (füüsilised isikud), kellele klient lõplikult kuulub või kes teda kontrollib, ja/või füüsiline isik, kelle nimel tehing tehakse. See hõlmab ka neid isikuid, kes teostavad lõplikku tegelikku kontrolli juriidilise isiku või üksuse üle. Väljendid „lõplikult kuulub või kontrollib“ ja „lõplik tegelik kontroll“ osutavad olukordadele, kus omandiõigust/kontrolli teostatakse omandiahelate kaudu või muu kui otsese kontrolli abil. Seda määratlust tuleks kohaldada ka elukindlustuspoliisi või muu investeeringutega seotud kindlustuspoliisi tegeliku tulusaaja või soodustatud isiku suhtes. Ilma et see piiraks eespool sätestatut, on lõplik tegelik tulusaaja eraisik, kes omab või kontrollib rohkem kui 25% juriidilisest isikust.

2.13. Mis on rahapesu andmebüroo?

Eesti rahapesu andmebüroo on sõltumatu valitsusasutus. Rahapesu andmebüroo analüüsib ja kontrollib teavet rahapesu või terrorismi rahastamise kahtluse kohta, võtab vajaduse korral meetmeid vara säilitamiseks ja edastab kuriteo tunnuste tuvastamise korral materjalid viivitamatult pädevatele asutustele.

Postiaadress: Rahapesu Andmebüroo, Pronksi 12, 10117 Tallinn. E-post: info@fiu.ee
Veebipõhine teate saatmise vorm: https://fiu.ee/saada-teade

2.14. Kes on kontaktisik?

Kontaktisik on Mainstoni juhatuse poolt määratud rahapesu andmebüroo kontaktisik. Kontaktisikuks võib määrata ainult Eestis alaliselt töötava isiku, kellel on kontaktisiku ülesannete täitmiseks vajalik haridus, erialane sobivus, vajalikud võimed, isikuomadused ja kogemused ning laitmatu maine. Kontaktisiku määramine lepitakse kokku rahapesu andmebürooga. Kontaktisiku ülesandeid võib täita töötaja või struktuuriüksus. Kui kontaktisiku ülesandeid täidab struktuuriüksus, vastutab nimetatud ülesannete täitmise eest vastava struktuuriüksuse juht. Mainstoni juhatuse poolt määratud kontaktisik on ka rahvusvahelise finantssanktsiooni rakendamise eest vastutav isik.

3. Klientide tuvastamise ja kontrollimise standardmenetlus (klientide registreerimine)

3.1. Asjaomane töötaja peab tuvastama kõik Mainstoni teenuseid kasutada soovivad kliendid isikut tõendava dokumendi alusel ning registreerima identifitseerimis- ja tehinguandmed sõltumata sellest, kas klient on püsiklient või mitte.

3.2. Isik tuleb tuvastada

a) enne ärisuhte loomist;
b) kliendi kahtlase käitumise korral;
c) teabe kontrollimisel või juhul, kui on kahtlusi eelnevalt kogutud dokumentide või andmete piisavuses või tõesuses, kui ajakohastatakse asjakohaseid andmeid.

3.3. Kui klient on eraisik, peab ta esitama

a) enda täisnime;
b) isikukoodi või selle puudumisel sünniaja ja -koha ning elukoha;
c) kui klient tegelikult esindab teist eraisikut, kes on tegelik klient (volikirja alusel või pärimise korral või muul viisil), teabe esindusõiguse tuvastamise ja kontrollimise ning selle ulatuse kohta ning juhul, kui esindusõigus ei tulene seadusest, esindusõiguse aluseks oleva dokumendi nimetuse, väljaandmise kuupäeva ja väljastaja nime;
d) telefoninumbri ja meiliaadressi.

3.4. Identifitseerimise aluseks on järgmised kehtivad dokumendid:

a) isikutunnistus;
b) pass;
c) diplomaatiline pass;
d) Euroopa Liidu kodaniku ID-kaart;
e) juhiluba, kui dokumendil on selle omaniku nimi, foto või näokujutis, allkiri või allkirjakujutis ja sünniaeg või isikukood.

3.5. Isiku tuvastamisel on asjaomane töötaja kohustatud kontrollima isikut tõendava dokumendi kehtivust, veenduma, et isik vastab dokumendis esitatud andmetele, ja kontrollima isiku vanust. Isikusamasuses kahtlemise korral on asjaomane töötaja kohustatud küsima isiku kohta lisateavet. Kui saadetakse dokument, mis ei vasta isikule või on kehtetu, peab asjaomane töötaja keelduma kliendi registreerimisest ja teavitama sellest kontaktisikut.

3.6. Asjaomane töötaja kontrollib kliendi andmete õigsust, kasutades selleks usaldusväärsest ja sõltumatust allikast pärinevat teavet. Kui tuvastatud isikul on punktis 3.4 nimetatud kehtiv 6ocument või samaväärne 6ocument, isik on tuvastatud ja tema isikusamasus on kontrollitud dokumendi alusel või elektrooniliste tehingute puhul elektroonilise identifitseerimise ja usaldusteenuste abil ning dokumendi kehtivus nähtub dokumendist või on tuvastatav elektrooniliste tehingute puhul elektroonilise identifitseerimise ja usaldusteenuste abil, ei ole vaja säilitada dokumendil olevaid täiendavaid andmeid.

3.7. Kui klient on Eesti juriidiline isik (näiteks äriühing), peab ta esitama järgmised andmed:

a) juriidilise isiku nimi või ärinimi;
b) registrikood või registreerimisnumber ja registreerimise kuupäev;
c) juhi, juhatuse või muu juhatust asendava organi liikmete nimed ja nende volitused juriidilise isiku esindamisel;
d) juriidilise isiku kontaktandmed.

3.8. Kui klient on välismaine juriidiline isik (näiteks äriühing), peab ta lisaks punktis 3.7 esitatud teabele esitama juriidilise isiku äriregistri (või Company House'i või sõltuvalt päritoluriigist muu sarnase registri) väljavõtte, mis on kinnitatud notariaalselt ja/või legaliseeritud ja/või apostilliga kinnitatud, kui rahvusvahelises lepingus ei ole sätestatud teisiti, mis näitab ka selle juriidilise isiku esindamise õigusi.

3.9. Asjaomane töötaja tuvastab juriidilise isiku vastava registri registrikaardi või vastava registri registreerimistunnistuse või muu sellise kaardi või tunnistusega võrdväärse dokumendi alusel.

3.10. Asjaomane töötaja peab tuvastama tegelikud tulusaajad ja nende isikusamasuse kontrollimiseks võtma meetmeid, mis võimaldavad asjaomasel töötajal veenduda, et ta teab, kes on tegelikud tulusaajad, ning mõistab kliendi või tehingus osaleva isiku omandi- ja kontrollistruktuuri.

3.11. Asjaomane töötaja kontrollib juriidilise isiku andmete õigsust, kasutades selleks usaldusväärsest ja sõltumatust allikast pärinevat teavet. Kui asjaomane töötaja saab teavet kontrollida sellise otsese juurdepääsu kaudu, ei ole vaja nõuda kliendilt punktis 3.9 nimetatud dokumentide esitamist.

3.12. Välisriigi juriidilise isiku esindaja peab asjaomase töötaja taotlusel, näiteks kui esindusõigus ei ole esitatud dokumendis/dokumentides märgitud, esitama oma volitusi tõendava dokumendi (volikirja), mis on notariaalselt kinnitatud ja/või legaliseeritud ja/või apostilliga kinnitatud, kui rahvusvahelises lepingus ei ole sätestatud teisiti.

3.13. Asjaomane töötaja võib küsida kliendi kohta lisateavet, kui tekib kahtlus kliendi isikuandmeid või kliendi käitumist puudutavate andmete kohta. Selline küsitav lisateave peaks olema seoses esinevate riskidega asjakohane, et selle saamisel võiksid risked osutuda seletatavaks.

