Rahapesu Andmebüroo juhi käskkirja „Juhendi "Rahapesu ja terrorismi rahastamise riskide juhtimine ning hoolsusmeetmete kohaldamine Rahapesu Andmebüroo järelevalvatavatele kohustatud isikutele" kinnitamine“ lisa

Rahapesu ja terrorismi rahastamise riskide juhtimine ning hoolsusmeetmete kohaldamine Rahapesu Andmebüroo järelevalvatavatele kohustatud isikutele

Rahapesu Andmebüroo

2026

Sisukord

1. Juhendi eesmärk, kohaldamisala ja põhimõtted 4
Juhendi eesmärk ja kohaldamisala ... 4
Juhend on suunatud järgmistele kohustatud isikutele: ... 4
Juhendi põhimõtted ... 7
2. Organisatsiooni ülesehitus ja riskide juhtimine 9
Juhatuse tegevus ja vastutava juhatuse liikme ülesanded ... 10
Organisatsiooniline ülesehitus ... 12
I kaitseliin ... 14
II kaitseliin, sealhulgas kontaktisiku funktsioon ... 15
III kaitseliin ... 17
Koolitus ... 18
3. Riskide juhtimine 19
Riskihinnang ja riskiisu ... 19
Protseduurireeglid ja sisekontrollieeskiri ... 26
4. Hoolsusmeetmed 30
Hoolsusmeetmete kohaldamise erisused ... 32
Riskipõhine lähenemine hoolsusmeetmete kohaldamisel ja kliendi riskiprofiil ... 35
Hoolsusmeetmed ärisuhte loomisel või juhuti tehtava tehingu puhul ... 39
Füüsilise isiku ja esindaja isikusamasuse tuvastamine ning andmete kontrollimine ... 41
Füüsilise isiku ja esindaja isikusamasuse tuvastamine ... 41
Füüsilise isiku ja esindaja isikusamasuse tuvastamise käigus saadud teabe kontrollimine ja kontrollimise viis ... 44
Füüsilise ja juriidilise isiku, s esindaja ja tegeliku kasusaaja isikusamasuse tuvastamise aeg ... 44
Usaldusväärne ja sõltumatu allikas füüsilise isiku isikusamasuse tuvastamiseks esitatud andmete kontrollimisel ... 45
Kaks erinevat allikat füüsilise isiku isikusamasuse tuvastamiseks esitatud andmete kontrollimisel ... 46
Juriidilise isiku isikusamasuse tuvastamine ... 47
Juriidilise isiku isikusamasuse tuvastamise käigus saadud teabe kontrollimine ja kontrollimise viis ... 49
Usaldusväärne ja sõltumatu allikas juriidilise isiku isikusamasuse tuvastamise käigus saadud teabe kontrollimisel ... 49
Kaks erinevat allikat juriidilise isiku isikusamasuse tuvastamise käigus saadud teabe kontrollimisel ... 50
Legaliseerimine ja apostilliga kinnitamine ning dokumentide keel ... 50
Füüsilise ja juriidilise isiku tegeliku kasusaaja tuvastamine ... 51
Juriidilisest isikust tegeliku kasusaaja tuvastamisel kogutud andmete kontrollimine ... 54

Riikliku taustaga isik, sealhulgas tema perekonnaliige või lähedane kaastöötaja 56
Rikkuse päritolu tuvastamine 59
Tehingus kasutatud vara päritolu tuvastamine 60
Ärisuhte või juhuti tehtava tehingu eesmärgi ja olemuse tuvastamine 61
Tegevusala 63
Maksetavad 64
Olulisemad tehingupartnerid 64
Finantseerimisasutuste erisus isikusamasuse (kaug)tuvastamisel 66
Lõplikult kasusaava isiku osas hoolsusmeetmete kohaldamata jätmine korrespondentsuhetes finantseerimisasutuste puhul 67
Hoolsusmeetmed ärisuhte kestel 68
Rakendatavad hoolsusmeetmed ärisuhte seirel ja kestel 68
Andmete uuendamine 69
Ärisuhte seire 70
Reaalajas jälgimine 72
Järelkontroll 74
Reaalajas tehingute ja klientide kontrollimine ja järelkontroll mittefinantssektoris 75
Tehingus kasutatud vahendite allika ja päritolu tuvastamine 76
Kõrgemale riskile viitavad tehingud 77
Lihtsustatud hoolsusmeetmed 78
Tugevdatud hoolsusmeetmed 79
Teise isiku kogutud andmetele tuginemine ja hoolsusmeetmete kohaldamise edasiandmine 84
Teise isiku kogutud andmetele tuginemine 84
Tegevuste edasiandmine 86
Hoolsusmeetmete kohaldamine kokkuvõtlikult 87
5. Ärisuhte loomisest või juhuti tehingu tegemisest keeldumine ning ärisuhte (erakorraline lõpetamine) 88
Ärisuhte loomisest või tehingu tegemisest keeldumine 88
Tehingu edasilükkamine 88
Ärisuhte (erakorraline) lõpetamine 88
6. Andmete registreerimine ja säilitamine 89
7. Teatamiskohustus 91
8. Rahapesu Andmebüroo pädevus 93
9. Lisad 95

1. Juhendi eesmärk, kohaldamisala ja põhimõtted

1.1. Juhendi eesmärk ja kohaldamisala

1.1.1. Käesolev juhend koosneb põhiosast ja lisadest. Põhiosas sätestatakse rahapesu ja terrorismi rahastamise tõkestamisega seotud põhimõtted, nõuded ning nende rakendamise üldised suunised. Lisad sisaldavad juhendi rakendamist toetavaid täiendavaid materjale, sealhulgas selgitusi, näiteid ja muid abivahendeid.

1.1.2. Juhendi eesmärk on suurendada kohustatud isikute võimekust rahapesu ja terrorismi rahastamise ennetamisel ja tõkestamisel, et vähendada Eesti rahandussüsteemi ja majandusruumi haavatavust ning edendada ausat ja läbipaistvat ettevõtluskeskkonda.

1.1.3. Käesolev juhend on soovituslik dokument, millele kohaldub põhimõte „täidan või selgitan“. See tähendab, et kohustatud isik peab vajadusel põhjendama, miks ta juhendist sätestatut ei rakenda või rakendab osaliselt, sealhulgas millele tugineb kohustatud isiku proportsionaalsuse hinnang. Juhend on suunatud Rahapesu Andmebüroo järelevalve all olevatele kohustatud isikutele, kes on loetletud juhendi punktis 1.2.[1] Kui juhendis ei ole erisusi välja toodud, kehtivad juhendi suunised kõigile juhendis nimetatud kohustatud isikutele. Lisaks kehtib juhend Rahapesu Andmebüroo tegevusluba omavatele Eesti filiaalidele, mida haldavad välisriigi kohustatud isikud.

1.1.4. Kuigi juhend on soovituslik, tugineb see rahapesu ja terrorismi rahastamise tõkestamise seaduse (edaspidi RahaPTS) nõuetele ning seetõttu kasutatakse juhendis läbivalt ka kohustuslikku kõneviisi.

1.1.5. Juhendis antakse ülevaade RahaPTS-i ning sellega seotud õigusaktide nõuetest ja nende täitmisest. Juhend suunab kohustatud isikuid looma ja toimivana hoidma rahapesu ja terrorismi rahastamise riskide juhtimiseks vajalikku protsesside ülesehitust.

1.2. Juhend on suunatud järgmistele kohustatud isikutele:

1.2.1. Finantseerimisasutused, kes omavad Rahapesu Andmebüroo tegevusluba ja on Rahapesu Andmebüroo järelevalve all[2]:

Finantseerimis-asutus	Võimalik osutada teenust tarbijatele[3]	Võimalik osutada teenust juriidi-listele isikutele	Eritingimused
Valuutavahetus-teenuse pakkuja	JAH	JAH	Rahapesu Andmebüroo tegevusluba juhul, kui teenuseosutajal on reaalne kontor või koht, kus klient saab

[1] Notarite ja advokaatide üle teostab rahapesu ja terrorismi rahastamise tõkestamise seaduse nõuete täitmise osas järelevalvet vastavalt Notarite Koda ja Eesti Advokatuuri juhatus. Käesolevas juhendis kirjeldatud põhimõtted võivad olla kohased ka notaritele ja advokaatidele RahaPTS-ist tulenevate kohustuste täitmisel.
[2] RahaPTS § 6 lg 2 ja krediidiasutuste seadus § 6 lg 1.
[3] Tulenevalt Tarbijakaitseseaduse § 2 lg 1 p-st 1 on tarbija füüsiline isik, kes tegutseb eesmärgil, mis ei ole seotud tema majandus- või kutsetegevusega.

			kohapeal teenust tarbida sularaha-sularaha vastu. Muul juhul on vajalik taotleda Finantsinspektsiooni väljastatavat tegevusluba.
Hoiu-laenuühistu	JAH	JAH	Hoiu-laenuühistu puhul ei ole tegemist tarbijate ja juriidiliste isikutega, vaid ühistu liikmetega. Mitte ühegi hoiu-laenuühistu sõlmitava või vahendatava krediidilepingu krediidi kulukuse määr ei ületa krediidi andmise ajal Eesti Panga viimati avaldatud viimase 6 kuu keskmist krediidiasutuste poolt füüsilistele isikutele antud tarbimislaenude kulukuse määra. Hoiu-laenuühistu liikmete arv on väiksem kui 3000. Eespool nimetatud tingimustest kõrvale kaldumisel on vajalik tegevuseks taotleda Finantsinspektsiooni väljastatavat tegevusluba.
Liisinguandja	EI	JAH	Tarbijatele teenuse osutamiseks on vajalik taotleda Finantsinspektsiooni väljastatavat tegevusluba.
Laenuandja, sealhulgas hüpoteeklaenud, faktooring ja muud äritehingute finantseerimise tehingud	EI	JAH	Teenuse osutamiseks tarbjatele on vajalik taotleda Finantsinspektsiooni väljastatavat tegevusluba.
Tagatis- ja garantiitehingute teenuse pakkuja	EI	JAH	Tarbijatele ei ole lubatud teenust osutada Rahapesu Andmebüroo tegevusloa alusel.
Fondivalitseja	JAH	JAH	Investeerimisfondide seaduse (IFS) § 453 mõistes tegevusloata väikefondi valitseja. Eeldab eelnevat registreerimist Finantsinspektsioonis.

			Fondi(de) vara kogumaht, sealhulgas kõigi fondide finantsvõimenduse kasutamise teel omandatud vara, ei ületa 100 miljonit eurot või fondi(de) vara kogumaht ei ületa 500 miljonit eurot, tingimusel et alternatiivfondide portfell koosneb finantsvõimenduseta alternatiivfondidest ja 5 aasta jooksul pärast igasse alternatiivfondi investeeringute tegemise kuupäeva ei ole võimalik kasutada osakute või aktsiate tagasivõtmise õigust (IFS § 3 lg 6).
Vara valitsemine (muu finantseerimisasutus)	JAH	JAH	Vara valitsemise teenuse osutamiseks seoses väärtpaberitega on vajalik taotleda Finantsinspektsiooni väljastatavat tegevusluba.
Klientide nõustamine			Klientide nõustamine majandustegevust puudutavates küsimustes ja äriühingute ühinemise, jagunemise või nendes osaluse omandamisega seotud tehingud ja toimingud.

1.2.2. Mittefinantseerimisasutused, kelleks on:

1.2.2.1. hasartmängu korraldajad, välja arvatud kaubanduslik loterii;

1.2.2.2. isikud, kes vahendavad kinnisasja ostu või müüki. Kui tegu on näiteks kinnisvara arendajaga, kes ei vahenda kinnisasja ostu või müüki, siis antud isik selle punkti alla ei liigitu;

1.2.2.3. isikud, kes vahendavad kinnisasja kasutustehinguid, kui tehinguga kokku lepitav kasutustasu on vähemalt 10 000 eurot kuus;

1.2.2.4. kauplejad, kui neile tasutakse või nad tasuvad sularahas vähemalt 10 000 eurot või sellega võrdväärse summa muus vääringus, sõltumata sellest, kas rahaline kohustus täidetakse tehingus ühe maksena või mitme seotud maksena kuni ühe aasta jooksul, kui seadus ei sätesta teisiti;

1.2.2.5. isikud, kes tegelevad vääriskivide, väärismetalli, väärismetalltoodete, välja arvatud tootmise, teaduse ja meditsiini vajadusteks kasutatavad väärismetallid ja väärismetalltooted, kokkuostu või hulgimüügiga;

1.2.2.6. vandeaudiitorid audiitorteenuse osutamisel ja raamatupidamisteenuse pakkujad;

1.2.2.7. raamatupidamise või maksustamise valdkonnas nõustamisteenuse pakkujad, kes osutavad teenuseid iseseisva majandus- või kutsetegevusena (ettevõttesiseselt tegutsevaid isikuid käesoleva punkti tähenduses teenusepakkujatena ei käsitata);

1.2.2.8. usaldushalduse ja äriühingute teenuse pakkujad;

1.2.2.9. pandimajapidajad;

1.2.2.10. kunstiteostega kauplejad ja isikud, kes vahendavad kunstiteoseid või ladustavad neid tolli vabatsoonis, kui neile sellega seoses tasutakse või nad tasuvad vähemalt 10 000 eurot korraga või mitme seotud maksena ühe aasta jooksul;

1.2.2.11. mittetulundusühingud mittetulundusühingute seaduse tähenduses ja teistele juriidilistele isikutele, kellele kohaldatakse mittetulundusühingute seaduse sätteid, ning sihtasutustele sihtasutuste seaduse tähenduses, kui neile tasutakse või nad tasuvad sularahas üle 5000 euro või sellega võrdväärse summa muus vääringus, sõltumata, kas tasutakse ühe maksena või mitme seotud maksena kuni ühe aasta jooksul või kui klient või tehingus osalev isik on seotud riigiga või jurisdiktsiooniga, mis rahastab või toetab terrorismi või mille territooriumil tegutsevad Euroopa Liidu või ÜRO poolt kindlaks määratud terroristlikud organisatsioonid.;

1.2.2.12. piiriülest sularaha ja väärtpaberite veo teenust osutavad ettevõtjad;

1.2.2.13. kohtutäiturid, pankrotihaldurid, ajutised pankrotihaldurid ja muu õigusteenuse osutajad majandus-, kutse- või ametitegevuses, kui ta tegutseb finants- või kinnisvaratehingus oma kliendi eest ja nimel. Samuti eelnimetatud isiku majandus-, kutse- või ametitegevuses, kui ta juhendab tehingu kavandamist või selle tegemist või teeb ametitoimingut või osutab ametiteenust, mis on seotud: kinnisasja, ettevõtte või äriühingu aktsiate või osade ostu või müügiga; kliendi raha, väärtpaberite või muu vara haldamisega; makse-, hoiu- või väärtpaberikontode avamise või haldamisega; äriühingu asutamiseks, tegevuseks või juhtimiseks vajalike vahendite hankimisega; usaldushalduse, äriühingu, sihtasutuse või muu juriidilise isiku staatust mitteomava isikute ühenduse asutamise, tegevuse või juhtimisega.

1.3. **Juhendi põhimõtted**

1.3.1. Juhendi kohaldamisel tuleb arvestada kehtivates õigusaktides sätestatud nõuetega ning rahvusvahelise praktikaga[4], samuti RahaPTS-iga vahetult seotud õigusaktides ja teistes Rahapesu Andmebüroo juhendites kirjeldatud nõuetega.

1.3.2. Õigusaktide kohustuslike nõuete ning juhendi vastuolu korral kohaldatakse RahaPTS-i ja sellega vahetult seotud õigusakte nende mõttest ja sisust lähtudes. Ingliskeelse RahaPTS-i puhul tuleb lähtuda selle algsest eestikeelsest originaalsõnastusest ning mõttest.

[4] Rahapesu ja terrorismi rahastamise tõkestamise valdkonnas kehtivad standardid ja parimad tavad, mis on välja töötatud rahvusvaheliste organisatsioonide poolt nagu FATF ja The Office of Foreign Assets Control.

1.3.3. Juhendi täitmisel tuleb lähtuda proportsionaalsuse ja riskipõhise lähenemise põhimõtetest ning arvestada kohustatud isiku tegevuse eripäradest tulenevaid rahapesu ja terrorismi rahastamise riske. Juhendi täitmisel arvestatakse kohustatud isiku suurust ning tema tegevuse ja osutatavate teenuste olemust, ulatust ja keerukust ning:

1.3.3.1. pakutavate toodete ja teenustega ning nende mahu ja keerukusega seotud riskidega, sealhulgas erinevate jurisdiktsioonidega seotud riskidega;

1.3.3.2. tooteid ja teenuseid tarbivate klientidega seotud riskidega ning kliendiportfelli struktuuriga[5];

1.3.3.3. müügikanalitega seotud riskidega, sealhulgas edasiandmisega kaasnevate riskidega;

1.3.3.4. riikide, geograafiliste piirkondade või jurisdiktsioonidega seonduvate riskidega, sealhulgas kohalolekuga teistes riikides või teenuste osutamine distantsilt piiriülestele klientidele;

1.3.3.5. tehingute, süsteemide ja tehnoloogiaga seotud riskidega.

1.3.4. Käesolevas juhendis esitatud näited, loetelud ja kirjeldused ei ole ammendavad.

1.3.5. Riskide hindamisel tuleb arvestada kohustatud isiku suurust turul ning Eesti[6] ja Euroopa Liidu[7] rahapesu ja terrorismi rahastamise riske, mille on tuvastanud järelevalveasutused, õiguskaitseasutused ja Euroopa Liidu asutused. Kontserni puhul tuleb arvestada ka teistes riikides kaasnevate riskidega ning isiku suurusega vastava riigi finantssektoris. Mida suurem on kohustatud isik, seda suuremad on tema tegevusega kaasnevad rahapesu ja terrorismi rahastamise riskid ning seda sagedamini tuleb kohaldada juhendis kirjeldatud meetmeid või seda ulatuslikumad peavad meetmed olema.

1.3.6. Termini „mõistlik aeg“ tõlgendamisel tuleb juhendis lähtuda riskipõhisest lähenemisest. Mõistlikku aega ei saa tulenevalt proportsionaalsuse ja riskipõhisel lähenemise põhimõttest kalendripäevades määratleda. Mõistliku aja all tuleb silmas pidada, et see on ajavahemik, mille jooksul kohustatud isik, arvestades konkreetse olukorra rahapesu ja terrorismi rahastamise riski, tegutseb viivitamata ja proportsionaalselt, et risk ei realiseeruks.

1.3.7. Juhendi kohaldamisel tekkivate rakenduslike ja tõlgenduslike probleemide korral tuleb lähtuda mõistlikkuse põhimõttest, tõlgendades juhendi punkte koosmõjus ja juhendi eesmärki silmas pidades. Samuti tuleb tegutseda heas usus ja kooskõlas valdkonnas eeldatava hoolsusega.

---

[5] Klientide struktuur ehk klientide koosseis hõlmab klientide tüüpe ja omadusi, kellega finantseerimisasutus tegeleb, näiteks füüsilised isikud, eraõiguslikud juriidilised isikud, mittetulundusühingud. Samuti hõlmab see klientide geograafilist asukohta, tehingute mahtu ja keerukust ning muid riskitegureid.

[6] Eesti rahapesu ja terrorismi rahastamise siseriiklik riskihinnang (inglise keeles *National Risk Assessment* ehk NRA): https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/riskihinnangud

[7] Euroopa Komisjoni riskihinnang (inglise keeles *Supranational Risk Assessment* ehk SNRA): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554

1.3.8. Rahapesu ja terrorismi rahastamise riskide tuvastamiseks ja juhtimiseks võib teatud asjaoludel olla vajalik kohaldada juhendist erinevaid või täiendavaid meetmeid. Õigusaktide täitmata jätmist ei saa põhjendada üksnes juhendi sätete sõnasõnalise järgimisega.

2. Organisatsiooni ülesehitus ja riskide juhtimine

2.1. Organisatsiooniline ülesehitus peab võimaldama efektiivselt tõkestada rahapesu ja terrorismi rahastamist. Rahapesu ja terrorismi rahastamise riske tuleb hinnata eraldiseisvalt ning samuti ka nende omavahelises koosmõjus. Nende riskide juhtimine peab olema lahutamatu osa organisatsiooni üldisest juhtimisest ja riskijuhtimissüsteemist.

2.2. Juhatus tagab, et töötajad ja käsunduslepinguga töötavad isikud tegutsevad keskkonnas, kus ollakse teadlik rahapesu ja terrorismi rahastamise tõkestamise nõuetest ja nendega kaasnevatest kohustustest. Juhatuse liikme(te)l, töötajatel ja käsunduslepinguga töötavatel isikutel, kes on otseselt seotud RahaPTS-i ja käesoleva juhendi rakendamisega, peavad olema oma ülesannete täitmiseks asjakohased teadmised, oskused ja teatud juhtudel kogemused (näiteks kontaktisik). Samuti peavad nad suutma õigusakte ja juhendit täita korrektselt, lähtudes oma vastutusalast. Lisaks peavad nimetatud isikud läbima vastava koolituse või olema muul viisil saanud vajalikud juhised.

2.3. Käsunduslepinguga tegutsevad isikud, kes täidavad RahaPTS-ist tulenevaid ülesandeid kohustatud isiku nimel, võivad lähtuda kohustatud isiku kehtestatud riskijuhtimise ja sisekontrolli süsteemist ning ei pea ise eraldi koostama riskihinnangut, riskiisu dokumenti, protseduurireegleid ega sisekontrollieeskirja. Küll aga võib käsunduslepingu alusel tegutsev isik olla ka ise kohustatud isik (näiteks maakler). Kui käsunduslepingu alusel tegutsev isik tuvastab, et kohustatud isikul, kelle alluvuses ta käsundit täidab, puuduvad korrektsed sisemised dokumendid ja protsessid, peab käsunduslepingu alusel töötav isik koostama vajalikud dokumendid, sealhulgas protseduurireeglid, sisekontrollieeskirja, riskihinnangu ja riskiisu.

2.4. Riskijuhtimine peab vastama proportsionaalsuse põhimõttele ehk arvestama organisatsiooni suurust ja tegevust, osutatavate teenuste olemust, ulatus ja keerukust, samuti ettevõtte riskiisu ja tegevusega kaasnevaid riske. See tähendab, et rakendatavad meetmed peavad olema piisavad ja põhjendatud, kuid mitte ebaproportsionaalselt koormavad.

2.5. Proportsionaalsuse põhimõte kehtib ka väikeste ning ühe töötajaga kohustatud isikute suhtes.

Ka lihtsama struktuuriga ettevõttel peavad rahapesu ja terrorismi rahastamise tõkestamise meetmed olema rakendatud, kuid nende ulatus ja vorm peavad vastama ettevõtte suurusele, tegevusmahule ja riskiastmele.