3.14. Klientide registreerimise kord on kooskõlas 1. ja 2. lisaga.

4. Isiku tuvastamine ja andmete kontrollimine infotehnoloogiliste vahendite abil

4.1. Asjaomane töötaja peab tuvastama isiku ja kontrollima andmeid infotehnoloogiliste vahendite abil, kui ärisuhe luuakse isikuga, kes on pärit Euroopa Majanduspiirkonna lepinguriigist või kelle elukoht või asukoht on sellises riigis ja kelle tehingu või teenuslepinguga seotud väljaminevate maksete kogusumma ületab 15 000 eurot kalendrikuus (füüsilise isiku puhul) või juriidilisest isikust kliendi puhul 25 000 eurot kalendrikuus ja/või kui hoolsusmeetmeid ei rakendata isiku või tema esindajaga füüsiliselt samas kohas viibides.

4.2. Asjaomane töötaja peab tuvastama isiku ja kontrollima andmeid infotehnoloogiliste vahendite abil, kui ärisuhe luuakse e-residendiga või isikuga, kes on pärit väljaspool Euroopa Majanduspiirkonda asuvast riigist või kelle elukoht või asukoht on sellises riigis, ja kui hoolsusmeetmeid ei rakendata isiku või tema esindajaga füüsiliselt samas kohas viibides.

4.3. Kliendiandmete tuvastamisel ja kontrollimisel infotehnoloogiliste vahendite abil peab asjaomane töötaja järgima rahandusministeeriumi määrusega kehtestatud tehnilisi nõudeid ja korda, mis on leitavad aadressil https://www.riigiteataja.ee/akt/104122020009?leiaKehtiv. Nõuded on täiendavalt esitatud järgnevates alapeatükkides pärast tabelit.

4.4. Kokkuvõte erinevatest rahapesu tõkestamise meetmetest, mida kohaldatakse üksikkliendi suhtes:

Erinevad rahapesu tasemed, mis võivad täiendavalt kehtida üksikkliendi suhtes	Rahapesuvastased meetmed

1. tase – mis tahes rahasumma kliendi registreerimisel.	Punkt 3.1 on sama, mis punkti 3.2 alapunkt a, kuid üksikasjalikuma selgitusega. Rahapesu tõkestamise hoolsusmeetmete tase (lihtsustatud, standardsed või tugevdatud) sõltub asjaomase kliendi riskihinnangust. Rahapesuvastane kontroll toimub Mainstoni kogutud dokumentide ja teabe põhjal. Punktis 4.2 on sätestatud, et väljaspool EMPd asuvate riikide residentide puhul tuleb kontrolli teostada „IKT-vahendite abil“.
2. tase – aastas rohkem kui 15 000 euro ülekandmine juhuti tehtavate tehingutena	Punkti 3.2 alapunkt d: kui kliendi tehingud ületavad selle piirmäära, tuleb klienti uuesti kontrollida tagamaks, et endiselt e I ole rahapesu või terrorismi rahastamise ohtu. Rahapesuvastane kontroll toimub Mainstoni kogutud dokumentide ja teabe põhjal. Ainult EMP-väliseid kodanikke tuleb kontrollida „IKT-vahendite abil“.

3. tase – üle 15 000 euro kuus (25 000 eurot kuus, kui klient on juriidiline isik).	Punkt 4.1: nõue, mida kohaldatakse Euroopa Majanduspiirkonna lepinguriigist pärit isiku suhtes, kui rahalised piirmäärad on ületatud; kontrollimine peab toimuma „IKT-vahendite abil“, mitte ainult kliendilt saadud dokumentide alusel.

4.5. Kui Mainston tuvastab ja kontrollib kliendi andmeid infotehnoloogiliste vahenditega, kasutab Mainston kliendi tuvastamiseks mõeldud dokumenti ja järgib järgmisi eeltingimusi:

a) kasutatakse väga usaldusväärseid tehnilisi vahendeid, mis koosnevad toimivast kaamerast, mikrofonist, digitaalseks tuvastamiseks vajalikust riist- ja tarkvarast ning piisava kvaliteediga internetiühendusest;

b) kasutatakse infotehnoloogilisi vahendeid, mis võimaldavad võrrelda biomeetrilisi andmeid. Biomeetriliste andmete hulka kuuluvad näokujutis, sõrmejälje kujutised, allkiri või allkirja kujutis ja iirise kujutised;

c) saadakse kliendilt kinnitus, et ta on lugenud infotehnoloogiliste vahendite kasutamist käsitlevat teavet ja nõustub infotehnoloogiliste vahendite abil oma isiku tuvastamise ja kontrollimise tingimustega;

d) saadakse kliendilt kinnitus, et ta viib identifitseerimis- ja kontrollimenetlused infotehnoloogilisi vahendeid kasutades isiklikult läbi, et esitatud andmed on tõesed ja täielikud ning et ta vastab Mainstoni poolt ärisuhte loomiseks ja juhuti tehtavate tehingute tegemiseks kehtestatud tingimustele;

e) saadakse kliendilt nõusolek Eesti õiguse kohaldatavuse kohta;

f) palutakse isikul (kui tegemist on välismaalasega) näidata kaamera ees välisriigi väljastatud kehtiva reisidokumendi isikuandmete lehekülge.

4.6. Kliendi isiku tuvastamine ja kontrollimine infotehnoloogiliste vahendite abil ei õnnestu, kui esineb mõni järgmistest asjaoludest:

a) isik esitas tahtlikult andmeid, mis ei vasta isikut tõendavate dokumentide andmebaasi kantud isikuandmetele või ei vasta muude menetluste käigus saadud teabele või andmetele;

b) infotehnoloogiliste vahendite abil toimuva identifitseerimise ja kontrollimise käigus seanss lõpeb või katkestatakse. Seanss lõpeb, kui isik ei ole 15 minuti jooksul ühtegi tegevust sooritanud;

c) isik ei ole andnud punktis 4.5 nimetatud kinnitusi;

d) isik keeldub infotehnoloogilisi vahendeid kasutades täitmast näo ja dokumendi kujutamist käsitlevaid juhiseid. Isiku pea ja õlad peavad olema nähtavad ja pildi keskel, nägu peab olema varjudeta ja katmata, taustast ja muudest objektidest selgelt eristatav ning äratuntav;

e) isik kasutab kolmanda isiku abi ilma Mainstoni loata;

f) esineb rahapesu või terrorismi rahastamise kahtlus.

4.7. Asjaomane töötaja koostab isiku tuvastamise ja küsimustiku (kui see on kohaldatav) ning muu kättesaadava teabe ning andmete süstematiseeritud kogumise ja analüüsi ning faktide selgitamise põhjal kliendiprofiili ja riskiprofiili. Lisaks peab asjaomane töötaja esitama arvamuse infotehnoloogiliste vahendite abil toimuva registreerimismenetluse tulemuste kohta ja tegema ettepaneku isiku suhtes kohaldatava ärisuhete jälgimise korra kohta. Teenuseosutaja asjaomase töötaja arvamus on aluseks, mille alusel tehakse otsus ärisuhte loomiseks.

4.8. Kui isiku tuvastamine ja kontrollimine ei õnnestu eelnimetatud asjaolude tõttu, peab teenuseosutaja esitama rahapesu andmebüroole aruande.

4.9. Mainston ei osuta teenuseid ega võimalda juhuti tehtavate tehingute sooritamist väljaspool ärisuhteid.

4.10. Mainston ei sõlmi lepingut ega tee otsust anonüümse konto või anonüümse virtuaalvaluuta rahakoti avamiseks.

4.11. Mainston saadab füüsilisele või juriidilisele isikule, kes soovib saada kliendiks ja kelle üldine riskiskoor on keskmine või kõrge, identifitseerimisküsimustiku (3. tasandi küsimustik, kontroll 5.8). Mainston võib lubada, et isik kasutab identifitseerimisküsimustiku täitmisel tehniliste probleemide kõrvaldamiseks teise isiku abi. Teenuseosutaja asjaomane töötaja peab hindama identifitseerimisküsimustikus antud vastuseid ning kandma oma arvamuse ja selle aluseks olevad asjaolud kliendiprofiili ja riskiprofiili.

Mainston pakub füüsilistele isikutele (üksikisikud), kes on edukalt läbinud 1. ja 2. tasandi, juurdepääsu 3. tasandile (rahapesuvastane küsimustik).

4.12. Kui tegemist on füüsilise isikuga, tuleb küsimustiku vastustes märkida järgmised andmed (pidades silmas, et isikut tõendavat dokumenti ja aadressi tõendavat dokumenti on juba varem küsitud):

a) amet/ametinimetus;

b) kliendi elukutse; üksikisiku või ettevõtte tegevusala (rippmenüü);

c) tegelemine äritegevusega ka teistes riikides peale selle, kus isik on maksukohustuslasena registreeritud (jah/ei vastus);

d) Mainstoni konto avamise eesmärk (rippmenüü);

e) Kavandatud igakuine käive eurodes ;

f) kliendi kontol olevate rahaliste vahendite allikas;

g) riigid, kust raha saadakse või üle kantakse;

h) finantsasutustes olevate kontode nimekiri (panga nimi ja riik);

i) kas klient või tema pereliige või lähedane kaastöötaja on riikliku taustaga isik.

4.13. Kasutajad (füüsilised isikud), kes on edukalt läbinud 3. tasandi, saavad veebipõhise juurdepääsu juriidiliste isikute 4. tasandi küsimustikule. Sellel etapil saab füüsiline isik muuta oma konto juriidilise isiku (ärikasutaja) kontoks.

4.14. Kui isik on juriidiline isik, tuleb küsimustiku vastustes märkida järgmised andmed:

a) registreerimisriik;

b) äriühingu nimi ja vorm;

c) registreerimise kuupäev;

d) registrinumber;

e) KMK registreerimisnumber;

f) veebisait;

g) riigi äriühingute registri portaali või avaliku allika (nt register või äriregister) link;

h) telefoninumber;

i) ühenduse võtmise meiliaadress;

j) asutamistunnistus või väljavõte kohalikust registrist või äriregistrist;

k) asutamisleping ja põhikiri;

l) registreeritud aadress;

m) tegevuskoha aadress;

n) andmed äriühingu juhi kohta (nimi, telefoninumber, meiliaadress, kodakondsus, aadress, passi või ID-kaardi number ja väljaandjariik);

o) andmed aktsionäride kohta (tegelike tulusaajate ja aktsionäride nimekiri; nõukogu liikmete nimekiri; pangakonto väljavõte (ükski dokument ei tohi olla vanem kui 6 kuud);

p) muud asjakohased dokumendid

4.15. Asjaomane töötaja viib isiku andmete tuvastamiseks ja kontrollimiseks läbi intervjuu, mille käigus asjaomane töötaja esitab küsimustiku tulemustest lähtudes osaliselt struktureeritud küsimusi. Asjaomane töötaja peab teostama ärisuhte loomiseks kohustusliku intervjuu reaalajas. Mainston võib lubada, et isik kasutab identifitseerimisküsimustiku täitmisel tehniliste probleemide kõrvaldamiseks teise isiku abi. Asjaomane töötaja peab hindama isiku reaktsiooni intervjuu ajal, isiku esitatud teabe ja andmete usaldusväärsust koos muude menetluste käigus saadud andmetega ning registreerima oma arvamuse ja asjaolud, mille alusel koostatakse isiku profiil ja riskiprofiil, mis peavad olema kirjalikult taasesitatavad.

4.16. Mainston peab võimaldama isiku digitaalset tuvastamist ja digitaalset allkirjastamist.

4.17. Mainston peab tagama, et videopildi kasutamisel (nt punkti 4.9 kohase reaalajas intervjuu puhul) on tagatud selge, salvestatav ja reprodutseeritav sünkroonitud heli ja pildi edastamine, mis on piisav edastatava sisu üheseks ja usaldusväärseks mõistmiseks. Video tuleb salvestada nii, et seda oleks võimalik taasesitada esialgse ülekandega võrdse kvaliteediga.

4.18. Küsimustiku, isiku tuvastamise, ebaõnnestunud isiku tuvastamise ja kohustusliku reaalajas toimuva intervjuu käigus kogutud andmed tuleb salvestada vastavalt järgmistele nõuetele:

a) koos ajatempliga, mis peab olema seotud asjaomaste andmetega selliselt, et andmete hilisemad muudatused, muudatuste tegija ning nende tegemise aeg, viis ja põhjus oleksid tuvastatavad;

b) koos isiku IP-aadressiga;

c) koos tuvastatava isiku isikukoodiga;

d) koos sünniaja ja -koha ning elukohariigiga (isikukoodi puudumise korral);

e) andmed peavad olema reprodutseeritavad viie aasta jooksul pärast ärisuhte lõppu.

4.19. Isiku tuvastamise ja andmete kontrollimise teostamist infotehnoloogiliste vahendite abil kontrollib kontaktisik vastavalt käesoleva töökorra punktile 16.

4.20. Kliendi isiku tuvastamise ja kontrollimise kord on kooskõlas 1. ja 2. lisaga.

5. Klientide suhtes rakendatavad hoolsusmeetmed, lihtsustatud hoolsusmeetmed ja tugevdatud hoolsusmeetmed

5.1. Mainston kasutab klientide tuvastamiseks ja kontrollimiseks riskihindamise dokumendi punktis 3.5 nimetatud teenusepakkujaid.

5.2. Kriteeriumide alusel jagatakse kliendid kolme kategooriasse: väike, keskmine ja suur.

5.3. Mainston kohaldab kliendi suhtes lihtsustatud hoolsusmeetmeid, kui on kindlaks tehtud madalamat riski iseloomustav tegur ja täidetud on vähemalt järgmised kriteeriumid:

a) kliendiga on kirjalikult, elektrooniliselt või kirjalikult taasesitatavas vormis sõlmitud pikaajaline leping;

b) ärisuhte raames laekuvad maksed kohustatud isikule ainult sellise konto kaudu, mida peetakse Eesti äriregistrisse kantud krediidiasutuses või välisriigi krediidiasutuse filiaalis või krediidiasutuses, mille asukoht või tegevuskoht on Euroopa Majanduspiirkonna lepinguriigis või riigis, mis kohaldab Euroopa Parlamendi ja nõukogu direktiivis (EIJ) 2015/849 sätestatud nõuetega samaväärseid nõudeid;

c) ärisuhte raames tehtud tehingute sissetulevate ja väljaminevate maksete koguväärtus ei ületa 15 000 eurot aastas.

5.4. Enne lihtsustatud hoolsusmeetmete kohaldamist võetakse arvesse väiksemale riskile osutavaid asjaolusid ja kohustatud isik otsustab, kas neid asjaolusid rakendatakse kogumis, osaliselt või eraldi alustena.

5.5. Väiksemale riskile osutavate asjaolude hindamisel peetakse kliendi isikuga seotud riske vähendavaks olukorraks seda, kui klient vastab mõnele järgmistest tunnustest:

a) klient on reguleeritud turul noteeritud äriühing, mille suhtes kohaldatakse avalikustamiskohustust, millega on kehtestatud nõuded, et tagada tegeliku tulusaaja puhul piisav läbipaistvus;

b) klient on Eestis asutatud avalik-õiguslik juriidiline isik;

c) klient on Eesti või Euroopa Majanduspiirkonna lepinguriigi valitsusasutus või muu avalikke ülesandeid täitev asutus;

d) klient on Euroopa Liidu asutus;

e) klient on enda nimel tegutsev krediidiasutus või finantseerimisasutus, Euroopa Majanduspiirkonna lepinguriigis või kolmandas riigis asuv krediidiasutus või finantseerimisasutus, mille suhtes kohaldatakse tema asukohariigis Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849 nõuetega samaväärseid nõudeid, mille täitmise üle tehakse riiklikku järelevalvet;

f) klient on isik, kes on punktis 5.6 nimetatud tunnustele vastava riigi või geograafilise piirkonna resident.

5.6. Väiksemale riskile osutavate asjaolude hindamisel võib geograafiliseks riske vähendavaks asjaoluks pidada vähemalt selliseid olukordi, kus klient on pärit järgmisest riigist või tema elu- või asukoht on järgmises riigis:

a) Euroopa Majanduspiirkonna lepinguriik;

b) kolmas riik, kus on tõhusad rahapesu ja terrorismi rahastamise tõkestamise süsteemid;

c) kolmas riik, kus usaldusväärsete allikate kohaselt on korruptsiooni ja muu kuritegevuse tase madal;

d) kolmas riik, kus usaldusväärsete allikate, näiteks vastastikuste hindamiste, aruannete või avaldatud järelaruannete kohaselt on kehtestatud rahapesu ja terrorismi rahastamise tõkestamise nõuded, mis on kooskõlas rahapesuvastase töökonna ajakohastatud soovitustega, ja kus neid nõudeid tõhusalt rakendatakse.