Näiteks võib riskijuhtimine, sisekontroll ja otsustusprotsesside korraldus olla lihtsam ning vähem formaliseeritud kui keerulisema struktuuriga organisatsioonis. Samas peab ettevõte

suutma tuvastada ja hinnata riske, rakendada asjakohaseid hoolsusmeetmeid, dokumenteerida olulisi otsuseid ning vajadusel tõendada nõuete täitmist.

2.6. **Juhatuse[8] tegevus ja vastutava juhatuse liikme ülesanded**

2.7. Kui kohustatud isikul on rohkem kui üks juhatuse liige, määratakse juhatuse liige, kes vastutab RahaPTS-i ning selle alusel kehtestatud õigusaktide ja juhendite rakendamise eest[9].

2.8. Juhatuse pädevus ja vastutus peavad olema läbipaistvalt ja üheselt mõistetavalt kirjeldatud juhatuse liikmete ülesandeid reguleerivas dokumentatsioonis (nt juhatuse liikmete ametijuhendid, teenistuslepingud, vastutusvaldkonda kirjeldav dokument vms).

2.9. Vastutava juhatuse liikme määramisel tuleb tuvastada võimalikud huvide konfliktid, neid arvestada ja vajadusel rakendada asjakohaseid meetmeid nende vältimiseks või maandamiseks.

2.10. Juhatus peab mõistma huvide konflikti olemust, suutma seda oma tegevuses õigeaegselt tuvastada ja hinnata ning rakendada asjakohaseid meetmeid sellega seotud riskide maandamiseks. See kehtib ka olukorras, kus üks ja sama isik täidab ettevõttes mitut rolli või funktsiooni (sealhulgas tulenevalt kolme kaitseliini põhimõttest, ärihuvidest ja/või rahapesu ja terrorismi rahastamise tõkestamise nõuetest).

2.11. **Vastutav juhatuse liige peab:**

2.11.1. oma tegevuses üles näitama vajalikku asjatundlikkust, ausust, täpsust ja hoolikust, et tagada rahapesu ja terrorismi rahastamise tõkestamise nõuete täitmine;

2.11.2. pühendama piisavalt aega ja tagama piisavalt vahendeid rahapesu ja terrorismi rahastamise tõkestamisega seotud ülesannete tõhusaks täitmiseks;

2.11.3. tagama, et kogu juhatus on teadlik rahapesu ja terrorismi rahastamise riskidest ning nende mõjust kogu äritegevusele.

2.12. **Juhatus peab määratlema riskiisu ja koostama riskihinnangu. Selleks juhatus muu hulgas:**

2.12.1. lähtub käesolevas juhendis esitatud riskiisu ja riskihinnangu koostamise põhimõtetest (juhendi punktid 3.5. - 3.23.) ning tagab riskiisu ja riskihinnangu dokumentide koostamise ja nende regulaarse ülevaatamise;

2.12.2. tagab riskijuhtimise meetmete olemasolu, et hinnata riskiisu dokumendi järgimist ning tuvastada riskide muutused mõistliku aja jooksul (sealhulgas tuleb kajastada need riskihinnangu dokumendis). Kõrvalekalde ilmnemisel tegutseb juhatus või juhatuse tasandil määratud vastutav isik viivitamata ning teeb vajalikud muudatused organisatsioonilises ülesehituses ja protsessides, vajadusel peatades teenuste osutamise osaliselt või täielikult kuni riskide maandamiseni;

[8] Kui tegemist on filiaaliga, kellel ei ole juhatust, tuleb juhendi kontekstis lugeda juhatuseks filiaali juhti.
[9] Vastav kohustus peab kajastuma juhatuse liikme lepingus või ettevõtte vastava organi otsuses.

2.12.3. Juhatus peab kehtestama ja regulaarselt üle vaatama rahapesu ja terrorismi rahastamisega seotud riskide võtmise, juhtimise, jälgimise ning maandamise põhimõtted ja protseduurid. Need peavad hõlmama nii olemasolevaid kui ka potentsiaalseid riske. Juhatus tuvastab ja hindab regulaarselt kõiki tegevusega kaasnevaid rahapesu ja terrorismi rahastamise riske ning tagab nende jälgimise ja kontrolli. Juhatus peab tagama, et riskide juhtimiseks on olemas piisavad ressursid, sealhulgas pädevad töötajad ja asjakohased maandamismeetmed. Nimetatud kohustused kehtivad ka juhul, kui ettevõttes on üks juhatuse liige, kes täidab samaaegselt töötaja ülesandeid. Eelneva täitmiseks juhatus muu hulgas:

2.12.3.1. on jooksvalt kursis majandustegevusega seotud rahapesu ja terrorismi rahastamise riskidega. Juhatus tagab enda (või vähemalt vastutava juhatuse liikme) regulaarse koolitamise, et olla kursis rahapesu ja terrorismi rahastamise uute trendide, uuenenud õigusaktide, rahvusvahelise praktika, järelevalveasutuste juhendite, analüüside jmt dokumentidega;

2.12.3.2. kehtestab RahaPTS-i, sellega vahetult seotud õigusaktide ning käesoleva juhendi nõuete täitmiseks vajalikud protseduurireeglid ning tagab, et nende täitmisega otseselt seotud töötajad on vastavatest nõuetest teadlikud;

2.12.3.3. tagab sobiva organisatsioonilise ülesehituse ja ressursid. Juhatus loob organisatsioonilise ja protsessipõhise ülesehituse (sealhulgas vastava IT-võimekuse) ja kaasab vajalikud inimesed, et vastata maksimaalselt lubatavale riskiisule ning olla võimeline vastu seisma kaasnevatele riskidele/ohtudele ja neid maandama. Kui olemasolev organisatsiooniline ülesehitus ei vasta võetavatele riskidele, peab juhatus viivitamata tagama selle kohandamise. Samuti peab juhatus kehtestama meetmed, mis võimaldavad regulaarselt hinnata tegevusega kaasnevate riskide ulatust ning organisatsioonilise ülesehituse piisavust;

2.12.3.4. Hindab kolme kaitseliini põhimõttest tulenevat huvide konflikti riski ning vajadusel rakendab meetmeid selle maandamiseks ja vältimiseks, sealhulgas vajadusel ning lähtuvalt proportsionaalsuse põhimõttest loob kolme kaitseliini põhimõttest lähtuva organisatsioonilise ülesehituse;

2.12.3.5. tagab, et määratud vastutav(ad) isik(ud) rakendavad RahaPTS-is (eelkõige RahaPTS 4. ja 5. peatükis) sätestatud hoolsusmeetmeid ning juhendis toodud soovitusi. Juhatus peab veenduma, et meetmed on asjakohased, vastavad tegevusprofiilile ning on kooskõlas kliendi, tehingu iseloomu, suuruse ja ulatuse ning võimalike rahapesu ja terrorismi rahastamise riskidega. Juhatus peab korraldama sisekontrollisüsteemi tõhusa toimimise ja tagama kohustatud isiku, juhatuse ning töötajate tegevuse osas toimivad kontrollimehhanismid. Kontrollid peavad tagama vastavuse õigusaktidele, juhtimisorganite kinnitatud dokumentidele ja headele tavadele. Juhatus peab hindama regulaarselt RahaPTS-i ja käesoleva juhendi nõuete täitmiseks loodud sisekontrollisüsteemi tõhusust.

2.13. Kohustatud isiku juhatus dokumenteerib ja protokollib otsustusprotsessi ning vastuvõetud otsused rahapesu ja terrorismi rahastamise tõkestamise meetmete rakendamise kohta. Näiteks: riskihinnangu kinnitamine, otsus tõsta teatud klientide riskiastet, otsus muuta hoolsusmeetmete kohaldamist teatud klientide osas, vastutava isiku määramine/muutmine.

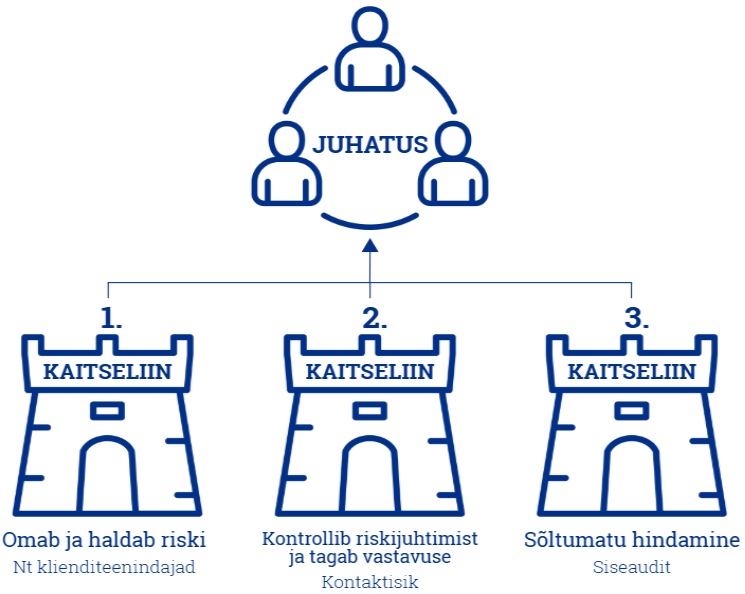
2.14. **Organisatsiooniline ülesehitus**

2.15. Tulenevalt riskipõhisest lähenemisest peab kohustatud isik hindama, milline organisatsiooniline lahend on tema tegevuse, teenuste ja riskide juures asjakohane ja proportsionaalne. Kolme kaitseliini põhimõtte rakendamine ei ole kohustuslik, kuid teatud juhtudel on riskide maandamiseks põhjendatud seda kasutada. Kolme kaitseliini põhimõte aitab eristada riskide võtmise, juhtimise ja kontrolli funktsiooni, sealhulgas maandada huvide konflikti riski. Kolme kaitseliini põhimõtte rakendamise ulatus ja vorm peavad vastama kohustatud isiku suurusele, tegevuse keerukusele ja riskiprofiilile.

Kolme kaitseliini põhimõtte rakendamine võib olla asjakohane näiteks olukordades, kus kohustatud isik:
- pakub väga mitut erinevat teenust või kõrge riskiga teenuseid;
- tegutseb kõrgema riskiga valdkonnas või puutub suurel määral kokku suurema rahapesu ja terrorismi rahastamise riskiga (nt enamus kliente on kõrge riskiga riigist);
- omab suurt kliendibaasi või tehingute mahtu.

2.16. Organisatsiooniline ülesehitus peab olema kooskõlas tuvastatud riskide olemuse, ulatuse ja mõjuga ning toetama nende tõhusat juhtimist ja kontrolli.

2.17. Kolme kaitseliini kirjeldused on leitavad juhendi punkides 2.25 - 2.46.



2.18. Riskijuhtimise mudeli väljatöötamisel tuleb arvestada funktsioonide lahususe ja huvide konflikti vältimise põhimõtetega. Huvide konflikti tuvastamiseks ja maandamiseks on soovituslik muu hulgas:

2.18.1. kehtestada huvide konflikti maandamise ja vältimise kord, milles määratakse õiguslikud, tehnilised ja organisatsioonilised meetmed. Vastav kord võib olla koostatud eraldiseisva sisemise dokumendina või olla osa muudest dokumentidest, nt protseduurireeglitest;

2.18.2. vältida olukordi, kus omanike, juhtide ning töötajate (ka käsundus või muudes õiguslikes suhetes olevate isikute) ja klientide isiklikud (sealhulgas majanduslikud) huvid on vastuolus kohustatud isiku huvidega.

2.19. Maandamismeetmete maht ja ulatus, samuti IT-süsteemide kasutamise vajalikkus ja ulatus ning täidetud töökohtade arv erinevates kaitseliinides (kui kohustatud isik on rakendanud kolme kaitseliini põhimõtet), peavad vastama kohustatud isiku suurusele ning tegevusele ja teenuste olemusele, ulatusele, keerukusastmele, sealhulgas riskiisule ja kaasnevatele riskidele.

2.20. Organisatsiooniline ülesehitus peab olema selge, õigustatud ja efektiivne ning ei tohi olla põhjendamatult või asjakohatult keeruline ega läbipaistmatu. Ebaselgus rollides, vastutusalades või dokumentatsiooni puudumine viitab ebaefektiivsusele.

Organisatsioonilist ülesehitust võib pidada ebaefektiivseks näiteks juhul, kui rahapesu ja terrorismi rahastamise tõkestamiseks vajalikud dokumendid läbivalt puuduvad või kui määratud kontaktisik ei ole pädev ega suuda oma ülesandeid nõuetekohaselt täita. Keerulisele ja läbipaistmatule ülesehitusele võib viidata ka ebaselgus isikute rollides, ülesannetes ja vastutusalades.

2.21. Kohustatud isiku organisatsiooniline ülesehitus ja iga funktsiooni ülesanded peavad olema selgelt ja arusaadavalt dokumenteeritud. Töötajad ja juhid peavad teadma enda tööülesandeid, vastutusala ja kohta organisatsioonistruktuuris.

2.22. Kolme kaitseliini põhimõtte rakendamise asjakohasust hindab kohustatud isik arvestades oma tegevuse iseloomu, mahtu ja riskiprofiili. Sõltuvalt nendest asjaoludest võib kohustatud isik kujundada riskijuhtimise ja kontrollisüsteemi ka muul viisil, kuid seda tingimusel, et riskid on piisavalt maandatud ning vastutuse jaotus on toimiv ja arusaadav. Kohustatud isik peab suutma selgitada, kuidas on muude asjakohaste meetmetega riskid ja huvide konflikt maandatud ning tagatud tõhus riskide juhtimine ja kontroll.

Kolme kaitseliini puudumine võib olla põhjendatud siis, kui teatud funktsioonide eraldi loomine ei ole proportsionaalne, arvestades teenuse ja tegevuse mahtusid (sealhulgas käive, klientide ja töötajate arv vms) ning riskid on piisavalt maandatud muude asjakohaste maandamismeetmetega (nt (pool)automatiseeritud IT-lahendused).

2.23. Kolme kaitseliini põhimõttest erineva lähenemise korral tuleb:

2.23.1. eristada funktsioone, mis on seotud hoolsusmeetmete kohaldamisega ärisuhte loomisel ning ärisuhte tavapärasel jälgimisel. Oluline on tagada, et (äri)tegevuse käigus tuvastatakse kahtlased või ebaharilikud tehingud ja tegevused, samuti tehingud või tegevused, millel puudub mõistlik majanduslik eesmärk või mis viitavad sellistele asjaoludele, ning muud ohumärgid. Nimetatud juhtumid tuleb suunata edasiseks analüüsiks isikule, kes vastutab teadete esitamise eest Rahapesu Andmebüroole. Kohustatud isik võib kontrollide tõhususe ja dokumenteerimise tagamiseks kasutada muu hulgas ka IT-lahendusi, mis võimaldavad kontrollida isikuandmeid sanktsiooninimekirjade ja riikliku taustaga isikute[10] andmebaaside suhtes ning salvestada kontrolli tulemused automaatselt. IT-lahenduste kasutamine ei vabasta kohustatud isikut kohustusest tagada funktsioonide lahusus ja maandada enesekontrolli riski.;

2.23.2. maandada enesekontrolli risk, eelkõige olukorras, kus ettevõttes on vähe töötajaid või üks töötaja täidab mitut või kõiki funktsioone. Selle riski maandamiseks võib muu hulgas kaaluda välise audiitori kaasamist või rakendada muid asjakohaseid lahendusi nagu näiteks perioodiline enesekontroll teatud klientide või tehingute valimi kohta, kontrollilistide jälgimine vms.;

2.23.3. kirjeldada ja vajadusel Rahapesu Andmebüroole tõendada, kuidas on tagatud funktsioonide lahusus ja välditud huvide konflikti, sealhulgas kuidas maandatakse enesekontrolli riski ning tagatakse toimingute dokumenteerimine ja tagantjärele kontrollimise võimalus (nt IT-lahenduste või väliste teenusepakkujate abil, kontrolli protsessi kirjeldamine ja kontrolli teostamine).

2.24. Riskijuhtimise funktsiooni edasiandmisel (*outsourcing*) kohaldatakse juhendi punktides 4.309. - 4.316. nimetatud põhimõtteid asjakohaste erisustega ja RahaPTS §-s 24 sätestatut.

2.25. **I kaitseliin**

2.26. I kaitseliin hõlmab tegevusi, mille käigus riskid[11] tekivad ning isikuid, kes riskide hindamise ja juhtimise eest vastutavad. I kaitseliini ülesannete hulka kuulub hoolsusmeetmete kohaldamine nii ärisuhte loomisel kui ka ärisuhte tavapärasel jälgimisel.

2.27. I kaitseliini ülesanne on omada head teadmist kliendist: füüsilise isiku puhul tema tegevusest ja juriidilise isiku puhul äritegevuse spetsiifikast, samuti nendega seotud riskidest. Eesmärk on tuvastada kliendi (äri)tegevuses tehingud või tegevused, mis on kahtlased või ebaharilikud, millel puudub mõistlik majanduslik eesmärk või viitab sellistele asjaoludele, ning muud ohumärgid (punased lipud[12]), et suunata need

[10] Riikliku taustaga isik on ka selle isiku pereliige või tema lähedaseks kaastöötajaks peetav isik. Käesolevas juhendis nimetatakse neid isikuid riikliku taustaga isikuteks (PEP).
[11] Riskihinnangus (juhendi punkt 3.5) tuvastatud riskid.
[12] Inglise keeles *red flags* või *alert*.

edasiseks analüüsiks II kaitseliinile. Sõltuvalt organisatsioonilisest ülesehitusest, võib selleks olla näiteks juhatus.

2.28. Juhatus hindab, millistel juhtudel ja olukordades on vajalik I kaitseliini töös riskide juhtimiseks kaasata IT-lahendusi või inimesi. Näiteks võib see hõlmata automatiseeritud lahendusi juhul, kui klientide arv muudab nende käsitsi kontrollimise ebaproportsionaalselt ressursimahukaks (meediamonitooring, sanktsioonikontroll või riikliku taustaga isikute kontroll). Ebaproportsionaalselt ressursimahukale käsitsi teostatavale kontrolliprotsessile võib viidata näiteks olukord, kus kohustatud isik ei suuda korduvalt tagada kontrollide õigeaegset läbiviimist või kui seire-, kontrolli- või audititegevuse käigus tuvastatakse puudusi kontrollide järjepidevuses, täielikkuses või kvaliteedis. IT-lahenduste kasutamisel tuleb tunda oma klienti ja tema tegevusi piisavalt, et tuvastada kahtlased või ebaharilikud tehingud ja tegevused.

2.29. **II kaitseliin, sealhulgas kontaktisiku funktsioon**

2.30. II kaitseliin hõlmab riskijuhtimise ja vastavuskontrolli funktsioone, mille eesmärk on tagada tegevuste vastavus kehtivatele õigusaktidele, juhenditele ning teistele asjakohastele dokumentidele, samuti hinnata õigusliku või regulatiivse keskkonna muudatuste võimalikku mõju kohustatud isiku tegevusele ja vastavuskontrolli raamistikule.

2.31. Riskijuhtimise ja vastavuskontrolli funktsioone võib täita sama isik või struktuuriüksus. Juhul kui II kaitseliini eest vastutav isik täidab samal ajal ka muid tööülesandeid või funktsioone, peab juhatus tuvastama võimalikud huvide konfliktid ning rakendama asjakohaseid meetmeid nende vältimiseks või maandamiseks.

2.32. II kaitseliini ülesandeks on toetada I kaitseliini, tuvastada kohad, kus riskid esinevad (näiteks kahtlaste või ebaharilike tehingute ja tegevuse analüüs), ning aidata I kaitseliinil efektiivselt neid riske juhtida. II kaitseliin ei võta riske, kuid tagab kõigi riskide tuvastamise, hindamise, mõõtmise, jälgimise ja juhtimise ning teavitab neist juhatust. Riskijuhtimise funktsiooni täitja keskendub eelkõige riskiisust kinnipidamisele, riskide muutumise tuvastamisele ja kaasnevate riskide ülevaate andmisele juhatusele.

2.33. Vastavuskontrolli osana või selle kõrval tegutseb II kaitseliinis tavapäraselt ka Rahapesu Andmebüroo kontaktisik (edaspidi kontaktisik), kelle määrab ettevõtte juhatus ja kelle vastavuse RahaPTS-i nõuetele kinnitab Rahapesu Andmebüroo. Kontaktisiku määramise kohustus, sealhulgas erisused, on sätestatud RahaPTS-i § 17. Seejuures:

2.33.1. Kontaktisiku paiknemine organisatsiooni struktuuris peab olema selline, et võimaldab täita rahapesu ja terrorismi rahastamise tõkestamise nõudeid, nagu on õigusaktides sätestatud. Samuti tuleb tagada, et kontaktisik alluks vahetult juhatusele või filiaali juhatajale ning oleks võimalikult sõltumatu ettevõtte tavapärastest äriprotsessidest;

2.33.2. Kontaktisikul peab olema vajalik pädevus, vahendid ja vahetu juurdepääs asjakohasele teabele igal ajahetkel kogu organisatsioonis. See tähendab eelkõige juurdepääsu ärisuhete loomise aluseks või eelduseks olevale informatsioonile, sealhulgas kliendi isikuandmetele ning tema majandustegevust kajastavatele andmetele, dokumentidele ja muule olulisele teabele. Samuti tagab juhatus kontaktisikule õiguse vajadusel osaleda juhatuse koosolekutel, kui kontaktisik peab seda oma ülesannete täitmisel vajalikuks.