5.7. Mainston rakendab neljatasandilist tuvastamismenetlust.

5.8.

1. tasand	ID-dokument, selfi
2. tasand	Elukoha tõendamine
3. tasand	Küsimustik
4. tasand	Küsimustik (juriidiliste isikute puhul)

5.9. Mainstoni kliendiks saamiseks tuleb läbida vähemalt 1. ja 2. tasand.

5.10.

Riskikategooria	Kriteeriumid	Kohaldatavad hoolsusmeetmed	Kohaldatavad hoolsusmeetmed
VÄIKE	• EMP-sisene klient • Aastatehingud alla 15 000 euro • 1. ja 2. tasandi kontroll on läbitud mõlema teenuseosutaja juures tulemusega KORRAS	Lihtsustatud	• Klient laadib ID-dokumendi üles • Klient teeb selfi • Klient esitab elukohatõendi
KESKMINE	• Klient väljaspool EMPd • Aastatehingud üle 15 000 euro • Riigid, kust raha saadakse, asuvad väljaspool EMPd. • 1. ja 2. tasandi kontroll on ühe teenuseosutaja juures lõppenud tulemusega KAHTLANE	Standardsed	• 3. tasandi küsimustik • Käsitsi kontrollib teine töötaja
SUUR	• Klient kõrge riskiga kolmandast riigist Aastatehingud üle 200 000 euro • Pärast küsimustiku täitmist ei ole lihtne kindlaks teha kliendi varade ja	Tugevdatud	• 3. tasandi küsimustik + kliendilt küsitavad lisaküsimused • Käsitsi kontrollib teine töötaja, aruanded

	rahaliste vahendite allikat. • Pärast küsimustiku täitmist ei ole lihtne kindlaks teha Mainstoni konto avamise eesmärki. • Ebasoodsad vasted meediast • 1. ja 2. tasandi kontroll on mõlema teenuseosutaja juures lõppenud tulemusega KAHTLANE.		esitatakse kontaktisikule. • Registreerimisek s on nõutav kontaktisiku heakskiit. • Elukoha tõendamine vähemalt iga 6 kuu järel.
KEELATUD	• Klient elab riskianalüüsi punktis 7.4 osutatud riigis. • Klient on riikliku taustaga isik. • Klient on sanktsioonide all. • Tegelikud ebasoodsad vasted meediast • Kliendi majandustegevuse l on rahapesule või terrorismi rahastamisele viitavaid tunnuseid.	Ei kohaldata	• Kontot ei avata • Kontaktisik esitab vajaduse korral rahapesu andmebüroole aruande

5.11. Riskiskoor arvutatakse põhimõtte „kehtib kõrgeim“ alusel. Kui esineb mitu väikese riski kategooria tunnust või kui lisaks väikese riski tunnustele esineb vähemalt üks keskmise riski tunnus, määratakse klient kategooriasse „keskmine“.

5.12. Asjaomane töötaja peab kindlaks tegema, millised on riskid igal konkreetsel juhul, ja võtma kõik asjakohased meetmed nende riskide vähendamiseks. Sõltuvalt juhtumist võib asjaomane töötaja kohaldada ühte või mitut järgmistest hoolsusmeetmetest:

1) isikusamasuse tuvastamisel täiendavalt esitatud teabe kontrollimine lisadokumentide, andmete või teabe põhjal, mis pärinevad usaldusväärsest ja sõltumatust allikast;
2) täiendava teabe kogumine ärisuhte, tehingu või toimingu eesmärgi ja olemuse kohta ning esitatud teabe kontrollimine lisadokumentide, andmete või teabe põhjal, mis pärinevad usaldusväärsest ja sõltumatust allikast;
3) täiendava teabe ja dokumentide kogumine ärisuhtes tehtavate tehingute tegeliku teostamise kohta, et välistada tehingute näilisus;
4) täiendava teabe ja dokumentide kogumine ärisuhtes tehtavas tehingus kasutatavate vahendite allika ja päritolu kindlakstegemiseks, et välistada tehingute näilisus;
5) tehinguga seotud esimese makse tegemine konto kaudu, mis on avatud tehingus osaleva kliendi nimel krediidiasutuses, mis on registreeritud või mille tegevuskoht asub Euroopa Majanduspiirkonnas või riigis, kus kehtivad Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849 nõuetega samaväärsed nõuded.

6) Tugevdatud hoolsusmeetmete kohaldamisel peab ettevõte tavapärasest sagedamini kohaldama ärisuhte seiret, sealhulgas hindama kliendi riskiprofiili uuesti hiljemalt kuus kuud pärast ärisuhte loomist.

6. Andmete kogumine ja dokumenteerimine

6.1. Mainston on kohustatud säilitama kõik andmed meie klientide ja nende käitumise kohta nii, et neid oleks alati võimalik esitada registreeritud tehinguid kontrollivatele inspektoritele,

6.2. Asjaomane töötaja paneb iga kande lõppu oma nime ja, kui dokument on paberkandjal, oma allkirja.

6.3. Kontaktisik vastutab kõigi asjakohaste andmete säilitamise eest.

6.4. Asjakohased andmed hõlmavad

a) Teavet ärisuhte loomisest või juhuti tehtava tehingu sooritamisest keeldumise asjaolude kohta;

b) teavet selle kohta, kui hoolsusmeetmeid ei ole võimalik infotehnoloogiliste vahendite abil võtta;

c) dokumentide originaale või koopiaid, mille alusel tuvastatakse isikusamasus ja kontrollitakse esitatud teavet;

d) tehingu kuupäeva või perioodi ja tehingu sisu kirjeldust;

e) ettevõtte nimel peetavate maksekontode nimekirja koos iga maksekonto unikaalse tunnuse ja kontohalduri nimega;

f) teavet, mille alusel täidetakse aruandluskohustust rahapesu andmebüroo ees.

6.5. Kliendi isikuandmeid, kliendi tehinguid ja muud asjakohast teavet tuleb säilitada vähemalt 5 aastat pärast ärisuhte lõppemist.

6.6. Andmeid, mis on olulised rahapesu või terrorismi rahastamise tõkestamiseks, avastamiseks või uurimiseks, võib säilitada pikema aja jooksul, kuid mitte kauem kui viis aastat pärast esimese tähtaja möödumist.

6.7. Vahetustehingu tegemisel kogub Mainston järgmised andmed:
a) füüsilise isiku puhul – isiku nimi, tehingu kordumatu tunnus, maksekonto või virtuaalvaluuta rahakoti tunnus, isikut tõendava dokumendi nimetus ja number ning isikukood või sünniaeg ja -koht ning elukoha aadress;
b) juriidilise isiku puhul – isiku nimi, tehingu kordumatu tunnus, maksekonto või virtuaalvaluuta rahakoti tunnus, isiku registrikood või selle puudumisel tema asukohariigi asjakohane tunnus (registrinumbriga samaväärne numbri- või tähekombinatsioon) ja asukoha aadress.

6.8. Kui klient ei esita kõiki vajalikke dokumente ja asjakohast teavet või kui asjaomasel töötajal tekib esitatud dokumentide põhjal kahtlus, et tegemist võib olla rahapesu või terrorismi rahastamisega, ei tee ta selle kliendiga tehingut ning teavitab sellest viivitamata kontaktisikut ja registreerib võimalikult palju kliendi andmeid, mis aitavad hiljem klienti tuvastada.

7. Riskipõhine lähenemisviis

7.1. Asjaomane töötaja, kes analüüsib klienti ja tema käitumist, peaks tegema uurimistoiminguid, mis on proportsionaalsed juhtumi riski ja keerukusega, ning koguma tõendeid, kasutades selleks juhtumi käigus tehtud tähelepanekuid.