2.34. Kontaktisiku ülesanded on järgmised:

2.34.1. korraldada tegevuses ilmnevate ebatavaliste või rahapesu kahtlusega tehingute või asjaolude või terrorismi rahastamisele viitava teabe kogumist ja analüüsimist. Selleks säilitab ta muu hulgas kirjalikku taasesitamist võimaldavas vormis kõik töötajatelt laekunud teated kahtlaste ja ebaharilike tehingute kohta, samuti nende teadete analüüsimiseks kogutud informatsiooni ja muud asjakohased dokumendid;

2.34.2. edastada teavet Rahapesu Andmebüroole rahapesu või terrorismi rahastamise kahtluse korral. See hõlmab kohustust säilitada kirjalikku taasesitamist võimaldavas vormis Rahapesu Andmebüroole edastatud teated koos teate edastamise aja ja teate edastanud töötaja andmetega;

2.34.3. teha juhatusele perioodiliselt kirjalikke ülevaateid. Ülevaadete perioodilisus sõltub kohustatud isiku suurusest ning tema tegevusega kaasnevatest riskidest. Kohustatud isik määrab perioodilisuse ise, kuid ülevaade tuleb koostada vähemalt üks kord aastas. Ülevaates tuleb käsitleda vähemalt järgmisi teemasid:

2.34.3.1. rahapesu ja terrorismi rahastamise nüüdisaegsed meetodid, konkreetsed tüpoloogiad/kaasused ja trendid ning nendega kaasnevad riskid, sealhulgas nende mõju ning vajadus maandada riske organisatsioonilise ülesehituse ja sisekontrollisüsteemi kaudu;

2.34.3.2. tegevuse, teenuse osutamisega ja/või toodete pakkumisega kaasnevad riskid, nende mahud ning võimalikud muutused (nt otsustatakse lõpetada mõne teenuse või toote pakkumine, uute teenuste või toodete turuletoomine, kliendibaasi laiendamine või teenuste/toodete pakkumine väljaspool Eestit);

2.34.3.3. hinnang riskide maandamismeetmete (sealhulgas IT-süsteemide ja inimressursi) piisavusele ja tõhususele;

2.34.3.4. riskiisust kinnipidamise hindamine ning ettepanekud rahapesu ja terrorismi rahastamise tõkestamise meetmete, riskiisu ja/või riskihinnangu muutmiseks või täiendamiseks;

2.34.3.5. rahapesu ja terrorismi rahastamise tõkestamisega seotud intsidendid, sealhulgas sisemised teated ja Rahapesu Andmebüroole edastatud teated;

2.34.3.6. muud asjaolud, mis on vajalikud rahapesu ja terrorismi rahastamise tõkestamise nõuete täitmise selgitamiseks ja hindamiseks;

2.34.3.7. teatud riskide või intsidentide esinemisel tuleb koostada ja esitada ülevaade ka erakorraliselt *ad-hoc* versioonis. Erakorralise ülevaate koostamise vajaduse ja sellega seotud asjaolud otsustab II kaitseliin.

2.35. Kontaktisik täidab ka muidu rahapesu ja terrorismi rahastamise tõkestamisega seotud ülesandeid, mis ei ole pandud vastavuskontrolli või riskijuhtimise ülesanneteks.

2.36. Protseduurid peavad sisaldama kontaktisiku asendamise korda. Ei ole lubatud olukord, kus kontaktisiku ülesanded on täitmata või nende täitmine ei ole tagatud.

2.37. Kontaktisiku määramine kooskõlastatakse Rahapesu Andmebürooga. Kui kontaktisikuks on määratud struktuuriüksus, siis täidab kontaktisiku ülesandeid, sealhulgas teadete esitamise kohustust, majandustegevuse registris märgitud ja Rahapesu Andmebüroo poolt kooskõlastatud struktuuriüksuse juht. Kui soovitakse, et struktuuriüksuses on teadete esitamise õigus ka teistel töötajatel peale struktuuriüksuse juhi, siis tuleb vastavad töötajad eelnevalt Rahapesu Andmebürooga kooskõlastada.

2.38. Uue kontaktisiku määramisest teavitatakse Rahapesu Andmebürood vähemalt 30 päeva enne kavandatava muudatuse jõustumist. Kui kontaktisiku muutmine on tingitud kohustatud isikust sõltumatutest asjaoludest, näiteks ootamatult töölt lahkumine, teavitab kohustatud isik Rahapesu Andmebürood viivitamata, kuid hiljemalt viie tööpäeva jooksul kontaktisiku muutumisest.[13]

2.39. **III kaitseliin**

2.40. III kaitseliini moodustab sõltumatu ja tõhus siseauditi või sisekontrolli funktsioon, mille eesmärk on hinnata organisatsiooni protsesside ja kontrollimehhanismide toimimist. Siseauditi funktsiooni võib näha ette organisatsiooni struktuuris või sisse osta vastava teenuse osutajalt. Kui õigusaktidest ei tulene kohustust siseauditi funktsiooni loomiseks, peab kohustatud isik tagama kontrollifunktsiooni täitmise muul proportsionaalsel ja sõltumatul viisil, arvestades kohustatud isiku suurust, tegevuse olemust, riske ja keerukust ning huvide konflikti riski (juhendi punkt 3.37.).

2.41. Organisatsioonisiseselt võib siseauditi või sisekontrolli funktsiooni täita üks või mitu töötajat ja/või selleks moodustatud struktuuriüksus. Sel juhul struktuuriüksuse juht vastutab siseauditi ülesannete nõuetekohase täitmise eest.

2.42. Siseauditi või sõltumatu sisekontrolli funktsiooni teostaja peamine ülesanne on seirata ning hinnata organisatsiooni kriitiliste protsesside ja süsteemide toimimist. Siseauditi või sisekontrolli funktsiooni täitja ei tohi hinnata (auditeerida) tegevusi või funktsioone, mille täitmises ta ise osaleb, vältimaks enesekontrolli riski ja huvide konflikti. Sama põhimõte kehtib ka sisemiste dokumentide väljatöötamise puhul – siseauditi funktsiooni täitja (siseaudiitor) ei tohi osaleda dokumentide koostamises või sisulises kujundamises, kui ta peab hiljem hindama nende dokumentide alusel toimiva sisekontrollisüsteemi tõhusust ja vastavust nõuetele.

2.43. Siseauditi või sisekontrolli teostajal peab olema piiramatu ja õigeaegne juurdepääs kogu asjakohasele teabele ning ta peab olema teadlik kohustatud isiku suurusest, tegevusest, teenustest, riskidest ja riskiisust ning omama ajakohast ülevaadet rahapesu ja terrorismi rahastamise riskidest, meetoditest ja trendidest.

[13] Majandustegevuse seadustiku üldosa seadus § 30 lõiked 1 ja 2.

2.44. Siseauditi või sisekontrolli funktsioon hindab muu hulgas, kas:

2.44.1. organisatsiooniline ülesehitus toetab rahapesu ja terrorismi rahastamise tõkestamist;
2.44.2. sisemised dokumendid ja protsessid on a(s)jakohased ning vastavuses kehtivate õigusaktide nõuetega, samuti organisatsiooni riskiisu ja strateegiatega;
2.44.3. igapäevane tegevus vastab õigusaktidest tulenevatele nõuetele, sisemistele protseduurireeglitele ning muudele sisemistele dokumentidele;
2.44.4. I ja II kaitseliini tegevus on asjakohane, kvaliteetne ja mõjus ning huvide konfliktid puuduvad või need on piisavalt tuvastatud, hinnatud ja maandatud.

2.45. Auditi või sisekontrolli teostamise regulaarsuse määramisel tuleb arvestada kohustatud isiku suurust ning tegevuse ja osutatavate teenuste olemust, ulatust ja keerukusastet, sealhulgas riskiisu ja tegevusega kaasnevaid riske.

2.46. Väiksemate või ühe töötajaga ettevõtete puhul ei pruugi eraldiseisva siseauditi funktsiooni loomine olla põhjendatud. Sellisel juhul peab kohustatud isik ise tagama ja olema võimeline tõendama, et kontrollimehhanismid on rakendatud, nõuete täitmist on hinnatud ning asjakohased toimingud ja andmed on dokumenteeritud viisil, mis võimaldab nende hilisemat kontrolli ja taasesitamist.

2.47. **Koolitus**

2.48. Kohustatud isik peab tagama rahapesu ja terrorismi rahastamise tõkestamisega seotud töötajate, kontaktisiku ja juhatuse koolituse. Töötajate all mõistetakse kõiki riskijuhtimise kaitseliinide töötajaid, sealhulgas ka käsunduslepingu alusel tööd tegevaid isikuid. Koolitus tuleb tagada ka isikutele, kellele on osa tegevusi edasi antud.

2.49. Koolitusega hõlmatud isikud peavad olema eelkõige teadlikud rahapesu ja terrorismi rahastamise tõkestamise nõuetest, sealhulgas hoolsusmeetmete rakendamisest ja teavitamise kohustusest Rahapesu Andmebüroole. Koolitusel tuleb muu hulgas edastada teavet:

2.49.1. riskiisu ja riskihinnangu dokumendis toodud põhimõtetest;
2.49.2. protseduurireeglites ettenähtud kohustustest ning nende täitmisest;
2.49.3. isikuandmete kaitse nõuetest;
2.49.4. rahapesu ja terrorismi rahastamise toimepanemise nüüdisaegsetest meetoditest ning konkreetsetest tüpoloogiatest ja kaasustest ning nendega kaasnevatest riskidest;
2.49.5. meetoditest, kuidas ära tunda võimalikke rahapesu või terrorismi rahastamisega seotud toiminguid, ning juhiseid sellistes olukordades tegutsemiseks.

2.50. Koolitus peab toimuma siis, kui töötaja alustab nimetatud tööülesannete täitmist ning edaspidi regulaarselt või vastavalt vajadusele. Koolituse käigus tuleb vajadusel kombineerida selgitavaid ja informatiivseid osi teadmiste kontrolli või hindamisega.

2.51. Koolituse regulaarsus sõltub kohustatud isiku suurusest ning tema tegevuse ja teenuste olemusest, ulatusest ja keerukusastmest, sealhulgas riskiisust ja tegevusega kaasnevatest riskidest. Koolituste korraldamine ja/või töötajate informeerimine on vajalik eelkõige: riskiisu, riskihinnangu või protseduurireeglite muutumisel, tegevusega kaasnevate riskide olulisel muutusel, uute rahapesu ja terrorismi rahastamise trendide ja

meetodite ilmnemisel, valdkonda reguleerivate õigusaktide muutumisel ning muudel sarnastel juhtudel, mis mõjutavad riskide hindamist ja töötajate kohustusi. Töötajate koolituse sisu ja sagedus peavad vastama nende rollile ja vastutusala riskidele. Kõrgema riskiga tegevustega seotud töötajad peavad saama põhjalikumaid ja regulaarsemaid koolitust.

2.52. Rahapesu Andmebüroo korraldatud infotunde ning nendel osalemist võib käsitleda koolitusena käesoleva juhendi tähenduses, eeldusel et infotunni sisu on seotud rahapesu ja terrorismi rahastamise tõkestamise nõuetega ning aitab kaasa kohustatud isiku töötajate teadlikkuse ja pädevuse tõstmisele. Kohustatud isik peab tagama, et selline osalemine on asjakohaselt dokumenteeritud ning vastab tema tegevusest tulenevatele koolitusvajadustele.

3. Riskide juhtimine

3.1. Riskide juhtimine on terviklik süsteem, mis koosneb hästi toimivast organisatsioonilisest lahendusest, riskihinnangust ja riskiisust, sisemistest protsessidest, riskipõhiste hoolsusmeetmete rakendamisest ning andmete säilitamisest. Kui selles süsteemis on mõni osa puudu või puudulik, muutub kogu kohustatud isiku tegevus haavatavaks ning riske ei ole võimalik maksimaalselt efektiivselt juhtida.

3.2. Kui kohustatud isik ei ole teadlik oma tegevuse ja klientidega seotud riskidest, ei saa ta rakendada eesmärgipäraseid ega tõhusaid hoolsusmeetmeid nende riskide maandamiseks. Samuti, kui protseduurireeglid ei ole piisavad ega kirjelda selgelt hoolsusmeetmete rakendamise korda (sealhulgas tugevdatud hoolsusmeetmeid ja nende kasutamise tingimusi), võivad kliendiga seotud riskid jääda maandamata, kuna töötajad ei tea, milliseid riske ja kuidas käsitleda.

3.3. Kui kohustatud isikul puudub sobiv organisatsiooniline lahendus või tema tegevuse mahule (sealhulgas kliendibaasi suurusele) vastavad IT-süsteemid, võivad riskid jääda maandamata ressursside puuduse tõttu. Samuti, kui andmeid ei säilitata, ei ole võimalik kliente ja tehinguid tõhusalt järelkontrollida ega riske tuvastada.

3.4. Kui riske ei tuvastata ega hinnata, ei ole võimalik täita ka teatamiskohustust. Seega moodustavad RahaPTS-is ja käesolevas juhendis sätestatud nõuded tervikliku süsteemi, mis peab vastama kohustatud isiku suurusele ja tegevusele ning olema proportsionaalne.

3.5. Riskihinnang ja riskiisu

3.6. Riskihinnangu eesmärk on tuvastada kohustatud isiku tegevusega kaasnevad riskid ning mõista, kuidas need riskid konkreetse kohustatud isiku tegevuses võivad avalduda ja see juures kohustatud isikut mõjutada. Riskide tuvastamine võimaldab kohustatud isikul rakendada riskipõhist lähenemist ning suunata ressursse eelkõige valdkondadesse, kus rahapesu ja terrorismi rahastamise risk on suurem. Riskihinnang on alus efektiivsele riskide juhtimise süsteemile.

3.7. Riskihinnang võib olla koostatud eraldiseisvalt või olla osa sisemistes dokumentides. Kui riskihinnang on osa sisemistest dokumentidest, peab see olema selgelt eristatav ja tuvastatav. Kohustatud isikud koostavad riskihinnangu võttes arvesse oma äritegevuse

laadi ja suurust, sealhulgas selle riske ja keerukust, proportsionaalselt sobivaid meetmeid, et tuvastada ja hinnata rahapesu ja terrorismi rahastamise riske, millega nad kokku puutuvad.

3.8. Riskihinnangu koostamiseks peab kohustatud isik omama terviklikku ülevaadet oma tegevusest ning analüüsima oma ettevõtte suurust ja olemust ka kvantitatiivselt. See tähendab, et kohustatud isik vajab ülevaadet pakutavatest teenusest ning nende mahtudest, millistes valdkondades võivad esineda rahapesu ja terrorismi rahastamise riskid, millistes jurisdiktsioonides tegutsetakse, kui suur on kohustatud isiku töötajaskond, millised on valdkonna tüpoloogiad[14] jne, et kaardistada peamised riskid. Kvantitatiivsete andmete osas ülevaate koostamine aitab mõista, kus on kõige suurem risk, kus on puudu töötajatest või finantsilisest vahenditest jne.

Näiteks, kui riskide kaardistamisel tuvastatakse, et kohustatud isiku kliendibaasis on oluline osakaal kõrge korruptsiooniindeksiga riikidega seotud kliente, võib see viidata, et rahapesu ja terrorismi rahastamise loomupärane risk geograafilises riskikategoorias võib olla kõrge.

Kõrge riskiga klientide puhul tuleb ärisuhte seiret teostada tavapärasest sagedamini. Kui kohustatud isik kvantitatiivsete andmete hindamisel tuvastab näiteks, et väga suure hulga kõrge riskiga klientide ärisuhte seire on koondunud ühe töötaja vastutusalasse, tuleb hinnata, kas seiret on võimalik tõhusalt teostada. Hindamisel tuleb arvestada ka olemasolevate kontrollimehhanismide ja tehniliste lahendustega. Ebapiisava kontrollikeskkonna või ressursside korral võib tegemist olla riskikohaga.

Kui tuvastatakse, et seire ei ole enam tõhus või on puudulik, peab kohustatud isik kaaluma tööülesannete ümberkorraldamist, täiendavate töötajate värbamist, tehniliste lahenduste kasutuselevõttu või vajadusel riskist osalist või täielikku loobumist.

3.9. Riskide hindamisel tuleb arvestada eraldi nii rahapesu kui ka terrorismi rahastamisega seotud riske ning neid eraldi hinnata ja analüüsida. Riskide eristamine peab olema selgelt tuvastatav ja arusaadav. See tähendab, et tuleb tuvastada ja selgelt defineerida, milliseid tooteid ja teenuseid kasutades ning mil viisil on võimalik kohustatud isikut kasutada rahapesuks ja mil viisil terrorismi rahastamiseks (st milline on risk). See hõlmab ka strateegilisi analüüse, et mõista organisatsiooni kitsaskohti (st milline on haavatavus).

3.10. Riskihinnangu sisu ning selle põhjalikkuse osas tuleb arvestada proportsionaalsuse põhimõtet. Arvestada tuleb, et riskihinnang vastaks organisatsiooni suurusele, tegevusele, osutatavate teenuste olemusele, ulatusele, keerukusastmele, tegevusega kaasnevatele riskidele ning riskiisule.

3.11. Riskide hindamisel tuleb arvestada ka Eesti riigi ning Euroopa Liidu riski- ja ohuhinnangutega. Analüüs sellest, kuidas vastavate riski- ja ohuhinnangutega on arvestatud, peab olema tuvastatav kohustatud isiku riskihinnangus. Riskihinnangu

[14] Tüpoloogiate tuvastamisel tulen lähtuda riiklikust riskihinnangust, Rahapesu Andmebüroo poolt avaldatud uuringutest ja muudest dokumentidest, FATF-i avaldatud materjalidest ning muudest usaldusväärsetest materjalidest.

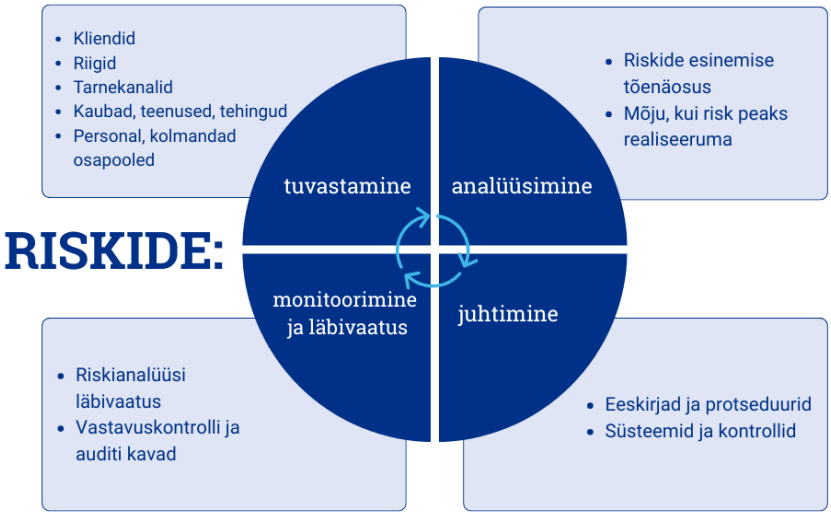
koostamisel tuleks lähtuda ka Financial Action Task Force-i[15] (edaspidi FATF) soovitustest, juhistest ja materjalidest ning The Authority for Anti-Money Laundering and Countering the Financing of Terrorism (edaspidi AMLA) soovitustest ja juhenditest. Samuti tuleb lähtuda ka Rahapesu Andmebüroo avaldatud materjalidest, sealhulgas märgukirjadest ja uuringutest, milles tuuakse välja riske sektori põhiselt või geograafiliselt.

3.12. Riskihinnangut tuleb pidevalt uuendada ja täiendada ning selles tuleks arvestada ka hoolsusmeetmete kohaldamise protsessis, sealhulgas ärisuhte seire käigus, kogutud teabega. Hoolsusmeetmete kohaldamise käigus kogutud teave muudab riskihinnangut näiteks siis, kui kohustatud isik tuvastab, et klientide tegevusmahud on suurenenud või kliendibaasis on suurenenud kõrge riskiga kolmandate riikidega seotud kliendid jne. Selliste muutuste tuvastamisel on kohustatud isikul soovitatav vastavad asjaolud ja tehtud järeldused ka dokumenteerida, et oleks võimalik hiljem hinnata riskide muutumist ajas ning mõista, milliste kaalutluste alusel on otsuseid tehtud ja meetmeid rakendatud.

3.13. Kui kohustatud isik kuulub kontserni, tuleb riskihinnangu koostamisel arvestada kontserni struktuuri, tegevuse, geograafilise ulatuse ning muude asjaoludega ulatuses, milles need mõjutavad kohustatud isiku riske ja riskide juhtimise meetmeid. Kontserni kuulumisel peab tütarettevõtja riskihinnang arvestama kontserni asjakohaste põhimõtete ja riskihinnangutega, arvestades seejuures kohaliku tegevuse eripärasid ja riske.

3.14. Riskihinnangu dokumendi kehtestab ja kinnitab juhatus enda otsusega kirjalikus vormis.

3.15. Riskid ei ole muutumatud ning nende hindamine on tsükliline protsess, mis tähendab, et regulaarselt tuleb riske hinnata, analüüsida, kontrollida ja testida.



[15] Financial Action Task Force on eesti keeles Rahapesuvastane töökond.

3.16. **Riskihinnangu dokument peab sisaldama vähemalt järgnevat:**

3.16.1. Esimeses etapis tuleb saada ülevaade ettevõttest, sealhulgas kaardistada pakutavad teenused, nende mahud, teenustega hõivatud töötajaskond jne. Eesmärgiks on hinnata, millised tooted või teenused on rahapesule ja terrorismi rahastamisele vastuvõtlikud ning millised on kohustatud isiku tegevusega kaasnevad riskid. Samuti tuleb esimeses etapis hinnata riske kategooriate kaupa (kliendiga seonduv risk; riikide või geograafiliste piirkondade või jurisdiktsioonidega seonduv risk; toodete teenuste või tehingutega kaasnev risk; kohustatud isiku ja kliendi vaheliste suhtlus- või vahenduskanalitega või toodete, teenuste või tehingute edastamiskanalitega seonduv risk) ning selgitada lühidalt riski olemust. Riskihindamisel tuleb arvesse võtta nii tegelikku riskipositsiooni kui ka võimalikku olukorda, kus riske võetakse maksimaalselt lubatud tasemel.

Selleks, et **hinnata kohustatud isiku riske efektiivselt**, peab kohustatud isik olema kursis oma valdkonna ja sektori **tüpoloogiatega**. Tüpoloogiad on kirjeldused ja mustrid sellest, kuidas rahapesu ja terrorismi rahastamise praktikas toimub.

Riskidena võiks kohustatud isik hinnata näiteks, kui suur tõenäosus on, et kohustatud isik võimaldab rahapesu ja terrorismi rahastamist:

- teenindades kliente, kellel on keeruline või läbipaistmatu omandistruktuur;
- tehes koostööd vahendajatega või agentidega;
- teenindades kliente, kelle tegelikud kasusaajad on kõrge riskiga riikidest;
- saades suuri rahasummasid kõrge riskiga riikidest;
- tundmatu kolmanda osapoole makse tõttu jne.

3.16.2. Teise etapina hinnatakse, milline on tuvastatud riskide loomuomane risk ehk kui suur on rahapesu ja terrorismi rahastamise risk, kui ettevõte ei rakendaks ühtegi maandamismeedet riskide maandamiseks. Selleks tuleb hinnata ja luua metoodika, et tuvastada kui suur on tõenäosus, et konkreetne risk kohustatud isiku tegevuses võib realiseeruda ning kui see risk realiseerub, siis kui suur on mõju kohustatutud isikule.