7.2. Kui asjaomane töötaja tuvastab täiendavaid riske, peab ta tegema uurimise, et mõista neid riske juhtumi kontekstis.

7.3. Kui tuvastatakse täiendavaid riske, on vaja läbivaatamist ja arusaamist toetavaid täiendavaid tõendeid.

7.4. Alltoodud küsimused võivad aidata kindlaks teha, kas tehing on kahtlane või kas esineb rahapesu või terrorismi rahastamise oht.

a) Kas see on vastuolus kliendi teadaoleva tegevusega?

b) Kas tehingu suurus ei ole kooskõlas kliendi tavapärase tegevusega, nagu see on kindlaks tehtud esialgses tuvastamisetapis?

c) Kas kõnealuse tehinguga on seotud muid tehinguid, millest Mainston on teadlik ja mille eesmärk võib olla raha varjamine ja selle suunamine muudesse sihtkohtadesse või muudele tulusaajatele?

d) Kas tehing on kliendi jaoks põhjendatud?

e) Kas kliendi tehingute muster on muutunud?

f) Kas kliendi pakutud makseviis on Mainstoni pakutavate teenuste kontekstis ebatavaline?

7.5. Rahapesu ja terrorismi rahastamise riskide kindlaksmääramine on kooskõlas Mainstoni riskihindamise dokumendiga.

8. Kliendiga suhtlemine rahapesu või terrorismi rahastamise korral

8.1. Asjaomane töötaja võib võtta kliendiga ühendust, et selgitada esitatud teavet või küsida lisateavet , mis on vajalik kliendi tuvastamiseks või tuvastatud riskide käsitlemiseks.

Kahtlaste või ebatavaliste tehingute ning tehingu eesmärgi ja tegeliku sisu väljaselgitamiseks võtab esindaja järgmised meetmed:

a) vajaduse korral paluda kliendil esitada (täiendavat) teavet kutse- või majandustegevuse kohta;

b) vajaduse korral küsida kliendilt selgitusi tehingu põhjuste kohta ja vajaduse korral dokumente, mis tõendavad rahaliste vahendite ja/või vara päritolu;

8.2. Asjaomane töötaja ei tohiks küsida mittevajalikku või ebaolulist teavet. Täiendava teabe küsimine peab olema seotud juhtumi riskidega ning pärast kliendi vastuse saamist võib asjaomane töötaja juhtumi sulgeda või teatada sellest kontaktisikule. Kui rahapesu või terrorismi rahastamise risk jääb alles, peab asjaomane töötaja teatama juhtumist kontaktisikule ilma kliendilt lisateavet küsimata.

8.3. Asjaomane töötaja ei tohi end kunagi väljendada viisil, mis annab kliendile mõista, et tema tegevus on kahtlane ja sellest võidakse edaspidi teavitada kontaktisikut.

9. Ärisuhte seire

9.1. Tehingu seire algatatakse kliendi käitumises esineva vastava teguri alusel või käsitsi asjaomase töötaja või kontaktisiku poolt. Asjaomane töötaja peab iga algatatud juhtumit uurima.

9.2. Asjaomane töötaja ei saa töötada juhtumi kallal, kui asjaomane klient on asjaomase töötaja lähedane isik või klient, kes on asjaomase töötajaga muul viisil seotud.

9.3. Asjaomane töötaja peaks kindlaks tegema, millised on juhtumi riskid. Iga riski tuleks käsitleda ja dokumenteerida.

9.4. Asjaomane töötaja peab tegema eeluuringu ja kontrollima, kas klienti on varem kontrollitud ja millised olid varasemad probleemid.

9.5 Asjaomane töötaja peab tegema kliendiuuringu, et teha kindlaks kliendi profiil ning tuvastada tehingus kasutatud raha päritolu ja allikas.

9.6. Asjaomane töötaja peab uurima kliendi tegevust ja tegema kindlaks, kas see on kooskõlas kliendiprofiiliga või kas käitumine tundub kahtlane. Tegevuse uuring hõlmab kõiki tähelepanekuid kliendi käitumise kohta ja kõiki tegevuses esinevaid ohutunnuseid.

9.7. Asjaomane töötaja peab uurima kõiki vastaspooli, kui see on juhtumi puhul asjakohane.

9.8. Juhtumi läbivaatamine võib varieeruda vastavalt sellele, milliseid tõendeid on vaja koguda kliendi ja tema tegevuse kohta. Asjaomane töötaja peaks kasutama riskipõhist lähenemisviisi, et käsitleda riske proportsionaalselt.

9.9. Asjaomane töötaja peab dokumenteerima kõik kliendi ja kliendi käitumise kohta tehtud tähelepanekud, mis toetavad asjaomase töötaja otsust juhtumi lõpetamise või kontaktisikule teatamise kohta.

9.10. Pidevate hoolsusmeetmete eesmärk on tagada klientide ja tehingute pidev seire. Ärisuhte pidev seire hõlmab järgmist:

a) ärisuhte raames tehtud tehingute kontrollimine tagamaks, et tehtavad tehingud on kooskõlas kliendi teadmiste, äritegevuse ja kliendi riskiprofiiliga;

b) hoolsusmeetmete rakendamise käigus saadud asjakohaste dokumentide, andmete või teabe korrapärane ajakohastamine;

c) tehingus kasutatud rahaliste vahendite allika ja päritolu tuvastamine;

d) erilise tähelepanu pööramine tehingutele ja kliendi käitumisele, mis viitavad kuritegelikule tegevusele või rahapesule või terrorismi rahastamisele, ning tehingute olemuse, põhjuste ja tausta selgitamine;

e) suurema tähelepanu pööramine ärisuhetele või tehingutele, mille puhul klient on pärit suure riskiga kolmandast riigist.

10. Kliendi riskiprofiili ning uute ja olemasolevate tehnoloogiatega seotud riskide mõistmine.

10.1. Ärisuhte seire käigus peab asjaomane töötaja koguma piisavalt tõendeid, et vähendada riske, mille kohta on esitatud hoiatus. Selleks peaks asjaomane töötaja uurima ja kasutama järgmist teavet:

a) vara allikas või tehingu rahastamisallikas (tööalane staatus, roll või ametikoht ettevõttes, tööandja, ligikaudne palk, täiendav sissetulekuallikas, tegevusala jne);
b) kliendi vanus;
c) kliendi ja kliendi vastaspoolte asukoht;
d) kliendi tehingute ajalugu;
e) tehingute tüüp;
f) kliendiga seotud mis tahes negatiivne teave;
g) kõik tegurid, mille tõttu klienti peetakse suure riskiga kliendiks;
h) kliendi ja kliendi vastaspoolte vahelised suhted;
i) kliendi ja kliendi elukoha vaheline suhe;
j) muu teave, mis aitab mõista klienti, kliendi tegevust ja tema vastaspooli.

10.2. Asjaomane töötaja peab alati olema teadlik, et uued, olemasolevad ja kujunemisjärgus tehnoloogiad võivad anda kliendile võimaluse varjata oma tegelikku identiteeti või korraldada pettust. Seetõttu peab asjaomane töötaja hindama uute ja kujunemisjärgus tehnoloogiate riske ning maandama neid kliendi registreerimisel ja tehingute seirel.

10.3. Asjaomane töötaja kogub ka teavet kliendi kasutatavate seadmete ja nende asukoha kohta ning lisab selle kliendi KYC-toimikusse.

10.4. Asjaomane töötaja kasutab ka proksikontrolli, et tuvastada, kas kasutaja üritab oma asukohta varjata, ja lisab selle teabe kliendi KYC-toimikusse.

10.5. Asjaomane töötaja registreerib iga virtuaalvaluuta rahakoti aadressi, mida kasutatakse süsteemi sissemaksmiseks või sealt väljavõtmiseks. Kõik need lisatakse samasse virtuaalvaluuta aadresside klastrisse.

11. Otsuste tegemine

11.1. Pärast iga juhtumi läbivaatamist teeb asjaomane töötaja juhtumi kohta kogutud tõendite põhjal lõpliku otsuse selle kohta, kas teatada juhtumist kontaktisikule või lõpetada juhtum, ning esitab lõpliku järelduse, mis toetab tehtud otsust.

11.2. Lõpliku otsuse tegemisel peaks asjaomane töötaja

a) viima lõpule kliendi, kliendi käitumise ja kliendi vastaspoolte uurimise;
b) mõistma kogutud tõendeid ja otsima märke ebatavalisest tegevusest;
c) kaaluma iga tõendusmaterjali eraldi ja kõiki tõendeid kogumina;
d) tõendite vastuolu korral vaatlema neid koos;
e) tegema kindlaks, millised tõendid avaldavad analüüsile kõige suuremat mõju;
f) tegema kindlaks kõik tõendid, millel on analüüsile kõige väiksem mõju;
g) määrama kindlaks, millist teooriat tõendid kõige tugevamalt toetavad.