TÕENÄOSUS × **MÕJU** = **LOOMUPÄRANE RISK**

3.16.3. Kolmandas etapis tuleb otsustada, millised maandamismeetmed tuleb kasutusele võtta, et loomuomast riski maandada või kõrvaldada. Selles etapis võib kohustatud isik ka tulenevalt liiga kõrgest loomupärasest riskist loobuda riski võtmisest. Kohustatud isik määrab riskihinnangu alusel olukorrad ja tingimused, millal majandustegevuses kohaldada tugevdatud või lihtsustatud hoolsusmeetmeid ning milline on tema tugevdatud või lihtsustatud hoolsusmeetmete sisu ja olemus.

Maandamismeetmeks võivad olla näiteks tugevdatud hoolsusmeetmete rakendamine, tihedam ärisuhte seire, täiendavate töötajate lisamine riskantsematesse protsessidesse, piirmäärade kehtestamine, sisekontrolli rakendamine, töötajatele koolituste korraldamine, automaatne sanktsiooninimekirjade kontroll, automaatsete süsteemide loomine, sisemiste dokumentide uuendamine jne.

3.16.4. Neljanda etapina, pärast riskide maandamiseks sobivate meetmete määramist, hinnatakse kehtestatud metoodika alusel iga tuvastatud riski jääkriski. Jääkrisk on risk, mis jääb alles pärast riskide maandamiseks rakendatud meetmete kasutamist. Kohustatud isik hindab jääkriski tulemuse pinnalt, kas jääkriski:

3.16.4.1. suurus jääb tema kindlaks määratud riskiisu piiridesse;

3.16.4.2. osas rakendatakse täiendavaid maandamismeetmeid;

3.16.4.3. suurusest tulenevalt otsustatakse riski mitte võtta.

3.16.5. Riskiisu on raamistik, mis määrab kindlaks riski tüübi ja taseme, mida kohustatud isik on valmis aktsepteerima. Riskiisu peaks näiteks täpsustama puudused ja rikkumised, millega kohustatud isik ei soovi olla seotud. Kui jääkrisk jääb välja kohustatud isiku riskiisust, tuleb kaaluda selliste teenuste osutamata jätmist või teatud tüüpi klientide teenindamata jätmist.

3.17. Riskiisu võib olla eraldi dokument või osa riskihinnangust. Riskiisu võib olla koostatud hinnates riske, riskiastmeid ja riskikategooriaid, mida kohustatud isik on valmis oma tegevuses võtma. Samuti võib riskiisu määratleda ka välistamismeetodil, st dokumendis tuuakse välja kõik need riskid, mida soovitakse vältida. Välistava meetodi rakendamisel tuleb riskiisu kirjeldada ja mõelda selliselt läbi, et see oleks üheselt arusaadav ning käsitleda tuleks riske lähtuvalt kõigist RahaPTS-i § 13 nimetatud riskikategooriatest. Näiteks, kui riskiisus on sätestatud, et ei teenindata riikliku taustaga isikuid ega virtuaalvääringu teenuse pakkujaid, aga samas geograafilise riskikategooria osas ei ole kehtestatud selgeid riskipiire, võib tekkida olukord, kus dokumentatsioonist ei selgu üheselt, milliste jurisdiktsioonidega seotud kliente on lubatud teenindada. Sellisel juhul võib jääda ebaselgeks ka see, kas näiteks kõrge riskiga jurisdiktsioonidest pärit või seal tegutsevate klientide teenindamine on lubatud või mitte, kuigi selline kliendiprofiil viitab selgelt kõrgendatud riskile. Seetõttu on oluline, et riskiisu oleks kehtestatud kõigis riskikategooriates ning et riskiisu oleks läbimõeldud, põhineks asjakohasel analüüsil, lähtuks kohustatud isiku tegevusalast ja pakutavatest teenustest ning oleks kirjeldatud selgelt ja üheselt mõistetavalt. Riskihinnangu, riskiisu ja riskipõhise lähenemise kujundamisel tuleb arvestada, et kõrge riskiga kliente või teenuseid ei pea automaatselt välistama. Riskipõhine lähenemine tähendab, et kõrgema

riskiga klientide, toodete või teenuste puhul rakendatakse vastavalt riskiastmele täiendavaid riskide maandamise ja juhtimise meetmeid.

Kliendi riskiprofiili määramise mudel (täpsemalt punktides 4.24. – 4.39.) ja kliendi riskiastme hindamine ei ole sama, mis kohustatud isiku ülene riskihinnang.

Kohustatud isiku üleses riskihinnangus hinnatakse kogu ettevõtte tegevusega kaasnevaid riske. Kliendi riski hindamisel hinnatakse konkreetse kliendi või tehinguga seotud riski.

Kliendi riskiprofiili ja riskiastme määramise mudel tugineb ettevõtte riskihinnangule ning arvestab selles tuvastatud riskitegureid.

Kliendi riskiprofiili mudeli ja ettevõtte riskihinnangu jaoks tuleb koostada eraldi mudelid või dokumendid.

3.18. **Riskide hindamise kategooriad:**

3.19. **Klientidega, sealhulgas tegeliku kasusaajaga seonduv risk**. Selles riskikategoorias hinnatakse kliendi isiksusest, taustast, tegevusalast ja käitumisest tulenevaid riske.

3.20. **Riikide või geograafiliste piirkondade või jurisdiktsioonidega seonduv risk.** Selles riskikategoorias hinnatakse kui suur on tõenäosus, et kohustatud isik tegevus on seotud kõrgema rahapesu riskiga riikide või piirkondadega. Siinjuures on oluline silmas pidada, et hinnata ei tule vaid suure riskiga kolmandaid riike vaid ka neid riike:

3.20.1. kus usaldusväärsete allikate kohaselt ei ole kehtestatud rahapesu ja terrorismi rahastamise tõkestamise tõhusaid süsteeme;

3.20.2. kus korruptsiooni või muu kuritegeliku tegevuse tase on märkimisväärne;

3.20.3. mille suhtes on kehtestatud sanktsioonid, embargo või sarnased meetmed Euroopa Liidu või ÜRO poolt;

3.20.4. riike või jurisdiktsioone, mis rahastavad või toetavad terrorismi või mille territooriumil tegutsevad Euroopa Liidu või ÜRO poolt määratud terroristlikud organisatsioonid;

3.20.5. samuti tuleks tähelepanu pöörata Rahapesu Andmebüroo väljastatud uuringutele ning tagasisidele, kus tuuakse välja erinevate riikide ja jurisdiktsioonidega seotud riske.

3.21. **Toodete, teenuste või tehingutega seonduv risk.** Hinnata tuleb kas ja kuidas pakutavad teenused, tooted või tehingud võivad võimaldada rahapesu ja terrorismi

rahastamist. Kui kohustatud isik pakub erinevaid tooteid ja teenuseid, siis tuleb hinnata kõikide toodete ja teenuste riske eraldi. Toodete, teenuste või tehingutega seonduvate riskide hindamisel on väga oluline hinnata erinevaid tüpoloogiaid ning olla kursis, millised on võimalused, et kohustatud isiku teenuseid, tooteid või tehinguid kasutatakse rahapesuks või terrorismi rahastamiseks. Tulenevalt tüpoloogiatest saab kohustatud isik hinnata, millised on need indikaatorid, mis seonduvad kohustatud isiku pakutavate toodete, teenuste või tehingutega. Mõned sektorispetsiifilised näited:

3.21.1. Kui kohustatud isik tegutseb valdkonnas, millele on FATF omistanud nn väravahoidja rolli[16] (kinnisvaramaakler, jurist, raamatupidaja või äriühingute ja usaldusfondide teenuse pakkuja), siis peavad kohustatud isikud riskihinnangu koostamisel sellega arvestama. See tähendab, et toodete ja teenustega seotud riskide hindamisel tuleb arvestada, et risk ei pruugi avalduda tehingu väärtuses, vaid mõjus, mida teenuse võimaldamine võib avaldada (sealhulgas on oluline pöörata tähelepanu ka tegeliku kasusaaja tuvastamisele, ärisuhte eesmärgi tuvastamisele, kliendi taustale, kas esitatud informatsioon vastab tema taustale ning kas teenuse saamise eesmärk on selge). Näiteks võib aadressi teenuse osakaal olla usaldushalduse ja äriühingute teenuse pakkujate teenustest summaliselt väiksem osa, kuid aadressiteenuse võimaldamine mõnes jurisdiktsioonis võib olla eelduseks tegevusloa saamiseks ning siis on kliendil võimalik hakata toime panema kuritegelikke tegevusi tegevusloaga valdkonnas, mis võib olla riikliku riskihinnangu kohaselt kõrge riskiga valdkond. Väravahoidjate puhul ei näita tehingu väärtus alati rahapesu ja terrorismi rahastamise riski, määrav on teenuse võimalik mõju ja kasutusviis. Audiitori ja raamatupidamise teenuse puhul ei pruugi risk avalduda üksikus tehingus ega selle rahalises mahus, vaid pigem olukordades, kus kliendi esitatud dokumendid, rahavood ja selgitused ei ole omavahel kooskõlas või ei vasta kliendi tegelikule majanduslikule profiilile. Raamatupidaja, kes kajastab tehinguid kliendi esitatud andmete põhjal, ning audiitor, kes hindab aruandlust sageli tagantjärele, võivad avastada riski eelkõige läbi selliste vastuolude, mitte läbi konkreetse tehingu väärtuse või suuruse.

3.21.2. Fondivalitseja puhul tuleks riske hinnata ka fondipõhiselt või investeerimisobjekti vaates. Tuleb mõista millisesse fondi investeeritakse ja millised on investeerimisobjektide jurisdiktsioonid ning nendega kaasnevad riskid. Näiteks võib riskiks olla see, kui klient soovib läbi fondivalitseja investeerida enda ettevõttesse, sest fondistruktuuri võidakse kasutada vahendite päritolu või tegeliku eesmärgi varjamiseks ning näilise õiguspärasuse loomiseks. Seetõttu on oluline tuvastada olukord, kus fondivalitsejat võidakse ära kasutada ning hinnata seda kas toote ja teenuse riski kategoorias või kliendi riskikategoorias.

3.21.3. Krediidiandjate puhul ei saa samuti riskihinnangus lähtuda alati ainult suurtest summades. Väikelaenu või järelmaksu summa võib olla individuaalselt väike, kuid mitme paralleelse või järjestikuse laenulepingu kaudu võidakse integreerida ebaseadusliku päritoluga raha finantssüsteemi, nt laenu ennetähtaegne tagastamine

[16] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/HRGTC.pdf.coredownload.inline.pdf, lk 4.

teadmata päritoluga vahenditest. Oluline on jällegi hinnata neid riske riskihinnangus.

3.22. **Kohustatud isiku ja klientide vaheliste suhtlus- või vahenduskanalitega või toodete, teenuste või tehingute edastamiskanalitega seonduv risk**. Riskidena tuleb hinnata, kuidas klient teenuseid tarbib ning kuidas tehinguid teostatakse ja kuidas on neid viise võimalik kasutada rahapesu ja terrorismi rahastamiseks. Kui suhtlus- või vahenduskanalina või tehingute/teenuste edastamiskanalitena kasutatakse uudseid lahendusi, siis tuleb ka nende kasutamise riske hinnata. Kui kohustatud isik kasutab agenti või vahendajat, siis tuleks hinnata ka neid riske.

3.23. Riskikategooriatega seotud märksõnad on toodud juhendi lisas 1.

3.24. **Riskihinnangu ja riskiisu uuendamine**

3.25. Riskihinnang ja riskiisu on dokumendid, mida on vaja pidevalt uuendada. Uuendamise regulaarsus sõltub kohustatud isiku suurusest, tema tegevusest ja teenuste olemusest, ulatusest, keerukusest ning tegevusega kaasnevatest riskidest.

3.26. Riskihinnangu ja riskiisu uuendamine ja ülevaatamine peab olema dokumenteeritud ning võimaldama hiljem tuvastada, millal on neid uuendatud või üle vaadatud, millised on sisse viidud muudatused jne.

3.27. Regulaarne riskihinnangu ja riskiisu uuendamine võimaldab tuvastada uusi riske, sealhulgas hinnata maandamismeetmete piisavust. Riskide ajakohastamine on oluline, et riskihinnang ja riskiisu vastaks muutuvale keskkonnale ning aitab tagada vastavuse seadusandlusega.

3.28. Sisemistes dokumentides on soovituslik kindlaks määrata konkreetne aeg, millal riskihinnang ja riskiisu üle vaadatakse. Dokumente on mõistlik vaadata üle ja uuendada vähemalt kord aastas. Kui ilmneb vajadus riskihinnangu ja/või riskiisu uuendada varem, vaadatakse see üle enne ettenähtud tähtaega. Riskihinnang ja riskiisu tuleks üle vaadata **vähemalt** siis, kui otsustatakse:

3.28.1. muuta oma teenuseid ja tooteid;

3.28.2. kasutada uusi või uuendatud müügikanaleid;

3.28.3. pakkuda tooteid või teenuseid uutele turgudele või uutes geograafilistes asukohtades;

3.28.4. muudetakse riskiisu rohkemate riskide võtmiseks:

3.28.5. uuendatakse riikliku riskihinnangut.

3.29. **Protseduurireeglid ja sisekontrollieeskiri**

3.30. Protseduurireeglid ja sisekontrollieeskiri peavad sisaldama selgeid käitumisjuhiseid, millest ettevõtte töötajad saavad lähtuda rahapesu ja terrorismi rahastamise riskide maandamisel. Protseduurireeglid ja sisekontrollieeskiri võivad sisalduda ühes või mitmes dokumendis, kuid need peab kinnitama kirjalikus vormis kohustatud isiku

kõrgem juhtkond[17]. Protseduurireeglid tehakse töötajatele alaliselt kättesaadavaks ja neid tutvustatakse töötajatele ning seda peab suutma pädevale järelevalveasutusele tõendada.

3.31. Protseduurireeglid ja sisekontrollieeskirja esitavad kohustatud isikud tegevusloa taotluse osana. Edaspidi tuleb nimetatud dokumente hoida ajakohasena ja vajadusel uuendada.

3.32. **Protseduurireeglid**

3.33. Juhatus kehtestab protseduurireeglid, millega maandatakse ja juhitakse tõhusalt rahapesu ja terrorismi rahastamisega seotud riske, mis on riskihinnangus tuvastatud.

3.34. Protseduurireeglites sisalduvad tegevuspõhimõtted ja käitumisjuhised peavad olema töötajatele arusaadavad ja lihtsasti jälgitavad. Protseduurireeglid peavad vastama kohustatud isiku suurusele ning tegevuse ja teenuste olemusele, ulatusele, keerukusastmele, sealhulgas riskiisule ja tegevusega kaasnevatele riskidele. Protseduurireeglid peavad kajastama kohustatud isiku tegelikku praktikat ning kirjeldama reaalselt rakendatavaid protsesse ja toiminguid.

3.35. Protseduurireeglid sisaldavad vähemalt:

3.35.1. **Kliendi suhtes rakendatavate hoolsusmeetmete loetelu ja nende rakendamise korda**, sealhulgas ka millal kasutatakse lihtsustatud ja millal tugevdatud hoolsusmeetmeid. Kirjeldada tuleb ka seda, millised on kohustatud isiku jaoks lihtsustatud ja tugevdatud hoolsusmeetmed. Kui kohustatud isik on rakendanud kolme kaitseliini põhimõtet, tuleks kirjeldada ka milliseid tegevusi teevad erinevad kaitseliinid hoolsusmeetmete rakendamisel.

3.35.2. **Mudelit kliendi ja tema tegevusega seotud riskide tuvastamiseks ja juhtimiseks ning kliendi riskiprofiili määramiseks**. Kliendi riskiprofiili mudel on süsteem või metoodika, mille abil hindab kohustatud isik kliendiga seotud rahapesu ja terrorismi rahastamise riski ning määrab tuvastatud riskide alusel kliendile riskiastme. Kliendi riskiprofiil aitab kohustatud isikul otsustada milliseid täiendavaid hoolsusmeetmeid, sealhulgas tugevdatud hoolsusmeetmeid kliendi osas tuleb rakendada, kui tihti tuleb ärisuhtes kliendi osas teostada ärisuhte seiret jne. Kliendi riskiprofiili mudel ei ole sama, mis ettevõtte ülene riskihinnang. Kliendi riskiprofiili määramisel tuleb arvestada kõiki kohustatud isiku tegevusvaldkonnale omaseid riske ning kasutada asjakohaseid ja kättesaadavaid andmeid, sealhulgas tehingutega seotud infot, rahavoogude iseloomu ning vajadusel ka kolmandate isikute osalust tehingutes (nt maksed kolmandatelt isikutelt). Riskiprofiili koostamisel on soovituslik lähtuda rahvusvahelistest juhistest, sealhulgas FATF-i soovitustest, ning arvestada sektori spetsiifiliste rahapesu ja terrorismi rahastamise tüpoloogiatega.

3.35.3. **Metoodikat ja juhendit, kui isikul tekib rahapesu ja terrorismi rahastamise kahtlus või on tegemist ebatavalise tehingu või asjaoluga**. Juhend peab kirjeldama

[17] Kõrgem juhtkond juhendi mõttes on isik, kellel on piisavalt kõrge amet, otsustusõigus ning põhjalikud teadmised organisatsioonist ja selle võimekusest, et teha teadlikke otsuseid äriühingu riskiprofiili otseselt mõjutatavates küsimustes ning tal on teadmised, et maandamismeetmed on sellise riski võtmiseks piisavad.

kohustatud isiku ettevõttesisest protsessi kahtluse tuvastamisest kuni otsuse tegemiseni, sealhulgas kahtluse edastamise ja läbivaatamise korda ning vastutust otsuste tegemisel. Ka juhul, kui kohustatud isik on ühemehefirma, tuleb selgelt reglementeerida tegevused ja otsustusprotsess alates kahtluse tuvastamisest kuni asjakohase otsuse tegemiseni, sealhulgas vajadusel teate esitamiseni pädevale asutusele. Juhend peab selgitama:

3.35.3.1. kuidas toimub kahtluse analüüs ja täiendavate andmete kogumine kahtluse kinnitamiseks või ümberlükkamiseks;

3.35.3.2. juhiseid, kuidas toimub kommunikatsioon kohustatud isiku sees, kui tuvastatakse kahtlane, ebaharilik või sularaha piirmäära ületav tehing. Juhendis peab olema selgelt määratletud info liikumise ahel ja erinevate etappide ja otsustusprotsesside vastutajad. Juhendis tuleb kirjeldada ka info liikumise ajakava ja otsustuspunktid, mis tagavad RahaPTS-ist tuleva teatamiskohustuse täitmise Rahapesu Andmebüroole viivitamata, kuid hiljemalt kahe tööpäeva jooksul alates asjaolude või kahtluse tuvastamisest.

3.35.4. **Andmete säilitamise ja nende kättesaadavaks tegemise korda.** Andmete säilitamise korra eesmärk on tagada, et kliendi ja tehingute andmed säilitatakse süstemaatiliselt, turvaliselt. Andmete säilitamise korrast peab selguma, milliseid andmeid säilitatakse, kui kaua neid andmeid säilitatakse, kus ja kuidas andmeid säilitatakse ja kuidas toimub andmete kättesaadavaks tegemine pädevatele ametiasutustele. Andmed peavad olema säilitatud viisil, mis võimaldab nende kiiret otsingut ja tuvastamist, sealhulgas kronoloogilises ja/või muul süstematiseeritud kujul (nt kliendi, tehingu või sündmuse põhiselt).

3.35.5. **Juhendit, kuidas tulemuslikult kindlaks teha, kas tegemist on riikliku taustaga isikuga või sanktsioneeritud isikuga või isikuga, kelle elu- või asukoht on suure riskiga kolmandas riigis või riigis, mis suurendab geograafilist riski** (RahaPTS § 37 lg 4). Juhendis peab olema selge juhis kohustatud isiku töötajale, kuidas kontrollida kliendi tasuta, et tuvasta kõrgema riskiga kliendid. Oluline on jälgida, et jurisdiktsioonide hindamisel arvestatakse nii elu-, asu-, kui ka tegevuskoha riikidega, residentsust ning päritolu ehk sünniriiki või kodakondsust.

3.35.6. **Korda, kuidas tuvastada ja juhtida riske, mis on seotud uute või olemasolevate tehnoloogiate, teenuste ja toodetega, sealhulgas uute või ebatavaliste müügikanalitega ning arenevate tehnoloogiatega.** Kui kohustatud isik kasutab või plaanib kasutusele võtta tehnoloogilisi lahendusi, siis tuleb hinnata ka nende tehnoloogiate rahapesu ja terrorismi rahastamise riskid ja dokumenteerida riskihinnangu tulemused. Riskihindamisel tuleb muu hulgas hinnata mõju kliendi tuvastamise ja kontrollimise protsessidele, tehingute jälgitavusele, võimalikele anonüümsuse riskidele ning kolmandate osapoolte või tehnoloogiliste platvormide kasutamisega seotud riskidele. Erilist tähelepanu tuleb pöörata kaugtuvastamisele, automatiseeritud otsustusprotsessidele, digitaalsetele platvormidele ning muudele uutele või ebatavalistele kliendisuhtluse ja müügikanalite vormidele. Riskide maandamiseks tuleb vajadusel rakendada täiendavaid kontrollimeetmeid, sealhulgas

tugevdatud hoolsusmeetmeid, tehingute täiendavat järelkontrolli, käsitsi kontrolli ning tehnoloogiliste lahenduste kasutuspiiranguid.

3.35.7. **Koolituste korraldamise korda**. Koolituste korraldamise kord peab sisaldama rahapesu ja terrorismi rahastamise tõkestamisega seotud töötajate, kontaktisiku ja juhatuse ning isikute, kellele on rahapesu ja terrorismi rahastamise tõkestamisega seotud tegevus edasi antud koolitamise sagedust, tingimusi ja plaani.

3.35.8. **Ärisuhte loomisest või juhtuti tehtavast tehingust keeldumise korda, tehingu tegemisest keeldumise õiguse rakendamise korda ning ärisuhte erakorralise ülesütlemise korda**. Kui kohustatud isikus on struktuurist ja koosseisust tulenevalt mitu isikut, kes vastutavad rahapesu ja terrorismi rahastamise tõkestamisega seotud ülesannete täitmise eest, siis tuleb protseduurireeglites ka kirjeldada, kes vastavad otsused ellu viib. Kui kohustatud isikul on teenuse osutamiseks erinevad IT lahendused või süsteemid, siis tuleb kehtestada ka kord, kelle ülesandeks ja millise aja jooksul sulgetakse kliendi ligipääsud süsteemidesse, kes teavitab klienti jne. Oluline on läbi mõelda kogu tegevuste protsess ning see kirjalikult fikseerida.