12. Riskivalmidus ja riikliku taustaga isikutega seotud nõuded

12.1. Mainston määrab riskivalmiduse kindlaks proportsionaalsuse ja mõistlikkuse põhimõtteid järgides ning järgides järgmiste riskide konteksti:

a) pakutavate toodete ja teenuste, nende mahtude ja keerukusega seotud riskid, sealhulgas erinevates jurisdiktsioonides;
b) tooteid ja teenuseid tarbivate klientide riskid ning kliendiportfelli struktuur;
c) müügikanalite riskid, sh allhankega seotud riskid;
d) geograafilised riskid, sealhulgas kohalolek teistes riikides või teenuste osutamine piiriülestele klientidele distantsilt.

12.2. Mainstoni juhatus on otsustanud, et ärisuhteid võib luua väljaspool Euroopa Majanduspiirkonda asuva riigi isikutega või e-residentidega.

12.3. Asjaomane töötaja kontrollib, kas klient või tegelik tulusaaja on rikliku taustaga isik, riikliku taustaga isiku pereliige või isik, kes on teadaolevalt riikliku taustaga isiku lähedane kaastöötaja.

12.4. Asjaomane töötaja keeldub kliendi registreerimisest või juba avatud konto korral blokeerib konto ja teatab sellest kontaktisikule, kui asjaomane töötaja avastab, et:

a) klient kasutab teenust suure riskiga riigist, mis on Mainstoni riskianalüüsi punkti 7.4 kohaselt keelatud riik;
b) klient on Euroopa Liidu või ÜRO sanktsioonide all;
c) kliendile on teadaolevalt esitatud süüdistus rahapesus või terrorismi rahastamises;
d) klient on riikliku taustaga isik, riikliku taustaga isiku pereliige või teadaolevalt riikliku taustaga isiku lähedane kaastöötaja.

13. Rahvusvahelised sanktsioonid

13.1. Asjaomane töötaja kontrollib iga kliendi suhtes rahvusvaheliste sanktsioonide kohaldamist. Kontrolli tuleb teha registreerimisprotsessi käigus ja seejärel regulaarselt. Kui asjaomane töötaja kahtleb, kas leitud tulemused käivad asjaomase kliendi kohta, peab ta konsulteerima kontaktisikuga.

13.2. Kontaktisiku juhiste kohaselt peab asjaomane töötaja küsima kliendilt täiendavat teavet tulemuste õigsuse tagamiseks.

13.3. Klienti ei teavitata sellest, et tema kuulumist rahvusvaheliste sanktsioonide nimekirjadesse uuritakse.

13.4. Asjaomane töötaja saab kontrollida rahvusvaheliste sanktsioonide alla kuuluvate isikute nimekirja, järgides linki
https://www.politsei.ee/en/money-laundering

13.5. Iga üksiku kontrolli puhul registreeritakse järgmised andmed kliendi kohta:

a) kontrolli aeg;
b) kontrolli teostanud töötaja nimi;
c) kontrolli tulemused;
d) võetud meetmed.

13.6. Kui asjaomane töötaja tuvastab kliendi, kelle suhtes kohaldatakse rahvusvahelisi sanktsioone, teavitab ta sellest kontaktisikut. Kui kontaktisik nõustub tulemustega, teavitab kontaktisik sellest juhatust.

14. Kahtlastest ja ebatavalistest tehingutest teatamise kord

14.1. Kui asjaomasel töötajal tekib kahtlus, et ta võib olla seotud kahtlase või ebatavalise tehinguga, peab ta sellest viivitamata teatama kontaktisikule. Lisaks eespool nimetatud tehingu- ja kliendiandmetele tuleks kontaktisikule edastada ka teatamise põhjus ja kliendi identifitseerimisandmed.

14.2. Asjaomane töötaja ei tohi klienti teavitada sellest, et kliendist on teatatud kontaktisikule.

14.3. Mis tahes kahtluse korral peab asjaomane töötaja teavitama kontaktisikut, täites selleks spetsiaalse teatamisvormi. Kontaktisik peab kaaluma iga teadet, et teha kindlaks, kas see annab alust teadmiseks või kahtluseks. Kui selline kahtlus tuvastatakse, saadetakse kontaktisiku koostatud kahtlase tehingu aruanne rahapesu andmebüroole.

14.4. Asjaomane töötaja peab kontaktisikut teavitama, kui ta avastab kiendi mis tahes kahtlase käitumise, mis on seotud rahapesuga, kaasa arvatud juhul, kui

a) klient teeb ülekandeid teistele isikutele erinevates riikides, mis ei vasta isiku tavapärasele tegevusele;
b) klient teatab, et raha võtab välja kolmas isik, kes tegutseb tema nimel ja tema arvel;
c) kliendi profiil ei vasta tema poolt teostatava tehingu laadile.

14.5. Terrorismi rahastamise kahtluse korral peab asjaomane töötaja tuvastama kliendiga seotud riski ja teavitama kontaktisikut, kui kliendiga seotud riske ei ole võimalik mõistlikult vähendada või selgitada.

14.6. Mainston peab viivitamata, kuid mitte hiljem kui kahe tööpäeva jooksul pärast tegevuse või faktide tuvastamist või kahtluse tekkimist teatama rahapesu andmebüroole kahtlastest või ebatavalistest tehingutest,

14.7. Terrorismi rahastamise riskid hõlmavad muu hulgas järgmist:

a) isik on sündinud suure riskiga riigis;
b) isik on suure riskiga riigi kodanik;
c) füüsilise isiku elukoht on suure riskiga riigis või juriidiline isik on asutatud suure riskiga riigis;
d) füüsiline isik on seotud suure riskiga riigis registreeritud juriidilise isiku või muu üksusega.

14.8. Kontaktisik teeb ettevõtte kliendiandmebaasis ja/või dokumentides kliendi nime taha märke „rahapesu / terrorismi rahastamise kahtlus“. Kui kliendi kohta on tehtud märge „rahapesu / terrorismi rahastamise kahtlus“, võib tehinguid teha ainult juhatuse eelneva nõusoleku korral.

15. Rahapesu ja terrorismi rahastamise tõkestamise kohustuste täitmise eest vastutav isik

15.1. Mainstoni määratud juhatuse liige vastutab RTRTS-i ja asjakohaste suuniste järgimise eest. Mainstoni juhatuse otsusega määrati juhatuse määratud liikmeks kontaktisik.

15.2. Juhatus määrab rahapesu ja terrorismi rahastamise tõkestamise ja terrorismi rahastamise vastaste ülesannete ja kohustuste täitmiseks kontaktisiku. Juhatus kooskõlastab kontaktisiku määramise rahapesu andmebürooga.

15.3. Kontaktisik on isik, kes tegutseb rahapesu andmebüroo kontaktisikuna, tagades rahapesu ja terrorismi rahastamise tõkestamiseks kehtestatud meetmete järgimise meie ettevõttes.

15.4. Kontaktisikul peab olema tema ülesannete täitmiseks piisav haridus, ametialane sobivus, võimed, isikuomadused, kogemused ja laitmatu maine.

15.5. Kontaktisiku ülesanded on järgmised:

a) rahapesu tõkestamise nõuete täitmise kontrollimine meie ettevõttes ja töötajate koolitamine;
b) kahtlaste tehingute kohta esitatud aruannete esialgne analüüs ja otsuse tegemine, kas suunata aruanne rahapesu andmebüroole või mitte;
c) rahapesu andmebüroole teabe saatmine rahapesu/terrorismi rahastamise kahtluse korral ning vastamine rahapesu andmebüroo esitatud päringutele ja ettekirjutustele;
d) töötajatelt kahtlaste ja/või ebatavaliste tegevuste kohta saadud teabe kogumine, sellise teabe töötlemine ja dokumenteerimine vastavalt kehtestatud korrale;
e) juhatuse kirjalik teavitamine käesoleva sisekorraeeskirja, suuniste ja muude õigusaktide järgimisega seotud probleemidest ning perioodiliste kirjalike teadete esitamine RTRTS-ist tulenevate nõuete täitmise kohta;
f) kirjalike ülevaadete koostamine juhatusele rahapesu ja terrorismi rahastamise tõkestamise nõuete täitmise kohta.