3.35.9. **Tegevuste edasiandmise kord ja teise isiku kogutud andmetele tuginemise korda**. Protsessijuhis peab kirjeldama, milliseid tegevusi võib edasi anda, kellele neid tegevusi edasi võib anda, kuidas kontrollitakse, et teenusepakkuja täidab temale pandud ülesandeid korrektselt, kuidas andmed teenusepakkujale edastatakse ja säilitatakse. Näiteks, kui kohustatud isik kasutab enda tegevuses tehnilisi lahendusi isikusamasuse tuvastamiseks, siis tuleb see protsess ka kaardistada.

3.35.10. **Protseduurireeglite uuendamise korda.** Kohustatud isik peab kirjeldama kuidas ja kui tihti vaadatakse üle ning uuendatakse protseduurireegleid. Eesmärk on tagada, et reeglid oleksid ajakohased, vastaksid seadustele ja kohustatud isiku tegelikule tegevusele. Samuti tuleb määratleda, kes vastutab uuendamise eest ning kuidas muudatused dokumenteeritakse ja kinnitatakse, sealhulgas ka seda, kuidas fikseeritakse, kui protseduurireeglid on üle vaadatud, kuid muudatusi ei tehta.

3.35.11. **Finantseerimisasutuste korral selget kirjeldust turvalistest meetoditest, mida kasutatakse isikusamasuse tuvastamiseks infotehnoloogiliste vahendite abil (ehk nn video teel tuvastamine** (juhendi punktides 4.196. – 4.203.).

3.36. Protseduurireeglite koostamisel tuleb lähtuda kohustatud isiku suurusest ning tegevuse ja teenuste olemusest, ulatusest, keerukusastmest, sealhulgas riskiisust ja tegevusega kaasnevatest riskidest.

3.37. **Sisekontrollieeskiri**

3.38. Protseduurireeglite täitmise kontrollimiseks kehtestatakse sisekontrollieeskiri. Sisekontrollieeskirjas peab olema selgitatud sisekontrollisüsteemi toimimine, sealhulgas vastavuskontrolli rakendamine ja töötajate kontrollimine, kasutatavate andmebaaside ja IT-süsteemide toimimine jmt. Kui kohustatud isikul on näiteks ainult üks töötaja, kes on ka juhatuse liige, siis viiakse sisekontroll läbi perioodilise enesekontrollina ning vastav protsess tuleb ka protseduurireeglites kirjeldada. See

tähendab, et toiminguid teostanud isik viib oma tegevuste üle läbi kontrolli mingi ajaperioodi vältel ning hindab, kas kõik vajalikud protsessid on läbitud, dokumendid kogutud, kas kliendi riskiprofiil on õigesti määratud jne.

3.39. Juhatus korraldab protseduurireeglite ja sisekontrollieeskirja täitmise ning rakendamise töötajate poolt.

3.40. Juhatus vastutab protseduurireeglite ja sisekontrollieeskirja ajakohasuse ning kooskõla eest riskiisu ja riskihinnanguga. Juhatus tagab, et reeglid vaadatakse regulaarselt üle ning vajaduse korral neid ka ajakohastatakse või kehtestatakse uued.

3.41. Keerukamate struktuuridega kohustatud isikute juhatus nimetab protseduurireeglites erinevate töölõikude täitva(te) isiku(te) või struktuuriüksus(t)e nimed ning eraldi nende ajakohastamise, muutmise või koostamisega seotud isiku(d) või struktuuriüksuse.

4. Hoolsusmeetmed

4.1. Kohustatud isiku üks peamisi kohustusi rahapesu ja terrorismi rahastamise tõkestamisel on hoolsusmeetmete kohaldamine. Hoolsusmeetmete kohaldamise eesmärk on eelkõige takistada kuritegelikul teel saadud vara varjamist, muundamist ja kasutamist rahapesu erinevates faasides ning tõkestada terrorismi rahastamist illegaalsetest kui ka legaalsetest allikatest pärit rahaliste vahendite abil. Hoolsusmeetmete peamiseks eesmärgiks on tagada Eesti ettevõtluskeskkonna usaldusväärsus ja läbipaistvus ning tõkestada Eesti rahandussüsteemi ja majandusruumi kasutamist rahapesuks ja terrorismi rahastamiseks.

4.2. Hoolsusmeetmeid tuleb kohaldada vähemalt RahaPTS-is sätestatud minimaalses ulatuses, lähtudes riskipõhisest lähenemisest ning rakendades kõrgema riski korral tugevdatud hoolsusmeetmeid. Kohustatud isik on hoolsusmeetmeid kohaldanud piisavalt, kui nende rakendamise tulemusel tekib veendumus, et hoolsusmeetmete kohaldamise kohustus on täidetud. Veendumuse kujundamisel lähtutakse mõistlikkuse põhimõttest. See tähendab, et hoolsusmeetmete kohaldamisel peab kohustatud isikul tekkima teadmine, arusaam ja veendumus, et andmeid on kogutud piisavalt kliendi, kliendi (äri)tegevuse, ärisuhte eesmärgi ning ärisuhte raames tehtavate tehingute eesmärgi ja rahaliste vahendite päritolu kohta. Kogutud andmete põhjal peab kohustatud isik mõistma klienti ja tema (äri)tegevust, arvestades seejuures kliendi riskiastet ning ärisuhtega kaasnevat riski ja olemust (ehk ärisuhte profiili). Selline veendumus peab võimaldama tuvastada keerukaid, suure väärtusega ja ebatavalisi tehinguid ning tehingumustreid, millel puudub mõistlik või nähtav majanduslik või õiguspärane eesmärk või mis ei ole konkreetsele ärispetsiifikale iseloomulik. Veendumuse kujunemine peab olema dokumenteeritud viisil, mis võimaldab seda vajadusel esitada järelevalveasutustele. Samuti peab kohustatud isik suutma selgitada kohaldatud hoolsusmeetmete ulatust ning veendumuse kujunemist.

4.3. Hoolsusmeetmete kohaldamine jaguneb hoolsusmeetmeteks ärisuhte loomisel ja ärisuhte pideval jälgimisel (ehk seirel). Seadus sätestab hoolsusmeetmete

miinimumnõuded, mida kohustatud isik võib vajadusel täiendada vastavalt kliendi, tehingu ja riskide eripärale. Hoolsusmeetmete kohaldamine peab olema riskipõhine.

4.4. **Hoolsusmeetmeid tuleb kohaldada** (erandid alates juhendi punktist 4.13. kuni 4.14.):

4.4.1. ärisuhte loomisel (ärisuhte selgitus punktis 4.11.);

4.4.2. ärisuhte pideva seire käigus;

4.4.3. ärisuhte väliselt tehingu juhuti tegemisel (juhuti tehingu selgitus punktis 4.12.) või vahendamisel, kui tehingu väärtus on vähemalt 15 000 eurot[18] või sellega võrdväärne summa muus vääringus, sõltumata sellest, kas rahaline kohustus täidetakse tehingus ühe maksena või mitme seotud maksena kuni üheaastase perioodi jooksul, kui seadus ei sätesta teisiti. Hoolsusmeetmeid tuleb kohaldada kohe, kui nimetatud summa saabumine on teada, või kui summa kujuneb mitmest seotud maksest, siis hetkest, mil see piirmäär ületatakse;

4.4.4. varem kogutud dokumentide või andmete piisavuse või õigsuse kahtluse korral nende kontrollimisel või ajakohastamisel;

4.4.5. rahapesu või terrorismi rahastamise kahtluse korral, sõltumata seaduses sätestatud eranditest või piirmääradest.

4.5. Kohustatud isikul on keelatud luua ärisuhet või võimaldada tehingu tegemist, kui isik ei esita piisavat informatsiooni enda isikusamasuse tuvastamiseks või tehingu eesmärgi ja olemuse kohta või kui tema (äri)tegevusega kaasneb rahapesu või terrorismi rahastamise kahtlus. Ärisuhte kestel on kohustatud isikul kohustus keelduda tehingute tegemisest, kui hoolsusmeetmete kohaldamiseks vajalik teave puudub, on ebapiisav või on tekkinud rahapesu või terrorismi rahastamise kahtlus.

4.6. Kohustatud isik on kohustatud ütlema kestvuslepingu üles etteteatamistähtaega järgimata, kui isik ei esita hoolsusmeetmete kohaldamiseks piisavat teavet.

4.7. Hoolsusmeetme kohaldamisel tuleb arvestada rahapesu ja terrorismi rahastamise riske ning meetodeid.

4.8. Hoolsusmeetmete kohaldamine on kohustatud isiku kohustus. Hoolsusmeetmed on keelatud kohaldamata jätta ka juhul, kui sama isiku või tema tehingute suhtes on või oleks pidanud hoolsusmeetmeid kohaldama teine kohustatud isik.

4.9. Hoolsusmeetmete ning rahapesu ja terrorismi rahastamise tõkestamise meetmete kohaldamisel kogutud informatsioon ja andmed tuleb säilitada (juhendi punkt 6).

4.10. Juhatus vastutab hoolsuskohustuse täitmise eest, tagades, et rakendatavad meetmed on asjakohased, proportsionaalsed ning kooskõlas teenusepakkuja tegevusprofiili, klientide, tehingute iseloomu ja ulatuse ning nendega kaasnevate rahapesu ja terrorismi rahastamise riskidega.

[18] Kui teenuse osutaja on käibemaksukohustuslane, arvestatakse tehingu summa koos käibemaksuga. Kui teenuse osutaja ei ole käibemaksukohustuslane, arvestatakse tehingu summat ilma käibemaksuta

4.11. Ärisuhe on kliendi ja kohustatud isiku vaheline kutsealane või äriline suhe, mille loomise hetkel on põhjendatult eeldatav selle kestvus või korduvus. Ärisuhe ei pea alati põhinema kirjalikult lepingul. Ärisuhe võib tuleneda ka teenuse tegelikust kasutamisest, kliendi registreerimisest, kasutajakonto avamisest või püsiva teenuse osutamisest. Ärisuhtele võivad viidata järgmised tunnused (loetelu on näitlik):

4.11.1. kliendile luuakse konto või püsiv ligipääs teenusele;

4.11.2. teenuseid kasutatakse korduvalt või regulaarselt;

4.11.3. kliendiga toimub püsiv suhtlus või andmete ajakohastamine;

4.11.4. tehingud toimuvad pikema ajaperioodi jooksul;

4.11.5. teenuse olemus eeldab jätkuvat kliendisuhet või järelevalvet.

4.12. Juhuti tehtav tehing on tehing või teenus, mida tehakse väljaspool ärisuhet ning millel puudub põhjendatud eeldus pikemaks kestvuseks või korduvuseks. Juhuti tehing on üldjuhul ühekordne ja piiratud konkreetse toiminguga. Kui kliendi tegevuses ilmneb ajas korduvus, regulaarne teenuse kasutamine või muu püsivuse element, siis tuleb hinnata, kas juhuti tehtav tehing on sisuliselt kujunenud ärisuhteks. Juhuti tehingu võiva viidata järgmised tunnused (loetelu on näitlik):

4.12.1. tegemist on üksiku või erandliku tehinguga;

4.12.2. kliendile ei looda püsivat kontot ega ligipääsu;

4.12.3. puudub jätkuv teenuse osutamine või suhtlus;

4.12.4. pooled ei eelda koostöö jätkamist pärast tehingu lõpuleviimist.

4.13. **Hoolsusmeetmete kohaldamise erisused**

4.14. Erisustes viidatud asjaomastel juhtudel lähtuda piirmäärade arvestamisel tehingu kogusummast. Kui teenuse osutaja on käibemaksukohustuslane, arvestatakse tehingu summa koos käibemaksuga. Kui teenuse osutaja ei ole käibemaksukohustuslane, arvestatakse tehingu summat ilma käibemaksuta.

4.15. Erisuste puhul arvestatakse ühekuulist perioodi kliendi viimase tehingu kuupäevast tagasiulatuvalt ühe kuu ulatuses ning üheaastast perioodi kliendi viimase tehingu kuupäevast tagasiulatuvalt ühe aasta ulatuses.

4.16. **Finantseerimisasutuste hoolsusmeetmete erisused**

4.16.1. Finantseerimisasutus kohaldab hoolsusmeetmeid ärisuhte väliselt tehingute juhuti tegemisel või vahendamisel, kui tegemist on rahaülekandega ning tehingu väärtus on vähemalt 1 000 eurot või sellega võrdväärne summa muus vääringus, sõltumata sellest, kas rahaline kohustus täidetakse tehingus ühe maksena või mitme seotud maksena kuni ühe kuu jooksul, kui seaduses ei ole sätestatud teisiti. Seejuures tuleb hoolsusmeetmeid kohaldada kohe, kui finantseerimisasutusele saab teatavaks, et tehingu väärtus ulatub nimetatud summani. Kui summa kujuneb mitme seotud makse teostamisest, kohaldatakse hoolsusmeetmeid hetkest, kui piirmäär 1 000 eurot ületatakse.

4.16.2. Valuutavahetusteenust võib osutada tehingus osaleva isiku isikusamasust tuvastamata juhul, kui sularahas vahetatava summa väärtus ühekordses tehingus või seotud tehingutena ei ületa 1 000 eurot.

4.16.3. Finantseerimisasutus ei tohi osutada teenuseid, mida on võimalik kasutada ilma tehingus osaleva isiku isikusamasust tuvastamata ja esitatud teavet kontrollimata.

4.16.4. Kohustatud isik peab fondiosakute tehingute puhul, arvestades kliendi riskiprofiili ja temaga seotud riske ning kohustatud isiku riskihinnangut, asjakohasel juhul tuvastama fondi osaku ostukorralduse andnud isiku ja osaku eest tasunud isiku vahelise seose, sellise seose põhjendatuse ja arusaadavuse ning fondi osaku müügikorralduse andnud isiku ja osaku müügist laekuvate rahaliste vahendite saaja vahelise seose ja sellise seose põhjendatuse ning arusaadavuse. Eesmärgiks on tuvastada keerukaid, suure väärtusega ja ebatavalisi tehinguid ning tehingumustreid, millel ei ole mõistlikku või nähtavat majanduslikku või õiguspärast eesmärki või mis ei ole konkreetsele ärispetsiifikale iseloomulik.

4.17. **Usaldushalduse ja äriühingute teenuse pakkujate hoolsusmeetmete erisused**

4.17.1. Usaldushalduse ja äriühingute teenuse pakkuja kohaldab hoolsusmeetmeid lisaks üldpõhimõtetele iga kord, kui ta osutab äriühingu või muu juriidilise isiku asutamisega seotud teenuseid, sealhulgas osaluse võõrandamisega seotud toimingute tegemisel sõltumata tehingu summast või teenuse maksumusest.

4.18. **Mittetulundusühingu ja sihtasutuse hoolsusmeetmete erisused**

4.18.1. Mittetulundusühingud ja sihtasutused kohaldavad lisaks juhendi punktis 1.2.2.11. toodud põhimõttele järgmisi hoolsusmeetmeid alati siis, kui tekib kahtlus isikusamasuse tuvastamise, esitatud teabe kontrollimise või andmete ajakohastamise käigus varem kogutud dokumentide või andmete piisavuses või õigsuses, samuti rahapesu või terrorismi rahastamise kahtluse korral:

4.18.1.1. kliendi või juhuti tehtavas tehingus osaleva isiku isikusamasuse tuvastamine ning esitatud teabe kontrollimine usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal, sealhulgas e-identimise ja e-tehingute usaldusteenuste vahendite abil;

4.18.1.2. kliendi või juhuti tehtavas tehingus osaleva isiku esindaja isikusamasuse ja esindusõiguse tuvastamine ning kontrollimine;

4.18.1.3. tegeliku kasusaaja tuvastamine ja tema isikusamasuse kontrollimiseks meetmete rakendamine sellises ulatuses, mis võimaldab kohustatud isikul veenduda, kes on tegelik kasusaaja, ning mõista kliendi või juhuti tehtavas tehingus osaleva isiku omandi- ja kontrollistruktuuri;

4.18.1.4. ärisuhtest, juhuti tehtavast tehingust või toimingu eesmärgist ja olemusest arusaamine ning asjakohasel juhul selle jaoks täiendava teabe kogumine;

4.18.1.5. teabe hankimine tuvastamaks, kas isik on riikliku taustaga isik, tema pereliige või tema lähedaseks kaastöötajaks peetav isik.

4.19. **Õigusteenuse osutajale kohaldatavate hoolsusmeetmete erisused (muu hulgas, kohtutäitur, pankrotihaldur, (vande)audiitor, raamatupidamisteenuse pakkuja)**

4.19.1. Kohtutäitur, pankrotihaldur, audiitor ja muu õigusteenuse osutaja võivad kliendi, juhuti tehingus osaleva isiku ja tegeliku kasusaaja isikusamasuse tuvastada ja esitatud teavet kontrollida ärisuhte loomise või tehingu tegemise ajal, kui see on vajalik kutsetegevuse tavapärase käigu mittekatkestamiseks ning kui rahapesu või terrorismi rahastamise risk on väike. Sellisel juhul tuleb hoolsusmeetmete kohaldamine lõpule viia mõistliku aja jooksul pärast esmakontakti ja enne siduvate toimingute tegemist.

4.19.2. Audiitor tuvastab majandusaasta aruande auditi või ülevaatuse tegemisel tegeliku kasusaaja ning rakendab meetmeid tema isikusamasuse kontrollimiseks ulatuses, mis võimaldab tal veenduda, kes on tegelik kasusaaja, ning mõista kliendi või juhuti tehtavas tehingus osaleva isiku omandi- ja kontrollistruktuuri auditi või ülevaatuse ajal. Sealjuures vaatab läbi kliendi juhatuse[19] poolt tegeliku kasusaaja tuvastamiseks kogutud teabe. Ka vandeaudiitorile rakenduvad eelnevad RahaPTS-i kohustused teenuste osutamisel, eelkõige audiitorteenuse osutamisel.

4.19.3. Raamatupidamisteenuse pakkujale kohalduvad RahaPTS-i kohustused raamatupidamisteenuse osutamisel. Kohustused rakenduvad ka juhul, kui osutatakse piiratud ulatusega teenust, näiteks üksnes palgaarvestuse teenust või koostatakse kliendile majandusaasta aruanne ühekordse teenusena.

4.20. **Kauplejate hoolsusmeetmete erisused**

4.20.1. Kaupleja kohaldab hoolsusmeetmeid vähemalt iga kord, kui talle tasutakse või ta tasub sularahas vähemalt 10 000 eurot või sellega võrdväärse summa muus vääringus, sõltumata sellest, kas rahaline kohustus täidetakse ühe maksena või mitme seotud maksena kuni ühe aasta jooksul.

4.21. **Kinnisasja kasutustehingute vahendaja hoolsusmeetmete erisused**

4.21.1. Isik, kes vahendab kinnisasja kasutustehinguid, kohaldab hoolsusmeetmeid vähemalt iga kord, kui tehinguga kokku lepitud kinnisasja kasutustasu (näiteks üür) väärtus on vähemalt 10 000 eurot kuus.

4.22. **Kunstiteostega kauplejate hoolsusmeetmete erisused**

4.22.1. Kunstiteostega kaupleja ja isik, kes vahendab kunstiteoseid või ladustab neid tolli vabatsoonis, kohaldab hoolsusmeetmeid vähemalt iga kord, kui kunstiteosega seotud makse on vähemalt 10 000 eurot ühe maksena või mitme seotud maksena ühe aasta jooksul.

4.23. **Hasartmängukorraldaja hoolsusmeetmete erisused**

4.23.1. Hasartmängukorraldaja kohaldab hoolsusmeetmeid vähemalt võidu väljamaksmisel, panuse tegemisel või mõlemal juhul, kui kliendi makstav või

[19] Eraõigusliku juriidilise isiku osanikud, aktsionärid või liikmed peavad tegeliku kasusaaja andmete tuvastamise võimaldamiseks andma juriidilise isiku juhatusele kogu neile teadaoleva teabe tegeliku kasusaaja kohta, sealhulgas teabe tema omandiõiguse või kontrolli tegemise viiside kohta.

saadav summa on vähemalt 2 000 eurot või sellega võrdväärne summa muus vääringus, sõltumata sellest, kas rahaline kohustus täidetakse ühe maksena või mitme seotud maksena kuni ühekuuse perioodi jooksul. 2 000 euro piirmäära tuleb arvestada summeeritult ning selle hulka arvestatakse ka klientide sissemaksed. RahaPTS ei anna kohustatud isikule kaalutlusõigust otsustada, kas piirmäära arvestamisel lähtuda üksnes sissemaksetest, väljamaksetest või panustest. Kohustatud isikud peavad olema võimelised tuvastama piirmäära täitumist kliendi lõikes ning omama ülevaadet teenuste kasutamisest külastuskorra või mängusessiooni tasandil, et oleks võimalik pidada kuupõhist arvestust.

4.24. **Riskipõhine lähenemine hoolsusmeetmete kohaldamisel ja kliendi riskiprofiil**

4.25. Riskipõhine lähenemine hoolsusmeetmete kohaldamisel tähendab, et kohustatud isik ei rakenda kõigi klientide suhtes samu hoolsusmeetmeid, vaid hoolsusmeetmeid rakendatakse vastavalt kliendi riskiastmele, st riskipõhiselt.

4.26. Riskipõhiseks hoolsusmeetmete kohaldamiseks peab kohustatud isik hindama kliendi ja ärisuhte/teostatava tehingu riske ning määrama kliendile riskiastme. Kliendi riskide hindamiseks ja riskiastme määramiseks luuakse kliendi riskiprofiili määramise mudel.

4.27. Kohustatud isik peab nii enda kui ka oma klientide (äri)tegevuses ära tundma, mõistma ning hindama rahapesu ja terrorismi rahastamisega seotud riske (st riske, mis avalduvad enne maandamismeetmete kohaldamist). Selliselt hinnatakse riskipõhisel lähenemisel, milline on tõenäosus riskide realiseerimiseks ning milline on nende realiseerumise tagajärg. Tõenäosuse hindamisel tuleb arvestada vastavate asjaolude esinemise võimalikkusega, sealhulgas peab arvestama võimalikke ohtusid, mis võivad mõjutada nii kliendi kui ka kohustatud isiku tegevust, ja võimalust, et antud ohu esinemise tõenäosus suureneb.

4.28. Kliendiga ning eraldi ärisuhtega või juhuti tehtavas tehingus osaleva isikuga seotud konkreetsete riskide hindamisel määratakse iga kliendi või tehingus osaleva isiku riskiprofiil. Nende asjaolude põhjal määratakse kliendi või tehingus osaleva isiku riskiaste, mida väljendatakse tavapäraselt skaalal: madal (keskmisest madalam), keskmine ja kõrge (keskmisest kõrgem). Riskiastme määramine on vajalik, et kohustatud isik saaks rakendada hoolsusmeetmeid riskipõhiselt.

4.29. Riskiastmete kujunemise põhimõtted peavad olema arusaadavad kohustatud isiku töötajale ja pädevale asutusele (võimalik tuvastada, kui suure kaaluga on mingi riski tunnus).

4.30. Riskiastme määramine tähendab, et kohustatud isik hindab iga kliendi või ärisuhte riskiprofiili. Selle põhjal otsustatakse, kui palju tuleb konkreetsele kliendile või tehingule ressurssi suunata. Kõrgema riskiastme määramine ei tähenda, et klient või tehing oleks seotud rahapesu ja terrorismi rahastamisega, vaid asjaolusid kogumis arvestades tuleb kliendi (äri)tegevusele ja temaga seotud asjaoludele rohkem tähelepanu pöörata. Sama kehtib ka madala riskiastme määramisega. Madal riskiaste tähendab, et ebatavaliste või riskantsete tegevuste tõenäosus on väike ning selliste

klientide puhul saab rakendada näiteks lihtsustatud hoolsusmeetmeid või teostada ärisuhte seiret harvemini.

4.31. Oluline on, et kliendi või tehinguga seotud riskid oleksid pidevalt hinnatud. See tagab, et riskid oleks maandatud, sest kliendi riskiaste võib muutuda tulenevalt tema tegevusest, struktuurimuutustest, tegevuse ümberkorraldamisest jne. Kui kliendi riskiaste muutub, siis tuleb see alati ka dokumenteerida ning fikseerida riskiastme muutmise tinginud asjaolud. Riskiastme manuaalne vähendamine tavapärasemast kõrgemast keskmiseks on võimalik, kuid seda tehakse üksnes põhjendatud asjaolude esinemisel, võttes arvesse muu hulgas asjaolu, miks kliendile või tegevusele ei ole vaja pöörata täiendavat tähelepanu. Riskiastme sellisel muutmisel tuleb olla vajadusel valmis selgitama (sealhulgas Rahapesu Andmebüroole), miks eelnevalt tuvastatud riskid ei ole enam olulised või asjakohased ning miks on riskiastme allapoole toomine põhjendatud. Asjaolu, et klient ei ole teatud perioodil tavapärasemast kõrgemale riskile viitavaid tehinguid teinud või ei ole teinud tehinguid, mida kõrgema riskiastme määramisel arvati võimalikuks pidavat, ei tähenda, et klient neid tehinguid või toiminguid tulevikus ei tee või et kõrgemale riskiastmele viitavad tunnused ja asjaolud oleksid ületatud/kadunud jne.

4.32. **Riskiprofiili ja riskiastme määramisel võetakse arvesse vähemalt:**

4.32.1. ettevõtteülest riskihinnangut (juhendi punktid 3.5. – 3.23.). Oluline on arvesse võtta ettevõtteülest riskihinnangut, sest iga kohustatud isiku riskid on tema tegevusest, teenustest, protsessidest jne tulenevalt erinevad. Seega võib sama klient olla ühe kohustatud isiku jaoks madala riskiga, kuid teise jaoks kõrgema riskiga;

4.32.2. ärisuhte või juhuti tehtava tehingu eesmärki ning teavet, mis on kogutud ärisuhte eesmärgi või juhuti tehtud tehtava tehingu kohta, sealhulgas tuleb hinnata kõiki andmeid, mida kogutakse;

4.32.3. kliendi hoiustatava vara mahtu või juhuti tehtava tehingu varalist mahtu, kui vastavalt tegevusalast ja osutatavatest teenustest on asjakohane. Eeskätt on see nõue mõeldud näiteks finantseerimisasutustele, kinnisvaramaakleritele ning audiitoritele, kes tegelevad kliendi varaga seotud tehingutega.;

4.32.4. eeldatavat ärisuhte kestvust;

4.32.5. väiksemat ja suuremat riski iseloomustavad asjaolud tulenevalt RahaPTS § 34 ja 35 ning § 37, 39, 40, 41 sätestatust;

4.32.6. Euroopa Liidu organisatsioonide, Euroopa Nõukogu rahapesu ja terrorismi rahastamise tõkestamise meetmeid hindava ekspertkomitee Moneyval, FATF-i ja Euroopa järelevalveasutuste vastavasisulisi juhiseid ja suuniseid.

4.33. Riskiastme määramisel hinnatakse kliendi ja ärisuhte/tehingu riske ning erinevaid riskitegureid ja nende mõju kliendi riskiastmele.

4.34. Riski hindamisel tuleb arvestada, et rahapesu ja terrorismi rahastamise risk ei pruugi avalduda ühe selgelt eristatava tehingu või üksiku kõrge riskiga tehingu tunnusena. Kliendi riskiprofiil ja kõrgem riskiaste võib kujuneda ka mitme nõrga või kaudse

riskiteguri koosmõjus ning tuua kaasa olukorra, mis vajab näiteks tugevdatud hoolsusmeetmete kohaldamist või teate esitamist Rahapesu Andebüroole jne.

4.35. Riskiastme määramisel arvestatakse, et:

4.35.1. riskiastme määramist või selle kaalumist ei tohi mõjutada ainult üks riskifaktor, va juhul, kui riskifaktor iseseisvalt ei eelda kõrge riskiastme määramist (näiteks riikliku taustaga isik);

4.35.2. riskifaktori kaalu ei tohi mõjutada kohustatud isiku majanduslikud ega kasumiga seotud kaalutlused;

4.35.3. riskiastme määramise metoodika ei tohi põhjendamatult kaasa tuua olukorda, kus ühtki ärisuhet ei ole võimalik liigutada kõrgema riskiga ärisuhteks;

4.35.4. riskiastme metoodika ei tohi põhjendamatult kaasa tuua olukorda, kus kõik kliendisuhteid on madala riskiastmega, sest riskide hindamine peab võimaldama tegelike riskide sisulist eristamist ning kõrgema riskiga klientide ja tegevuste tuvastamist.;

4.35.5. kliendi riskifaktorite kaalumine ei tohi minna vastuollu Euroopa Parlamendi ja nõukogu asjakohaste direktiivide, RahaPTS-i või juhendiga, milles käsitletakse olukordi, mis kujutavad endast alati suuremat rahapesu või terrorismi rahastamise riski/ohtu.

Kui kliendi riskiastme määramist mõjutab vaid üks riskifaktor (va erandid) või kõik kohustatud isiku kliendid on kõrge või madala riskiastmega, siis ei ole tegemist riskipõhise lähenemisega ja efektiivse riskide juhtimisega ning kohustatud isik ei mõista kõiki oma tegevuse ja kliendiga kaasnevaid riske.

Samuti ei ole riskide juhtimine efektiivne ja tõhus, kui hoolimata määratud riskiastmest rakendatakse kõikidele klientidele alati ühesuguseid hoolsusmeetmeid. Madalama riskiastmega klientidele vähemate hoolsusmeetmete rakendamine on ka kliendisõbralikum ning klienti ja kohustatud isikut vähem koormav.

Mida suurem on kliendi või tehinguga seotud risk ning mida keerulisem on ettevõtte enda tegevus, seda põhjalikum ja tihedam peab olema kliendi ja ärisuhte seire.

4.36. Kõrgemale riskile viitavad ning tugevdatud või muid asjakohaseid hoolsusmeetmeid tuleb alati kohaldada muu hulgas, kui:

4.36.1. klient või tegelik kasusaaja on riikliku taustaga isik. Kõrge riskiga riikliku taustaga isik tähendab, et riikliku taustaga isiku osas esineb lisaks veel mõni kõrgemale riskile viitav asjaolu;

4.36.2. esitatud teabe või isikusamasuse tuvastamisel on tekkinud kahtlus andmete tõele vastavuses või dokumentide ehtsuses või tegeliku kasusaaja tuvastamises;

4.36.3. teenuseid osutatakse füüsilistele või juriidilistele isikutele, kes on pärit riigist, mis on kantud FATF-i kõrge riskiga või koostööd mittetegevate riikide nimekirja, või

kes on seotud suure riskiga kolmanda riigi või muu kõrgema riskiga riigi või territooriumiga, sealhulgas riigiga, kus korruptsioonitase on kõrgem või mis on kantud maksualast koostööd mittetegevate jurisdiktsioonide Euroopa Liidu loetellu. Samuti loetakse riskiteguriks olukord, kus isikul on nimetatud riigi kodakondsus, tema elu- või asukoht paikneb sellises riigis või territooriumil või makse saaja makseteenuse pakkuja asub nimetatud riigis või territooriumil.

4.36.3.1. „Pärit olema“ mõiste sisustamisel tuleb lähtuda sellest, et kliendi seose hindamisel vastava riigiga tuleb arvesse võtta ka kliendi kodakondsust ja/või kliendi sünniriiki. Seega kliendi puhul, kelle kodakondsus või sünniriik on kõrge riskiga riikide nimekirja kantud riigis, tuleks seaduse kohaselt rakendada tugevdatud hoolsusmeetmeid. Tugevdatud hoolsusmeetmete rakendamisel tuleb lähtuda kliendi riskiprofiilist tervikuna, ärisuhte ja tehingute iseloomust ning juba kogutud ajakohastest ja usaldusväärsetest andmetest. Seega ei tähenda kõrge riskiga riigi või territooriumiga seotud asjaolude esinemine automaatselt seda, et kõiki tugevdatud hoolsusmeetmeid tuleb igas ärisuhtes rakendada ühekorraga täies ulatuses ja igal puutepunktil korduvalt. Kohustatud isikul on võimalik rakendada meetmeid riskipõhiselt ja proportsionaalselt, arvestades ka olemasolevaid kontrollimeetmeid ja muid riski maandavaid asjaolusid.

4.36.4. virtuaalvääringu ülekandmise tehingud on suunatud isehallatavale aadressile või pärinevad isehallatavalt aadressilt;

4.37. Tugevdatud hoolsusmeetmete kohaldamisel tuleb arvesse võtta ka järgmistes punktides viidatud suuremale rahapesu ja terrorismi rahastamise riskile viitavaid asjaolusid. Kohustatud isik peab järgmiste punktide juures riskipõhiselt hindama ja protseduurireeglites kirjeldama, kas mõni järgmistest asjaoludest on piisav tugevdatud hoolsusmeetmete rakendamiseks eraldiseisvalt või on vajalik mitme asjaolu koos esinemine või kasutatakse järgnevaid asjaolusid täiendavate riskifaktoritena. Kohustatud isik peab suutma selgitada, miks järgmistes punktides viidatud asjaolud toovad kaasa või ei too kaasa tugevdatud hoolsusmeetmete kohaldamise. Suuremale riskile viitavate asjaolude hindamisel arvestatakse:

4.37.1. tehingud on seotud keerukate, suure väärtusega või ebatavaliste tehingutega ja tehingumustritega, millel ei ole mõistlikku või nähtavat majanduslikku või õiguspärast eesmärki või mis ei ole konkreetsele ärispetsiifikale iseloomulik;

4.37.2. esineb samaaegselt mitu riiklikus riskihinnangus või Rahapesu Andmebüroo juhendis kirjeldatud kahtlase tehingu tunnust[20];

4.37.3. klienti või tema esindajat ei tuvastata näost-näkku ning ei kohaldata erisusi isikusamasuse kaugtuvastamisel. Samas kohas viibimine tähendab, et klient või tema esindaja ja kohustatud isiku esindaja viibivad eesmärgipärasel kohtumisel

[20] „Juhend kahtlaste tehingute tunnuste kohta“ https://fiu.ee/sites/default/files/documents/2024-07/Juhend%20kahtlaste%20tehingute%20tunnuste%20kohta_22.07.2024.pdf

samas kohas. See tähendab, et potentsiaalsel kliendil või tema esindajal on kohustatud isiku esindajaga vahetu kontakt. Vahetu kontakti käigus saadud info põhjal on võimalik täpsemalt määrata kliendi riskiastet.;

4.37.4. kohustatud isiku riskihinnangu kohaselt võib teatud majandus- või kutsetegevuse, tegevusvaldkonna või muude asjaolude esinemisel olla tegemist olukorraga, millega kaasneb tavapärasest suurem rahapesu või terrorismi rahastamise risk;

4.37.5. kliendiks on juriidiline isik või muu juriidilise isiku staatust mitteomav isikute ühendus, mis tegeleb personaalse varahaldusega;

4.37.6. kliendiks on suuri sularahakoguseid käitlev ettevõtja;

4.37.7. kliendiks oleval või temaga seotud äriühingul on variaktsionärid või esitajaaktsiad;

4.37.8. kliendiks oleva äriühingu omandistruktuur näib äriühingu tegevust silmas pidades ebatavaline või liiga keeruline;

4.37.9. kliendiks on kolmanda riigi kodanik, kes taotleb Eestis elamisõigust või kodakondsust kapitalisiirete, vara või riigivõlakirjade ostmise või Eestis tegutsevatesse äriühingutesse investeerimise eest;

4.37.10. pakutakse tooteid või teenuseid või vahendatakse selliseid tooteid või teenuseid, mis võivad soodustada anonüümsust;

4.37.11. maksed laekuvad tundmatutelt või mitteseotud kolmandatelt isikutelt, sealhulgas virtuaalvääringutes;

4.37.12. uute toodete ja uute äritavadega, sealhulgas uue edastamismehhanismi või uue või areneva tehnoloogia kasutamine nii uute kui ka olemasolevate toodete puhul;

4.37.13. tehingud on seotud nafta, relvade, väärismetalli, väärismetalltoodete või tubakatoodetega;

4.37.14. tegemist on tehingutega, mille esemeks on kultuuriväärtused või muud arheoloogilise, ajaloolise, kultuurilise või usulise tähtsusega või haruldase teadusliku väärtusega esemed, elevandiluu või kaitstud liigid.

4.38. Kohustatud isik võib kliendi riskiprofiili mudeli koostamisel kasutada ettevõtte ülese riskihinnangu kategooriaid, et tagada ühtne riskide juhtimise süsteem nii kohustatud isiku üleselt kui kliendi põhiselt. Riskiprofiili koostamisel tuleb siiski lähtuda kohustatud isiku konkreetsest äritegevusest ning sellega seotud riskidest ning vajadusel hinnata ja arvesse võtta täiendavaid riskitegureid, mida ettevõtteülene riskihinnang ei pruugi täielikult katta.

4.39. Näide kliendi riskiprofiili lihtsustatud mudelist on lisas 2.

4.40. **Hoolsusmeetmed ärisuhte loomisel või juhuti tehtava tehingu puhul**

4.41. Kliendi või juhuti tehtavas tehingus osaleva isiku isikusamasuse tuvastamine ning esitatud teabe kontrollimine usaldusväärsest ja sõltumatust allikast saadud teabe põhjal, sealhulgas e-identimise ja e-tehingute usaldusteenuste vahendite abil (juhendi punktid 4.76. – 4.86. ja 4.98. – 4.111.2.).

4.42. Kliendi või juhuti tehtavas tehingus osaleva isiku esindaja isikusamasuse ning esindusõiguse tuvastamine ja kontrollimine (juhendi punktid 4.53. – 4.72.).

4.43. Tegeliku kasusaaja tuvastamine ja meetmete rakendamine tema isikusamasuse kontrollimiseks ulatuses, mis võimaldab veenduda, kes on tegelik kasusaaja, ning saada aru kliendi või juhuti tehtavas tehingus osaleva isiku omandi- ja kontrollistruktuurist (juhendi punkt 4.113.).

4.44. Teabe hankimine asjaolu kohta, kas isik on riikliku taustaga isik, tema pereliige või tema lähedaseks kaastöötajaks peetav isik (juhendi punktid 4.135. – 4.136.).

4.45. Rikkuse päritolu tuvastamine, kui see on asjakohane (juhendi punkt 4.155.).

4.46. Ärisuhtest, juhuti tehtavast tehingust või toimingust arusaamine ehk olemuse mõistmine ja asjakohasel juhul selle kohta täiendava teabe kogumine (juhendi punkt 4.170.).

4.47. Ärisuhte või juhuti tehtava tehingu eesmärgi mõistmine, muu hulgas tuleb tuvastada kliendi või juhuti tehingus osaleva isiku püsiva asu-, tegevus- või elukoha, kutse- või tegevusala, olulisemad tehingupartnerid ja maksetavad. Samuti tuleb välja selgitada, kas isik tegutseb kellegi teise eest või nimel ja juriidilise isiku puhul ka kogemus.

4.48. Ärisuhte väliselt juhuti tehtava tehingu puhul kogub kohustatud isik tehingu või toimingust arusaamise asemel teavet tehingus kasutatud vara päritolu kohta.

4.49. Hoolsusmeetmete kohaldamise eesmärk on tunne-oma-klienti põhimõtte täitmine. Tunne-oma-klienti põhimõtte täitmise eesmärgiks on saada aru, mis teenust ning millisel põhjusel klient saada soovib ehk kas kliendi soov läheb kokku tema tegeliku tegevuse, võime ja vajadustega ning arusaamaga kliendi (äri)tegevuse spetsiifikast, olemusest jne. Kliendi tundmise ulatus peab vastama ettevõtteülese riskihinnangu tulemustele ning kliendiga seotud riskile ehk mida suurem on kliendiga kaasnev risk, seda rohkem peab hoolsusmeetmeid rakendama, et kliendist ja tema (äri)tegevusest aru saada.

4.50. Kohustatud isik peab määrama eelnevalt loetletud hoolsusmeetmete kohaldamise ulatuse ja täpse viisi ning tehingus kasutatud vara päritolu ja rikkuse päritolu andmete kogumise vajaduse. Seejuures tuleb lähtuda konkreetse ärisuhtega või juhuti tehtava tehingu, toimingu või isikuga seonduvatest rahapesu ja terrorismi rahastamise riskidest (riskipõhine lähenemine). Hoolsusmeetmete rakendamist hinnatakse mõistlikkuse põhimõtte järgi, nagu see on sätestatud võlaõigusseaduses. Kohustatud isik peab tegutsema viisil, nagu käituks samas olukorras keskmiselt hoolas ja professionaalne isik ehk hoolsusmeetmeid rakendatakse proportsionaalselt riskile ja olukorrale. Hoolsusmeetmete kohaldamisel tuleb lisaks arvestada ka asjakohaste sektori- ja valdkonnapõhiste riskidega, mis tulenevad riiklikust riskihinnangust ning FATF-i juhistest. See tähendab, et riskipõhine lähenemine ei põhine ainult kliendi individuaalsetel tunnustel, vaid ka teenuse, tegevusvaldkonna ja ärimudeli olemuslikel riskidel. Näiteks võib, aga ei pruugi, kõrgem risk esineda olukorras, kus klient on Eesti füüsiline isik ning tema tehingud on mahult väiksed, kuid ta kasutab teenuseid või

tegutseb sektoris, mis on riiklikus riskihinnangus kõrgema riskiga. Sellises olukorras tuleb kaaluda täiendavate hoolsusmeetmete kohaldamist vastavalt tuvastatud riskiastmele ja kliendi riskiprofiilile. Hoolsusmeetmeid ei kohaldata kõikide klientide suhtes ühetaoliselt, vaid lähtudes kliendi riskiprofiilist, kliendisuhte olemusest ja konkreetsete tehingute riskitasemest. Näiteks:

4.50.1. Kui klient on Eesti füüsiline isik ning tema tehingute maht, sagedus ja iseloom on kooskõlas kliendi profiili ja kliendisuhte eesmärgiga ning asjaolud ei viita kõrgendatud riskile, piisab enamasti isikusamasuse tuvastamisest ja põhiteabe kogumisest kliendi tegevuse kohta.

4.50.2. Kui klient soovib teha suure väärtusega tehingu või raha liikumine ei vasta kliendi tavapärasele majandustegevusele, tuleb koguda lisateavet tehingu eesmärgi ja vara päritolu kohta.

4.50.3. Kui juriidilise isiku omandistruktuur on keerukas või hõlmab välisriigi ettevõtteid, tuleb rakendada täiendavaid hoolsusmeetmeid tegeliku kasusaaja tuvastamiseks.

4.50.4. Kui klient on riikliku taustaga isik, ning esinevad kõrgemale riskile viitavad tunnused, siis tuleb rakendada tugevdatud hoolsusmeetmeid, näiteks tuvastada tehingus kasutatavate vahendite allikas ja päritolu.

4.50.5. Kui tehingu eesmärk ei ole selge või see ei ole kooskõlas kliendi tavapärase tegevusega, tuleb küsida kliendilt täiendavaid selgitusi.

4.51. Hoolsusmeetmete kohaldamisel kogutud andmed fikseeritakse tavapäraselt muu hulgas kliendi kohta koostatud ning kliendi poolt kinnitatud kliendiankeedis. Kliendiankeet peab sisaldama kliendi kinnitust selle kohta, et klient on teadlik ja saanud aru nende tingimustega seatud kohustustest, sealhulgas kohustusest esitada ärisuhte loomiseks vajalik teave nõutud vormis ning esitatud valeandmetega kaasnevast vastutusest. Valeandmete esitamise või olulise teabe varjamise korral võib kohustatud isik ärisuhte loomisest keelduda, selle lõpetada ning kliendil võib tekkida lepinguline või tsiviilõiguslik vastutus.

4.52. Kokkuvõtvalt on kohustatud isiku eesmärk mõista ja tuvastada kliendi ja tema ärisuhtega kaasnevat riskiprofiili. Kogutud teabe põhjal saab hinnata kliendi edaspidist eeldatavat tegevust ning teostada ärisuhte seiret. Kliendi riskiprofiili alusel määratakse tema suhtes rakendatava hoolsusmeetmena ärisuhte edasine seirerežiim. Samuti peab kohustatud isik veenduma, et kliendi (äri)tegevus ja asjaolud ei viita rahapesule, sellega seotud kuritegude toimepanemisele ega terrorismi rahastamisele.

4.53. **Füüsilise isiku ja esindaja isikusamasuse tuvastamine ning andmete kontrollimine**

4.54. **Füüsilise isiku ja esindaja isikusamasuse tuvastamine**

4.55. Ärisuhte loomisel või juhuti tehtava tehingu tegemisel peab füüsilisest isikust kliendi või juhuti tehtavas tehingus osaleva füüsilise isiku isikusamasuse ning esitatud teavet kontrollima (verifitseerima) usaldusväärsest ja sõltumatust allikast hangitud teabe

põhjal. Füüsilise isiku ja esindaja tuvastamise protsess peab olema kirjeldatud protseduurireeglites.