15.6. Kontaktisiku õigused:

a) teha ettepanekuid käesoleva töökorra, rahapesu tõkestamise poliitika ja muude Mainstoni poliitikate muutmiseks, mis on seotud rahapesuvastase võitluse ja terrorismi rahastamise tõkestamisega;
b) jälgida töötajate tegevust rahapesu ja terrorismi rahastamise tõkestamise meetmete rakendamisel.
c) saada kontaktisiku ülesannete täitmiseks vajalikke andmeid ja teavet;
d) teha ettepanekuid kahtlastest ja ebatavalistest tehingutest teatamise protsessi ümberkorraldamiseks,
e) saada kohapeal väljaõpet.

15.7. Kontaktisik võib saata talle teatavaks saanud teavet või andmeid seoses rahapesu/terrorismi rahastamise kahtlusega ainult järgmistele isikutele:

a) Mainstoni juhatus või juhatuse poolt spetsiaalselt määratud töötaja;
b) rahapesu andmebüroo;
c) eeluurimisasutus kriminaalmenetluses;
d) kohus kohtumääruse või kohtuotsuse alusel.

15.8. Rahapesu või terrorismi rahastamisega seotud põhjendatud kahtluse korral teavitab kontaktisik sellest viivitamata, kuid mitte hiljem kui kahe tööpäeva jooksul rahapesu andmebürood.

15.9. Rahapesu andmebüroole saadetakse aruanne, kasutades veebipõhist aruandevormi aadressil https://fiu.ee/saada-teade. Täidetud aruandevormile tuleb lisada koopiad dokumentidest, mille alusel tehing tehti, ning andmed või dokumentide koopiad, mille alusel isik tuvastati.

15.10. Mainston peab saatma rahapesu andmebüroole teate punkti 4.6 alapunktides a ja f sätestatud asjaolude korral.

15.11. Klienti ei teavitata kunagi tema kohta rahapesu andmebüroole saadetud aruannetest.

15,12. Kui kliendi tegevus ei ole käesoleva töökorra kohaselt täielikult liigitatav rahapesu andmebüroole teatamisele kuuluvaks tegevuseks, tuleb sellise kliendi mis tahes tulevast

tegevust rangemalt kontrollida. Kui kliendi käitumise suhtes on põhjendatud kahtlus, tuleb sellest viivitamatult rahapesu andmebüroole teatada.

15.13. Ükski ettevõte, töötaja, kontaktisik ega mõni muu Mainstoni nimel tegutsev isik ei vastuta kahju eest, mis võib tekkida tehingu tegemata jätmisest või hilinemisest, mida klient kannab terrorismi rahastamise või rahapesu kahtluse tõttu, millest on heauskselt teatatud rahapesu andmebüroole.

15.14. Rahapesu andmebüroole teatamist ja asjakohase teabe saatmist ei käsitata seaduses või lepingus sätestatud konfidentsiaalsuskohustuse rikkumisena ning nende isikute suhtes ei kohaldata õigusaktides või lepingus sätestatud vastutust sellise asjakohase teabe avalikustamise eest.

16. Auditeerimine ja sisekontroll

16.1. Mainston määrab audiitori, kes auditeerib ettevõtte raamatupidamise aastaaruandeid.

16.2. Audiitorfirmat ei nimetata kauemaks kui 5 aastaks.

16.3. Mainstoni juhatus määrab siseauditiüksuse ülesannete täitmiseks siseaudiitori.

16.4. Siseaudiitor ei tohi täita ülesandeid, mis põhjustavad või võivad põhjustada huvide konflikti.

16.5. Siseaudiitori ülesanne on kontrollida, kas Mainstoni ja selle juhtide tegevus vastab

a) õigusaktidega kehtestatud nõuetele;
b) kõikidele rahapesu andmebüroo poolt väljastatud vastavusteatistele;
c) teenuseosutaja juhtorganite otsustele;
d) sisekorraeeskirjadele;
e) teenuseosutaja sõlmitud kokkulepetele ja parimatele tavadele.

16.6. Mainston tagab, et siseaudiitoril on kõik õigused ja töötingimused, mis on vajalikud tema ülesannete täitmiseks, sealhulgas õigus saada selgitusi ja teavet teenuseosutaja juhtidelt ja töötajatelt ning jälgida avastatud puuduste kõrvaldamist ja tehtud ettepanekute elluviimist.

17. Töötajate koolitus

17.1. Mainstoni töötajatele viib rahapesu ja terrorismi rahastamise ennetamise koolitust läbi kontaktisik või muu rahapesuvastane ekspert.

17.2. Töötajaid tuleb teavitada rahapesu ja terrorismi rahastamise tõkestamise nõuetest ning hoolsusmeetmete rakendamisest ja rahapesukahtlustest teatamisest. See hõlmab järgmist:

a) ettevõtte riskivalmiduses määratletud põhimõtted;
b) ettevõtte tegevusest ja pakutavatest teenustest tulenevad riskid;
c) käesolevas töökorras sätestatud kohustused;
d) rahapesu ja terrorismi rahastamise tänapäevased meetodid ja konkreetsed liigid/juhtumid ning nendega seotud riskid;
e) võimaliku rahapesu või terrorismi rahastamisega seotud tegevuste tuvastamine ning suunised selle kohta, kuidas sellistes olukordades tegutseda.

17.3. Kontaktisik vastutab regulaarse koolituse läbiviimise eest. Iga asjaomane töötaja kinnitab osalemist oma allkirjaga. Koolitusi soovitatakse korraldada vajaduse korral, kuid mitte vähem kui üks kord aastas.

17.4. Kontaktisik on kohustatud andma kõigile uutele asjaomastele töötajatele ettenähtud korras pärast töölepingu sõlmimist hiljemalt ühe nädala jooksul alates asjaomase töötaja tööle asumisest juhiseid ja sissejuhatavat koolitust ning tutvustama uuele asjaomasele töötajale allkirja vastu käesolevat töökorda.

17.5. Kontaktisikul on õigus esitada juhatusele ettepanekuid selle kohta, milliseid koolitusi tuleks korraldada.

18. Teabe registreerimise ja dokumenteerimise kohustuse rikkumine

18.1. Käesoleva töökorra ning rahapesu ja terrorismi rahastamise tõkestamise seadusega ettenähtud teabe registreerimise ja dokumenteerimise kohustuse rikkumise eest karistatakse vastavalt seadusele.

19. Rahapesu andmebüroo taotlused

19.1. Rahapesu andmebüroo järelevalveametniku taotlusel esitatakse inspektoritele viivitamata kõik vajalikud dokumendid ja teave.

20. Allhanked

20.1. Käesoleva töökorra kohaste kohustuste allhankimine on lubatud ainult juhatuse vastava otsuse alusel. Allhankeid võib teha ainult isikult, kes kohaldab käesolevas töökorras ja RTRTS-is sätestatud hoolsusmeetmeid ning tingimusel, et vastav osapool on valmis alluma Mainstoni üle teostatava järelevalvega sarnasele järelevalvele kooskõlas RTRTS-iga.

20.2. Tegevuse sisseostmiseks sõlmib kohustatud isik teise isikuga kirjaliku lepingu. Leping peab tagama

a) tegevuse sisseostmisega seotud õiguste ja kohustuste jagamise;
b) et tegevuse sisseostmine ei takista Minstoni tegevust ega seaduses ja suunistes sätestatud kohustuste täitmist;
c) et teine isik täidab kõik ettevõtte kohustused, mis on seotud tegevuse sisseostmisega;
d) et tegevuse sisseostmine ei takista järelevalve teostamist Mainstoni üle;
e) et pädev asutus saab teostada järelevalvet sisseostetud tegevust teostava isiku üle;
f) sisseostetavat tegevust teostava isiku nõutava teadmiste ja oskuste taseme ning suutlikkuse;
g) et Mainstonil on piiramatu õigus kontrollida, kas allhanke korras tegutsev isik vastab nõuetele;
h) et kogutud dokumendid ja andmed vastaksid seadusest ja asjakohastest suunistest tulenevatele nõuetele;
i) kohustatud isiku õiguse lõpetada vajaduse korral allhankeleping teise isikuga, kui viimane ei ole täitnud lepingulisi kohustusi või ei ole neid nõuetekohaselt täitnud.