4.56. **Füüsilisest isikust kliendi ja vajadusel tema esindaja kohta kogutakse ja säilitatakse järgmised andmed:**

4.56.1. nimi;

4.56.2. isikukood, selle puudumisel sünniaeg ning elu- ja asukoht;

4.56.3. teave esindusõiguse kohta (esindusõiguse ulatus, faktid esindusõiguse kontrollimise kohta. Kui esindusõigus ei tulene seadusest, siis esindusõiguse alusel oleva dokumendi nimetus, väljaandmise kuupäev ja väljaandja nimi või nimetus);

4.56.4. sidevahendite andmed (telefoninumber ja/või elektroonposti aadress).

4.57. **Füüsilise isiku isikusamaust tuvastatakse järgmiste dokumentide alusel:**

4.57.1. isikut tõendav dokument;

4.57.2. välisriigis välja antud kehtiv reisidokument;

4.57.3. juhiluba, mis on kehtiv dokumenti on kantud kasutaja nimi, foto või näokujutis, allkiri või allkirjakujutis ja sünniaeg või isikukood;

4.57.4. alla 7-aastase isiku puhul perekonnaseisutoimingute seaduse §-s 30 nimetatud sünnitõend.

4.58. Kohustatud isik peab olema veendunud, et isikusamasuse tuvastamiseks esitatud dokument on sobiv ja vastab seaduses sätestatud loetelule.

4.59. Kui isikut tõendavat dokumenti ei ole võimalik näha, siis võib kasutada isikusamasuse kontrollimiseks notariaalselt tõestatud või notariaalselt või ametlikult kinnitatud isikusamasuse tuvastamise aluseks olevat dokumenti või muud Usaldusväärne ja sõltumatu allikas füüsilise isiku isikusamasuse tuvastamiseks esitatud andmete kontrollimiselpärit teavet, sealhulgas e-identimise ja e-tehingute usaldusteenuste vahendeid. Sellisel juhul tuleb andmete kontrollimiseks kasutada vähemalt Kaks erinevat allikat füüsilise isiku isikusamasuse tuvastamiseks esitatud andmete kontrollimisel. Kahte erinevat allikat ei pea rakendama piiratud teovõimega kliendi suhtes, kelle nimel loob ärisuhte või teeb tehingu tema esindaja.

4.60. Tuleb kindlaks teha, kas isik tegutseb enda või teise (füüsilise või juriidilise) isiku nimel, st vajadusel tuvastada füüsilise isiku tegelik kasusaaja.

4.61. Kui isik tegutseb teise isiku nimel, peab rakendama meetmeid selle isiku suhtes, kelle nimel tehinguid tehakse (vt ka juriidilise isiku isikusamasuse tuvastamise osas juhendi punkti 4.87.).

4.62. Juhul, kui kliendi või juhuti tehtavas tehingus osaleval isikul on esindaja, tuleb esindaja isikusamasus tuvastada ning esitatud teavet kontrollida usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal.

4.63. Esinduse puhul peab kohustatud isik lisaks tuvastama ja kontrollima ka esindusõiguse olemasolu ning selle ulatust. Kohustatud isik peab jälgima esindajatele antud esindusõiguse tingimusi ning osutama teenuseid ainult esindusõiguse ulatuses (näiteks, kas tegemist on ühekordse tehinguga või korduvate tehingute tegemisega teatud perioodi jooksul).

4.64. Piiratud teovõimega isikute, sealhulgas alaealiste, puhul peab lisaks juhendis antud juhistele ning RahaPTS-is sätestatule, lähtuma tsiviilseadustiku üldosa seaduses, võlaõigusseaduses ja perekonnaseaduses sätestatud normidest. Lisaks piiratud teovõimega isiku isikuandmetele tuleb isikusamasuse tuvastamisel kontrollida seadusliku esindaja (lapsevanema(te) või eeskostja(te)) isikuandmeid.

4.65. Kliendi tundmine või tema avalik tuntus ei ole aluseks seaduses sätestatud isikusamasuse tuvastamise protseduuri mittetäitmiseks. Isikusamasust tuleb kontrollida ka tehingute või toimingute tegemiseks pöörduvate avalikult tuntud ning nendega otseselt või kaudselt seotud isikute puhul.

4.66. Füüsilise isiku isikusamasuse tuvastamist ja kontrollimist ei pea kohaldama uuesti, kui sama füüsilise isikuga on juba kehtiv ärisuhe ja sama füüsiline isik soovib sõlmida uut kestvuslepingut või saada uut teenust. Samuti siis, kui uut ärisuhet soovib luua füüsiline isik, kelle isikusamasus on juba tuvastatud ja kontrollitud muu õigussuhte raames, kus see isik on olnud teise kliendi esindaja. Eeltoodu kehtib eeldusel, et ei ole kahtlust isikusamasuse tuvastamise kohustuse tekkimise hetkel klienti puudutavate andmete (sealhulgas isikusamasuse tuvastamise ja tegeliku kasusaaja tuvastamise käigus kogutud andmete) õigsuses ja kehtivuses. Füüsilise isiku eelnimetatud tingimustel tuvastamata jätmine ei tähenda, et kliendi osas ei peaks tuvastama uuesti ärisuhte eesmärki juhendi punkti 4.170. mõttes või et ärisuhet ei peaks jälgima juhendi punkti 4.222. mõttes. Kirjeldatud erandit kasutades peab kliendikaustas (ehk kohas, kus hoolsusmeetmete käigus kogutud andmeid säilitatakse) olema selge viide asjakohaste isikusamasuse tuvastamise käigus kogutud dokumentide kättesaamise kohale (ehk nö kliendikaustale, kus algse isikusamasuse tuvastamise käigus kogutud andmed on säilitatud).

4.67. Vajadusel peab kohustatud isik olema valmis selgitama isikusamasuse tuvastamise meetme ja kasutatava kontrollimeetmete valikut pädevale järelevalveasutusele. Ühtlasi peab olema ka valmisolek, et näidata, millisel põhjusel on tegemist usaldusväärse ja sõltumatu allikaga, millised on kaks erinevat allikat (kui sellist viisi kasutatakse), ning põhjendama, miks valitud meede on kooskõlas kliendi ja temaga seotud ärisuhte riskiprofiili ning riskiastmega. Olenevalt tegutsemise valdkonnast tuleb olla valmis järelevalveasutusele näitama kaugtuvastuse teel tehtud toiminguid ja kogutud andmeid (nt videointervjuu).

4.68. Kui kohustatud isikul ei ole võimalik isikusamasuse tuvastamiseks kasutatavat originaaldokumenti näha, võib kasutada isikusamasuse kontrollimiseks ka dokumenti, mis on notariaalselt tõestatud, notariaalselt või ametlikult kinnitatud või muud usaldusväärsest ja sõltumatust allikast pärinevat teavet, sealhulgas ka e-identimise ja e-tehingute usaldusteenuste vahendeid. Kui originaaldokumenti pole võimalik näha,

siis tuleb eelnimetatud andmete kontrollimiseks kasutada vähemalt kahte erinevat allikat.

4.69. **Füüsilise isiku ja esindaja isikusamasuse tuvastamise käigus saadud teabe kontrollimine ja kontrollimise viis**

4.70. Isikusamasuse tuvastamiseks ning andmete kontrollimiseks tuleb kasutada isikut tõendavate dokumentide andmekogusse kantud isiku tuvastamise andmeid. See tähendab, et teabe kontrollimise eesmärgiks on saada kinnitus, kas see isik, kes soovib ärisuhet luua või juhuti tehtavat tehingut teostada, on see isik, kes ta väidab end olevat. Identiteedi kontroll peab põhinema ametlikul isikut tõendaval dokumendil või selle andmetel, mitte ainult kliendi enda esitatud suulisel infol. Näiteks peab kontrollima, kas dokumendil on nimi ja isikukood, kas dokument on kehtiv ja kas fotol olev isik vastab isikule, kes dokumendi esitas.

4.71. Isikusamasust saab tuvastada muu hulgas välisriigis välja antud kehtiva reisidokumendi alusel. Kohustatud isik peaks ka tuvastama, kas esitatud reisidokument on kehtiv ning võimekuse piires kontrollima kas dokumendil esinevad võltsingu tunnused. Erinevate reisidokumentide vormi ja turvaelementide kontrollimiseks võib kohustatud isik kasutada Ehtsate isikut tõendavate ja reisidokumentide avalikku veebiregistrit PRADO[21].

4.72. **Füüsilise ja juriidilise isiku, sealhulgas esindaja ja tegeliku kasusaaja isikusamasuse tuvastamise aeg**

4.73. Isikusamasuse peab tuvastama ja kontrollima mõistliku aja jooksul enne kestvuslepingu sõlmimise toimingutega alustamist või selle sõlmimise ajal. Tehingus osaleva isiku isikusamasus tuleb tuvastada enne tehingu tegemise toimingutega alustamist või tehingu tegemise hetkel. Isikusamasuse tuvastamine enne kestvuslepingu sõlmimist on vajalik eelkõige selleks, et vältida olukorda, kus leping sõlmitakse vale isikuga. Näiteks võib kasutada kellegi teise identiteeti, väidetav klient võib tegutseda ilma volituseta teise isiku nimel või kohustatud isik võib luua kliendisuhte anonüümse isikuga, kelle osas ei ole võimalik rakendada hoolsusmeetmeid ega hinnata temaga seotud riske.

4.74. Isikusamasus on tuvastatud mõistliku aja jooksul enne kestvuslepingu sõlmimist või tehingu tegemist, kui see ajaperiood võimaldab usaldusväärsel viisil kontrollida isikusamasust, sealhulgas kontrollida esitatud andmete õigsust ja hinnata riske, samas piisavalt lähedal kestvuslepingu sõlmimise või tehingu teostamise ajale, et andmed oleks endiselt ajakohased ja kehtivad.

4.75. Kohustatud isiku nõudmisel esitab klient isikusamasuse tuvastamiseks vajalikud dokumendid ja annab asjakohast teavet. Kohustatud isiku nõudmisel kinnitab klient hoolsusmeetmete kohaldamiseks esitatud teabe ja dokumentide õigsust oma allkirjaga.

[21] Council of the European Union - PRADO - Otsing dokumendi väljastanud riigi järgi

4.76. **Usaldusväärne ja sõltumatu allikas füüsilise isiku isikusamasuse tuvastamiseks esitatud andmete kontrollimisel**

4.77. Kohustatud isik peab isikusamasuse tuvastamisel kogutud teavet kontrollima usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal.

4.78. Isikusamasuste tuvastamise käigus saadud teabe usaldusväärseks ja sõltumatuks kontrollimiseks peetakse olukorda, kus:

4.78.1. isik tuvastatakse näost-näkku;

4.78.2. infotehnoloogilise seadme abil;

4.78.3. notariaalselt või ametlikult kinnitatud isikut tõendava dokumendi ärakirja alusel ja selle ärakirja dokumendi originaali nägemisel.

4.79. Kui punktis 4.78. nimetatud dokumente ei esitata või pole võimalik esitada, siis on usaldusväärseks ja sõltumatuks allikaks isikusamasuse tuvastamise käigus saadud muu teabe kontroll, mis peab vastama järgmistele tingimustele ja olema korraga täidetud:

4.79.1. teave pärineb kahest erinevast allikast (juhendi punkt 4.82.);

4.79.2. keskmise või kõrgema riski korral peab klient saatma vahetult enne andmete edastamist tehtud näofoto, ja kohustatud isik peab veenduma, et foto on värske;

4.79.3. teave on usaldusväärne ja sõltumatu ning vastab järgmistele tunnustele:

4.79.3.1. teave, mille on välja andnud (isikut tõendavad dokumendid) või mis on saadud kolmandalt isikult või kohast, kellel ei ole mingeid huve või seotust kliendi ega ka kohustatud isikuga ehk see on neutraalne. Näiteks ei ole selleks Internetist saadud informatsioon, sest see pärineb tihti kliendilt endalt või selle usaldusväärsusust ja sõltumatust ei ole võimalik kontrollida;

4.79.3.2. teave, mille usaldusväärsuse ja sõltumatuse määramiseks puuduvad objektiivsed takistused ning usaldusväärsus ja sõltumatus on arusaadav ka kolmandale ärisuhtega mitteseotud isikule. See tähendab, et allika usaldusväärsuses ja sõltumatuses ei ole põhjust kahelda ning ka kõrvalised isikud, sealhulgas järelevalveasutused saadavad aru, miks allikat on peetud usaldusväärseks. Usaldusväärne ja sõltumatu allikas võib olla näiteks ametlik riiklik register, pangakonto andmed, notariaalselt kinnitatud dokumendid jne. Mitte objektiivseteks võib pidada andmeid näiteks kliendi enda kodulehelt, sotsiaalmeedia profiili, juhuslikku infot internetist jne;

4.79.3.3. teave, milles olevad või mille kaudu saadud andmed on aja- ja asjakohased ning selles suudetakse veenduda (seejuures veenduda saab toimuda teatud juhtudel ka ülalnimetatud kahe punkti alusel). Näiteks kontrollides kliendi andmeid ametlikus registris või kehtiva isikut tõendava dokumendi alusel.

4.80. Usaldusväärse ja sõltumatu allika valikul peab kohustatud isik veenduma dokumendi kehtivuses ja selle vastavuses isikut tõendavate dokumentide seaduse nõuetele. Samuti peab kohustatud isik veenduma välises sarnasuses ja ealises sobivuses dokumendi fotol kujutatud isiku välimusega ning dokumendis sisalduvate andmetega.

4.81. Kohustatud isik hindab, millisel juhul peab usaldusväärse ja sõltumatu allika edastamisviis või selle allika saamine olema samuti usaldusväärne ja sõltumatu kanal või vahend (meede), võttes sellise hinnangu andmisel arvesse riskipõhist lähenemist ehk kliendi ja ärisuhtega kaasnevat riski ja nende riskiprofiili.

4.82. **Kaks erinevat allikat füüsilise isiku isikusamasuse tuvastamiseks esitatud andmete kontrollimisel**

4.83. Üheks allikaks peetakse alati:

4.83.1. pildiga isikut tõendavat dokumenti[22]; või

4.83.2. usaldusväärsetest ja sõltumatutest allikatest saadud samal dokumendil oleva isiku andmeid.

4.84. Teiseks allikaks võib olla ka usaldusväärsest ja sõltumatust allikast saadud järgnev teave:

4.84.1. teine dokument (selle koopia), mis on kirjeldatud eelnevates punktides 4.83.1. ja 4.83.2.

4.84.2. isiku digitaalse isikutuvastusvahendiga teostatud tugeva autentimise käigus saadud teave (minimaalselt nimi ning isikukood või isikukoodi puudumisel sünniaeg ja -koht) ning selle teostamist tõendav kontrolljälg;

4.84.3. isikuga vahetult seotud andmete kontroll rahvastikuregistri vm samaväärse registri kaudu, eeldusel, et tegemist on usaldusväärse ja sõltumatu allikaga;

4.84.4. kontrollmaksest saadud informatsioon (kui kohustatud isiku teenus võimaldab seda);

4.84.5. muud biomeetrilised andmed (sõrmejälg, näokujutis) vms informatsioon;

4.84.6. teave, et kontrollida isikuga vahetult seotud andmeid (näiteks töö-, elu- või õppimiskohta).

4.85. **Erisused volitatud esinduse puhul**

4.86. Volitatud ja seadusjärgsete esindajate esindusõiguse käsitlemisel tuleb kindlaks teha, kas esindaja tunneb oma klienti. Esindaja ja esindatava tegelike suhete olemuse selgitamiseks peab esindaja teadma tema poolt esindatava isiku tahteavalduste sisu ja eesmärki, samuti peab ta oskama vastata muudele asjakohastele küsimustele esindatava (äri)tegevuse asukoha, tegevusalade, käibe ja tehingupartnerite, teiste seotud isikute ja tegelike kasusaajate kohta. Lisaks peab esindaja kinnitama, et on teadlik ja veendunud esindatava tehingus kasutatavate vahendite allikast ning legaalsest päritolust, mis tähendab seda, et esindaja peab alati olema teadlik esindatava vahendite päritolust.

[22] (i) isikut tõendav dokument, vastavalt isikut tõendavate dokumentide seaduse §-s 2 lg 2 nimetatud loetelule;
(ii) välisriigis välja antud kehtiv reisidokument;
(iii) juhiluba, mis vastab isikut tõendavate dokumentide seaduse § 4 lg 1 sätestatud tingimustele;
(iv) alla 7-aastase isiku puhul perekonnaseisutoimingute seaduse §-s 30 nimetatud sünnitõend;
(v) notariaalselt tõestatud või notariaalselt või ametlikult kinnitatud ülalnimetatud dokument või muud usaldusväärsest ja sõltumatust allikast pärit teavet, sealhulgas e-identimise ja e-tehingute usaldusteenuste vahendeid, kasutades sellisel juhul andmete kontrollimiseks vähemalt kahte erinevat allikat.

4.87. **Juriidilise isiku isikusamasuse tuvastamine**

4.88. Ärisuhte loomisel või juhuti tehtava tehingu tegemisel peab tuvastama juriidilisest isikust kliendi või juhuti tehtavas tehingus osaleva juriidilise isiku isikusamasuse ning esitatud teavet kontrollima (verifitseerima) usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal, sealhulgas e-identimise ja e-tehingute usaldusteenuste vahendite abil.

4.89. Lisaks juriidilise isiku isikusamasuse tuvastamisele, tuleb tuvastada ka juriidilise isiku esindaja ning tegeliku kasusaaja isikusamasus ning saadud andmeid kontrollida. Juriidilise isiku esindaja isikusamasuse tuvastamisel jälgitakse punktis 4.53. toodut. Juriidilise isiku esindaja on:

4.89.1. juhatuse liige;

4.89.2. prokurist;

4.89.3. volitatud esindaja;

4.89.4. muu seaduslik esindaja, kelle esindusõigus tuleneb seadusest.

4.90. Välisriigi juriidilise isiku esindaja peab kohustatud isiku nõudel esitama oma volitusi tõendava notariaalselt või sellega võrdsustatud korras kinnitatud dokumendi, mis on legaliseeritud või kinnitatud legaliseerimist asendava tunnistusega (apostilliga), kui välislepingust ei tulene teisiti.

4.91. Isikusamasuse tuvastamise protsess tuleb kirjeldada protseduurireeglites. Protsessi kirjelduses peab olema selgitatud, milliseid andmeid juriidilise isiku isikusamasuse tuvastamisel säilitatakse. Näiteks, kui juriidilise isiku isikusamasust kontrollitakse läbi registri päringu, siis tuleb protsessides kirjeldada, kas ja millistel tingimustel registri väljavõtteid päringu tegemise kohta säilitatakse. Näiteks ei ole selge ja arusaadav protsess, kui osaliselt klientide registrikaarte säilitatakse ning osaliselt mitte. Sellises olukorra puudub järelevalveasutusel ülevaade, kas konkreetse kliendi registripäring on teostatud või mitte. Protsess peab olema läbivalt ühetaoline ja jälgitav. Kui registrikaardi väljavõtet ei säilitata, siis tuleb protsessides kirjeldada, kuidas on taasesitamist võimaldaval viisil võimalik kontrollida päringu tegemise logi.

4.92. **Juriidilise isiku tuvastamisel säilitab kohustatud isik järgmised andmed:**

4.92.1. juriidilise isiku nimi või ärinimi, sealhulgas juriidilise isiku õiguslik vorm;

4.92.2. registrikood või registreerimisnumber ja -aeg;

4.92.3. juhataja nimi või juhatuse liikmete või muu seda asendava organi liikmete nimed ja nende volitused juriidilise isiku esindamisel;

4.92.4. juriidilise isiku sidevahendite andmed;

4.92.5. juriidilise isikuga vahetult seotud andmed nagu juriidilise isiku asukoht (st kus riigis juriidiline isik asutati) ning tegevuskoht.

4.93. **Juriidilise isiku isikusamasus tuvastatakse järgmiste dokumentide alusel:**

4.93.1. asjakohase registri registrikaart;

4.93.2. asjakohase registri registreerimistunnistus; või

4.93.3. eelnimetatud dokumendiga võrdväärne dokument. Muu võrdväärne dokument peab pärinema usaldusväärsest allikast (registrist või ametiasutuselt) ning sisaldama ettevõtte põhiandmeid. Muu dokument peab tõendama ettevõtte registreerimist samaväärselt registrikaardi või registreerimistunnistusega.

4.94. Kui kohustatud isikul ei ole võimalik isikusamasuse tuvastamiseks kasutatavat originaaldokumenti näha, võib kasutada isikusamasuse kontrollimiseks ka dokumenti, mis on notariaalselt tõestatud, notariaalselt või ametlikult kinnitatud või muud usaldusväärsest ja sõltumatust allikast pärinevat teavet, sealhulgas ka e-identimise ja e-tehingute usaldusteenuste vahendeid. Kui originaaldokumenti pole võimalik näha, siis tuleb eelnimetatud andmete kontrollimiseks kasutada vähemalt kahte erinevat allikat.

4.95. Juriidilise isiku ja tema esindaja ning tegelike kasusaajate isiku tuvastamist ja isikusamasuse kontrollimist ei pea kohaldama uuesti, kui sama juriidilise isikuga on juba kehtiv ärisuhe ja sama juriidiline isik soovib sõlmida uut kestvuslepingut või saada uut teenust. Ülaltoodu kehtib ka juhul, kui uut ärisuhet soovib luua füüsiline isik, kelle isikusamasus on tuvastatud ja kontrollitud muu õigussuhte raames, kus see isik on olnud teise kliendi esindaja. Eeltoodu kehtib eeldusel, et ei ole kahtlust klienti puudutavate andmete (sealhulgas isikusamasuse tuvastamise ja tegeliku kasusaaja tuvastamise käigus kogutud andmete) õigsuses ja kehtivuses. Eeltoodu ei tähenda, et kliendi osas ei peaks tuvastama uue ärisuhte eesmärki juhendi punkti 4.170. mõttes või et ärisuhet ei peaks jälgima juhendi punkti 4.222. mõttes. Antud punktis kirjeldatud erandit kasutades peab kliendikaustas (ehk kohas, kus hoolsusmeetmete käigus kogutud andmeid säilitatakse) olema selge viide asjakohaste isikusamasuse tuvastamise käigus kogutud dokumentide kättesaamise kohale (ehk nö kliendikaustale, kus algse isikusamasuse tuvastamise käigus kogutud andmeid säilitatakse).

4.96. Kohustatud isik peab olema valmis selgitama ja põhjendama isikusamasuse tuvastamise meetme ja kasutatava kontrollimeetme valikut pädevale järelevalveasutusele. Sealhulgas tuleb vajadusel selgitada, miks on tegemist usaldusväärsest ja sõltumatust allikast pärit teabega, millised on need kaks erinevat allikat, ning põhjendama, miks valitud meede on kooskõlas kliendi ja temaga seotud ärisuhte riskiprofiili ning riskiastmega.

4.97. Kohustatud isiku nõudmisel peab klient esitama isikusamasuse tuvastamiseks vajalikud dokumendid ja andma asjakohast teavet. Samuti kinnitab klient kohustatud isiku nõudmisel hoolsusmeetmete kohaldamiseks esitatud teabe ja dokumentide õigsust oma allkirjaga. Juhul kui kohustatud isikul on ligipääs asjakohastesse registritesse, ei pea ta kliendilt nõudma isikusamasuse tuvastamiseks kasutatavate asjakohaste dokumentide esitamist, näiteks registrikaardi väljavõtet.

4.98. **Juriidilise isiku isikusamasuse tuvastamise käigus saadud teabe kontrollimine ja kontrollimise viis**

4.99. Isikusamasuse tuvastamise käigus saadud teabe kontrollimine tähendab seda, et isiku esitatud andmete õigsust ja tõesust kontrollitakse usaldusväärsest ja sõltumatust allikast pärit andmete abil. Kontrollimise käigus võrreldakse juriidilise isiku esitatud andmeid usaldusväärsest ja sõltumatust allikast saadud teabega, et saada kinnitust esitatud andmete õigsuse kohta. Kontrollimise eesmärk on veenduda, et isik, kes soovib luua ärisuhet või teha juhuti tehingut, on tegelikult see sama isik, kelleks ta end esitleb.

4.100. **Usaldusväärne ja sõltumatu allikas juriidilise isiku isikusamasuse tuvastamise käigus saadud teabe kontrollimisel**

4.101. Usaldusväärseks ja sõltumatuks allikaks loetakse, kui kohustatud isik:

4.101.1. näeb isikusamasuse tuvastamisel esitatud originaaldokumenti (juhendi punkt 4.93.);

4.101.2. näeb eelnimetatud originaaldokumendi notariaalselt tõestatud või notariaalselt või ametlikult kinnitatud ärakirja;

4.101.3. omab ligipääsu äriregistri, mittetulundusühingute ja sihtasutuste registri või välisriigi asjakohaste registrite andmetele arvutivõrgu kaudu.

4.102. Registrist väljastatav dokument ei tohi olla välja antud varem kui 6 kuud enne selle esitamist. Kehtib ka siis kui dokumendist on tehtud ärakiri.

4.103. Olukordades, mida juhendi punktis 4.101. nimetatud ei ole, on usaldusväärseks ja sõltumatuks allikaks juriidilise isiku isikusamasuse tuvastamise käigus saadud teabe kontroll, mis:

4.103.1. pärineb kahest allikast;

4.103.2. mille on välja andnud või mis on saadud kolmandalt isikult või kohast, kellel ei ole mingeid huve või seotust ei kliendi ega ka kohustatud isikuga ehk kontrollimiseks kogutud teave on neutraalne (näiteks ei ole selleks Internetist saadud informatsioon, sest see pärineb tihti kliendilt endalt või selle usaldusväärsust ja sõltumatust ei ole võimalik kontrollida);

4.103.3. mille usaldusväärsuse ja sõltumatuse määramiseks puuduvad objektiivsed takistused ning usaldusväärsus ja sõltumatus on arusaadav ka kolmandale ärisuhtega mitteseotud isikule;

4.103.4. milles olevad või mille kaudu saadud andmed on aja- ja asjakohased ning kohustatud isik suudab selles veenduda (seejuures veendumine saab toimuda teatud juhtudel ka ülalnimetatud kahe punkti alusel).

4.104. Kui aga juriidilise isiku esindaja tuvastamine toimub näost-näkku, tuleb kasutada juhendi punktis 4.53. nimetatud allikaid.

4.105. **Kaks erinevat allikat juriidilise isiku isikusamasuse tuvastamise käigus saadud teabe kontrollimisel**

4.106. Kaks erinevat allikat tähendab, et informatsiooni saamise andmekandja, koht või meede peavad olema erinevad (st selleks ei saa olla sama andmekandja).

4.107. Lisaks juhendi punktis 4.93. nimetatud dokumentidele, mille alusel juriidilise isiku isikusamasust tuvastatakse, võib teiseks allikaks olla ka usaldusväärsest ja sõltumatust allikast saadud teave, et kontrollida isikuga vahetult seotud andmeid (näiteks asukoht jms).

4.108. **Legaliseerimine ja apostilliga kinnitamine ning dokumentide keel**

4.109. Välisriigis välja antud avalikud dokumendid peavad olema legaliseeritud või kinnitatud tunnistusega (välja antud apostille[23]) ehk ühes riigis välja antud ametliku dokumendi kasutamiseks teises riigis on antud rahvusvaheliselt tunnustatud tõestus dokumendi ehtsuse kohta, kusjuures legaliseerimise ja apostillimisega ei kinnitata dokumendis sisalduva teabe õigsust.

4.110. Dokument peab olema legaliseeritud, kui sellele ei kohaldata apostille-ga rakendamise korda. Legaliseerimiseks peab dokument läbima nii selle väljastanud asutuse riigi kui ka dokumenti vastuvõtva riigi legaliseerimisega tegelevad ametiasutused (tavaliselt välisministeeriumid).

4.111. Samal ajal:

4.111.1. legaliseerimist ega apostillimist ei vaja avalikud dokumendid, mis on koostatud või tõestatud riikides, kellega Eestil on sõlmitud vastav õigusabileping;

4.111.2. legaliseerimist ega apostillimist ei vaja avalikud dokumendid, mis on välja antud riigis, mis kohaldab Euroopa Ühenduse liikmesriikide dokumentide legaliseerimisest loobumise konventsiooni.

4.112. Võõrkeelsete dokumentide korral on õigus nõuda dokumentide tõlget kohustatud isikule arusaadavasse keelde. Vältida tuleks tõlgete kasutamist olukorras, kus originaaldokumendid on koostatud arusaadavas keeles (nt ingliskeelsete originaaldokumentide tõlkimine vene keelde).

Isikusamasuse tuvastamise kontrollküsimuste näited:

- Kas kliendi ja esindaja isikusamasus on tuvastatud enne teenuse osutamist?

- Kas isikusamasuse tuvastamise protsess vastab sisemistes protseduurides kirjeldatule ja seaduses esitatud nõuetele?

- Kas esitatud isikut tõendav dokument vastab RahaPTS-is esitatud nõuetele (nt ei ole isikusamasuse tuvastamisel kasutatud mõne riigi sisepassi, mis ei ole välisriigis väljastatud kehtiv reisidokument)?

- Kas isikusamasuse tuvastamiseks kasutatud dokument on kehtiv?

[23] https://www.notar.ee/et/teabekeskus/apostillimine

- Kas isikusamasuse tuvastamisel esitatud andmed on kontrollitud usaldusväärsest ja sõltumatust allikast?

- Kas isikusamasuse tuvastamisel koguti ja säilitati kõik andmed, mida kohustab koguma RahaPTS?

- Kas kasutatud identifitseerimisviis on RahaPTS-i mõistes aktsepteeritav (asjakohasel juhul, kas on täidetud kaugtuvastamise nõuded finantseerimisasutuste puhul, sealhulgas andmete registreerimine ja säilitamine nõutud viisil)?

4.113. **Füüsilise ja juriidilise isiku tegeliku kasusaaja tuvastamine**

4.114. **Füüsilise isiku tegeliku kasusaaja tuvastamine**

4.115. Kui füüsilise isiku isikusamasuse tuvastamisel tekib kahtlus, et isik ei tegutse enda eest ja nimel, siis tuleb tuvastada ka füüsilise isiku tegelik kasusaaja ehk isiku tegevust kontrolliv ja sellest kasusaav isik.

4.116. Kahtlus tegeliku kasusaaja olemasolu kohta võib tekkida eelkõige juhul, kui hoolsusmeetmete rakendamisel tekib tunne, et füüsilist isikut on kallutatud ärisuhte loomisele või tehingu tegemisele. Sellisel juhul tuleb tegelikuks kasusaajaks pidada isikut, kes teostab kontrolli füüsilise isiku üle.

4.117. Juhul kui tuvastatakse, et tehinguid või toiminguid teostatakse tegelikult kolmanda isiku nimel, peab rakendama kõiki meetmeid, et tuvastada tegelik kasusaaja (juhendi punkt 4.113.) ning teostama kõiki toiminguid, et tuvastada ärisuhte tegelik eesmärk (juhendi punkt 4.170.).

Indikaatorid, mis võivad viidata, et füüsilise isiku tegelik kasusaaja on keegi kolmas:

- klient ei oska selgitada tehingu või ärisuhte eesmärki;
- ebamäärased selgitused rikkuse päritolu kohta;
- klient teeb väga suuri tehinguid, mis ei ole kooskõlas tema majandusliku olukorraga;
- kliendil puudub valdkonna kogemus;
- klient soovib arveid kolmanda isiku nimele;
- kliendi olemus ja käitumine on ebatavalised;
- tasumine toimub läbi vahendajate jne.

4.118. **Juriidilise isiku tegeliku kasusaaja tuvastamine**

4.119. Ärisuhte loomisel või juhuti tehtava tehingu tegemisel peab tuvastama kliendi või juhuti tehtavas tehingus osaleva isiku tegeliku kasusaaja. Tegeliku kasusaaja isikusamasuse kontrollimiseks meetmeid tuleb rakendada ulatuses, mis võimaldavad veenduda, kes on tegelik kasusaaja.

4.120. Tegelikuks kasusaajaks saab olla ainult füüsiline isik(ud), kellel on omandi või muul viisil kontrollimise (nt tegevuse finantseerimise) kaudu lõplik valitsev mõju füüsilise või juriidilise isiku üle või kelle huvides, kasuks või nimel tehing või toiming tehakse.

4.121. Ärisuhte loomisel või juhuti tehtava tehingu tegemisel peab saama aru juriidilisest isikust kliendist või tehtavas tehingus osaleva isiku omandi- ja kontrollistruktuurist.

4.122. Kohustatud isik võib tugineda omandi- ja kontrollistruktuuri hindamisel ja kontrollimisel kliendi esitatud andmetele, kuid peab veenduma, et esitatud andmed on õiged ning omandi-ja/või kontrollistruktuuris ei varjata tegelikke kasusaajaid või muid kliendi üle kontrolli omavaid isikuid. Näiteks esitatud andmed omandistruktuuri osas erinevad tegeliku kasusaaja kontrollimisel saadud andmetest.

4.123. Juriidilist isiku ja tema esindajat ning tegelikke kasusaajaid ei pea uuesti tuvastama juhul, kui sama kliendiga on juba kehtiv ärisuhe ja sama klient soovib sõlmida uut kestvuslepingut või saada uut teenust. Eeltoodu kehtib, kui ei ole kahtlust klienti

puudutavate andmete (sealhulgas isikusamasuse tuvastamise ja tegeliku kasusaaja tuvastamise käigus kogutud andmete) õigsuses ja kehtivuses. Eeltoodu ei tähenda, et kliendi osas ei peaks tuvastama uut ärisuhte eesmärki (juhendi punkti 4.170. mõttes) või et ärisuhet ei peaks jälgima (juhendi punkti 4.222. mõttes). Antud punktis kirjeldatud erandit kasutades peab kliendikaustas (ehk kohas, kus hoolsusmeetmete käigus kogutud andmeid säilitatakse) olema selge viide asjakohaste isikusamasuse tuvastamise käigus kogutud dokumentide kättesaamise kohale (ehk nö kliendikaustale, kus algse isikusamasuse tuvastamise käigus kogutud andmeid säilitatakse) või dubleeritult varasemalt kogutud andmed.

4.124. Vajadusel tuleb olla valmis selgitama pädevale järelevalveasutusele tegeliku kasusaaja ning omandi- ja kontrollistruktuuri tuvastamiseks kohaldatud meetmete ja selleks valitud kontrollimeetmete valikut.

4.125. Juriidilise isiku tegeliku kasusaaja tuvastamine käib astmeliselt. Iga järgmise astme juurde siirdub kohustatud isik siis, kui eelmise astme puhul ei ole võimalik juriidilise isiku tegelikku kasusaaja määrata. Juriidilise isiku tegeliku kasusaaja tuvastamisel lähtutakse järgnevatest astmetest:

4.125.1. tuvastatakse füüsiline isik või isikud, kes lõplikult kontrollivad juriidilist isikut või omavad selle üle muul viisil mõju, sõltumata nende aktsiate, osade, hääleõiguste või omandiõiguse suurusest ning sellest, kas kontroll on otsene või kaudne;

4.125.2. selgitatakse välja kelle huvides, kasuks või nimel tehing või toiming tehakse. Näiteks kui arveid maksab kolmas isik või on kahtlus, et ettevõtet rahastatakse varjatud isikute kaudu, võib see viidata, et tegelik kasusaaja on keegi teine, mitte see, kes ametlikult esitati;

4.125.3. tuvastatakse füüsiline isik või isikud, kes omavad või kontrollivad juriidilist isikut otsese või kaudse osaluse kaudu. Siinkohal tuleb arvestada ka võimalikku perekondlikku ja lepingulist seost, kui seda on võimalik tuvastada;

4.125.4. tuvastatakse füüsiline isik või isikud, kelle otsene24 ja kaudne osalus25 kokku ületab äriühingus 25%, sealhulgas osalused esitajaaktsiate või -osade kaudu või muul viisil.

4.125.5. Kui eelnevate sammude alusel ei ole võimalik tegelikku kasusaajat tuvastada, määratakse tegelikuks kasusaajaks juriidilise isiku kõrgema juhtorgani liige.

4.125.6. Kui eelnimetatud füüsilisi isikuid on mitu, käsitletakse tegeliku kasusaajana äriühingu üle faktilist kontrolli teostavat isikut või isikuid, kes teevad äriühingus strateegilisi otsuseid või juhivad selliste isikute puudumisel organisatsiooni.

4.126. Kõrgema juhtorgani liikme all tuleb mõista isikut, kes:

4.126.1. teeb strateegilisi otsuseid, mis fundamentaalselt mõjutavad äritegevust ja/või -tavasid ja/või äriühingu üldisi (äri)suundi; või selle puudumisel;

[24] Otsene osalus tähendab, et füüsilisel isikul on äriühingus osalus isiklikult.
[25] Kaudne osalus tähendab, et füüsilisel isikul on äriühingus osalus ühe või mitme isiku või isikute ahela kaudu.

4.126.2. juhib äriühingut igapäevaselt või regulaarselt (näiteks tegevusjuht (CEO), finantsjuht (CFO), direktor või president jne).

4.127. Seltsingu, ühisuse või muu juriidilise isiku staatust mitteomavate isikute ühenduse puhul on tegelik kasusaaja:

4.127.1. ühenduse looja;

4.127.2. vara säilimist tagav ja kontrolliv isik, kui selline isik on määratud;

4.127.3. soodustatud isik või kui soodustatud isik või isikud määratakse tulevikus, siis isikute ring, kelle huvides usaldushaldus või isikute ühendus loodi või tegutseb;

4.127.4. muu isik, kes ükskõik millisel moel omab lõplikku kontrolli usaldushalduse või ühenduse vara üle.

4.128. **Juriidilisest isikust tegeliku kasusaaja tuvastamisel kogutud andmete kontrollimine**

4.129. Tuvastatud tegeliku kasusaaja kontrollimiseks rakendatakse meetmeid ning tehakse seda ulatuses, mis võimaldab veenduda, kes on tegelik kasusaaja.

4.130. Juriidiliste isikute puhul on selleks järgmised võimalused:

4.130.1. kohustatud isik näeb juriidilise isiku isikusamasuse tuvastamisel esitatud dokumendi originaali[26];

4.130.2. omatakse ligipääsu äriregistri, mittetulundusühingute ja sihtasutuste registri või välisriigi asjakohaste registrite andmetele arvutivõrgu kaudu ning kontrollitakse tegeliku kasusaaja andmeid nimetatud registrist;

4.130.3. nähakse juriidilise isiku isikusamasuse tuvastamisel esitatud dokumendi notariaalselt või ametlikult kinnitatud ärakirja;

4.130.4. kasutatakse muid avalikult kättesaadavaid ja/või usaldusväärseid allikaid, mis on piisavad, et tuvastada tegelik kasusaaja.

4.131. Kui juriidilise isiku isikusamasuse tuvastamise dokumentidest või muudest esitatud dokumentidest ei nähtu otseselt, kes on juriidilise isiku tegelik kasusaaja, siis registreeritakse vastavad andmed (sealhulgas andmed kontserni kuuluvuse ning kontserni omanike- ja juhtimisstruktuuri kohta) juriidilise isiku esindaja ütluste või juriidilise isiku esindaja omakäelise kirjaliku dokumendi alusel. Sellisel juhul peab rakendama mõistlikke meetmeid, et esitatud teavet kontrollida.

4.132. Seltsingu, ühisuse või muu sarnase ühenduse puhul tuleb välja selgitada tegelik kasusaaja. Selleks kasutatakse lisaks avalikele ja usaldusväärsetele andmetele ka dokumente, nagu seltsinguleping või soovide avaldus (*letter of wishes*). Kui finantseerimisasutus soovib kasutada tegeliku kasusaaja ütlusi või tema omakäelist kirjalikku dokumenti, tuleb kohaldada juhendi punktis 4.130. toodut.

4.133. Kui ärisuhte jooksul või selle seirel toimuvad tasumised kolmandate isikute poolt, võib see viidata näiteks vajadusele pöörata täiendavalt tähelepanu ja kontrollida üle tegeliku kasusaaja tuvastamiseks võetud meetmed.

4.134. Kui kohustatud isik tuvastab tegeliku kasusaaja, kes erineb äriregistrisse märgitud tegelikust kasusaajast, siis annab kohustatud isik äriregistri pidajale mõistliku aja jooksul teada tuvastatud asjaoludest, välja arvatud juhul kui erinev tegelik kasusaaja või muu asjaolu on seotud sellise tegevuse või asjaoludega, mille puhul tuleb Rahapesu Andmebüroole esitada teade (RahaPTS § 49 lg 1). Kui esinevad RahaPTS-i § 49 lg 1 asjaolud, siis äriregistri pidajat ei teavitata.

Kontrollküsimuste näited tegelike kasusaajate tuvastamisel. Hinnat tuleks, kas:

- tegeliku kasusaaja tuvastamiseks võetud meetmed, teostatud toimingud ning kogutud andmed on dokumenteeritud ja tõendatavad?

- tuvastatud tegelik kasusaaja vastab avalikest andmebaasidest esitatud informatsioonile? Kui ei, siis miks?

[26] 1.asjakohase registri registrikaart;
2. asjakohase registri registreerimistunnistus või
3. eelnimetatud dokumendiga võrdväärne dokument. Muu võrdväärne dokument peab pärinema usaldusväärsest allikast (registrist või ametiasutuselt) ning sisaldama ettevõtte põhiandmeid. Muu dokument peab tõendama ettevõtte registreerimist samaväärselt registrikaardi või registreerimistunnistusega.

- tegeliku kasusaaja tuvastamiseks on vaja teostada täiendavaid päringuid või koguda kliendilt/allikatest täiendavaid andmeid?

- kliendi nimel suhtlevate isikute ring vastab volitatud isikute ringile või registrisse märgitud isikute ringile? Kui ei, siis kas sellel on mõistlik põhjendus?

- klient tasub oma arveid ise või teeb seda kolmas isik? Kas klient eelistab seletamatul põhjusel virtuaalvääringutes tasumist?

- saadakse aru kliendi omandistruktuurist? Kui ei, siis mida on vaja täiendavalt teha, et omandistruktuurist aru saada?

- kliendiga seotud isikute seas on nomineeritud aktsionäre või juhatuse liikmeid või muid tegeliku kasusaaja varjamise viise? Kui jah, siis kas on olemas protseduur varjamise tuvastamiseks ja vajadusel Rahapesu Andmebüroole teatamiskohustuse täitmiseks?

4.135. **Riikliku taustaga isik, sealhulgas tema perekonnaliige või lähedane kaastöötaja**[27]

4.136. Riikliku taustaga isik on füüsiline isik, kes täidab või on täitnud avaliku võimu olulisi ülesandeid ja kelle suhtes jätkuvalt esinevad avaliku võimu teostamisega seotud riskid. Riikliku taustaga isikuks loetakse ka isik, kes on Euroopa Komisjoni avaldatud loeteludes määratletud avaliku võimu oluliste ülesannete täitjana Euroopa Liidu liikmesriigi, Euroopa Komisjoni või Euroopa Liidus akrediteeritud rahvusvahelise organisatsiooni poolt. Loetelu Eesti ametikohtadest, mille täitjad loetakse riikliku taustaga isikuteks, kehtestab valdkonna eest vastutav minister määrusega.

4.137. Juriidilisest isikust kliendi või juhuti tehtavat tehingut tegeva isiku puhul peab seda isikut pidama riikliku taustaga isikuks, kui tema esindaja või tegelik kasusaaja on riikliku taustaga isik või riikliku taustaga isiku perekonna liige või lähedane kaastöötaja.

4.138. Riigi omanduses oleva juriidilisest isikust kliendi või juhuti tehtavat tehingut tegeva isiku puhul peab isikut pidama riikliku taustaga isikuks, kui riikliku taustaga isik omab ettevõttes olulist ja prominentset funktsiooni ning sellest ettevõtjast omab 50%-list osalust riik. Sellise olulise ja prominentse funktsiooni hindamisel tuleb muu hulgas ka hinnata, kas riikliku taustaga isik omab (olulist) volitust riigi varade või rahaliste vahendite, poliitikate või tegevuse üle, kas tal on õigus väljastada litsentse või lubasid, teha erandeid, kas tal on kontroll või mõju riigi või äriühingu kontodele ja rahalistele vahenditele jne. Tegemist on võimalike näidetega, mis aitavad kõrge riskiga riikliku taustaga isiku kindlaks tegemisel. Kõiki asjaolusid tuleb hinnata kogumis.

4.139. Kohustatud isikul on õigus riskipõhisel lähenemisel riikliku taustaga isiku ametipositsioone täiendada ning seeläbi rakendada täiendavaid meetmeid ka teistele ametipositsioonidele. Sellisel juhul peavad avaliku võimu ülesanded olema olulised ning ei tohi seostuda kesk- või alamastme ametniku staatuses olevate isikutega.

[27] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf

4.140. Riikliku taustaga isiku pereliige on abikaasa või abikaasaga samaväärseks peetav isik, registreeritud elukaaslane, vanem, laps, lapse abikaasa või abikaasaga samaväärseks peetav isik, lapse registreeritud elukaaslane.[28]