20.3. Mainston või asjaomane töötaja võib tugineda kolmanda isiku poolt kogutud andmetele ja dokumentidele, kui ettevõte või asjaomane töötaja

a) saab kolmandatelt isikutelt teavet ärisuhet loova või tehingut sooritava isiku, tema esindaja ja tegeliku tulusaaja isiku kohta ning ärisuhte või tehingu eesmärgi ja laadi kohta;

b) on taganud, et vajaduse korral on ettevõttel või asjaomasel töötajal võimalik kohe saada kõik andmed ja dokumendid, mille kolmas isik on kogunud;

c) on kindlaks teinud, et kolmas isik on kohustatud täitma ja tegelikult täidab asjaomases seaduses kehtestatud nõuetega võrdseid nõudeid ning on nõuete täitmise osas riikliku järelevalve all või on valmis seda tegema.

20.4. Kui isiku tuvastamine ja andmete kontrollimine toimub punktis 4 kirjeldatud infotehnoloogiliste vahendite abil, võib isiku tuvastamise ja andmete kontrollimise ning küsimustiku koostamise teostada asjaomane töötaja, Mainstoni partner või automatiseeritud süsteem.

21. Huvide konflikti vältimine

21.1. Huvide konflikti tuvastamiseks ja haldamiseks Mainston

a) on määratlenud riskivalmiduse ja oma tegevusest tulenevad riskid;

b) väldib olukordi, kus omanike, juhtide, töötajate ja klientide isiklikud huvid on vastuolus ettevõtte huvidega;

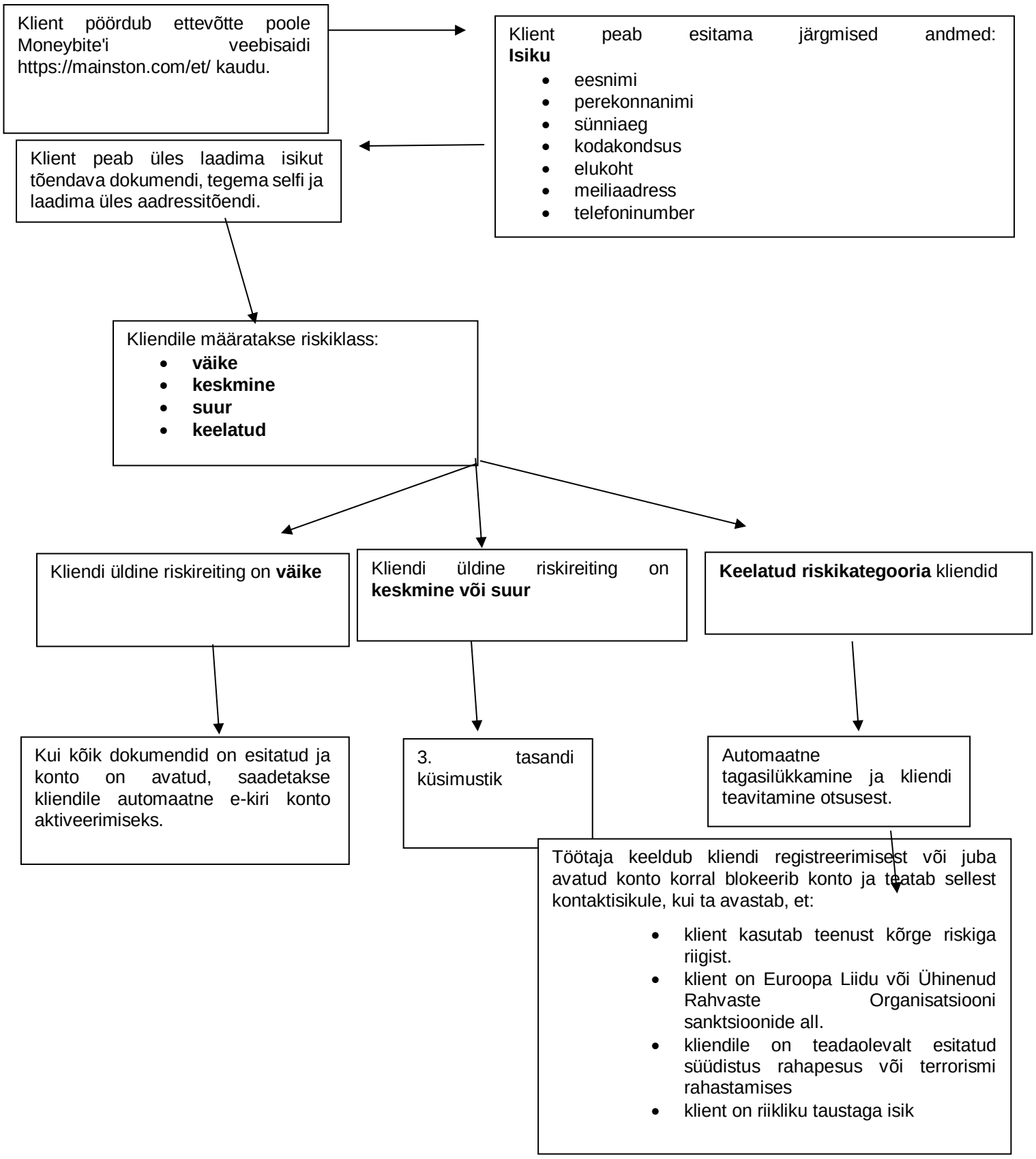
c) palub töötajatel ja juhtidel esitada andmed oma majanduslike huvide kohta, mis võivad tekitada huvide konflikti. Mainston ajakohastab neid majanduslike huvide deklaratsioone regulaarselt;

d) tuvastab ja analüüsib, kas isikutel, kes juhatavad kliendi Mainstonisse, on huvide konflikt ettevõtte ja kliendi vahel. Sellise huvide konflikti ohjamise meetmeks võib olla sellise ärisuhte loomise vältimine.

22. Käesoleva töökorra muutmine

22.1. Käesolevat töökorda võib muuta juhatuse otsusega, mis põhineb häälteenamusel vastavalt Mainstoni põhikirjale.

Lisa 1: Mainston International OÜ kliendi registreerimise skeem, B2C



Füüsilise isiku tuvastamise aluseks on järgmised kehtivad dokumendid:

a) isikutunnistus;
b) pass;
c) diplomaatiline pass;
d) Euroopa Liidu kodaniku ID-kaart;
e) juhiluba, kui dokumendil on selle omaniku nimi, foto või näokujutis, allkiri või allkirjakujutis ja sünniaeg või isikukood.

Ettevõtte poolt AWS-is salvestatud kogutud andmed hõlmavad isiku nime, sünnikuupäeva ja aadressi, kuid kõik isikuandmed, nagu biomeetrilised andmed ja isikut tõendavad dokumendid (nagu ID-kaardi numbrid või pildid), kogub ja salvestab Onfido (turvaline, tehisintellektipõhine identiteedi kontrollimise lahendus nende SDK kaudu ja Mainston saab API kaudu ainult viite sellele teabele.

Kogutud andmed, mida tuleb säilitada, hõlmavad järgmist:

a) teave ärisuhte loomisest või juhuti tehtava tehingu sooritamisest keeldumise asjaolude kohta;
b) teave selle kohta, kui hoolsusmeetmeid ei ole võimalik infotehnoloogiliste vahendite abil võtta;
c) dokumentide originaalid või koopiad, mis on aluseks isikusamasuse kindlakstegemisele ja esitatud teabe kontrollimisele;
d) tehingu kuupäev või periood ja tehingu sisu kirjeldus;
e) ettevõtte nimel peetavate maksekontode nimekiri koos iga maksekonto unikaalse tunnuse ja kontohalduri nimega;
f) teave, mille alusel täidetakse aruandluskohustust rahapesu andmebüroo ees.

Lisa 2: Mainston International OÜ kliendi registreerimise skeem, B2B

Enne ettevõtte konto registreerimist tuleb klient registreerida füüsilise isikuna. Registreerimine toimub 1. lisa alusel.
Ettevõtte konto avamisel küsitakse kliendilt järgmised lisaandmed: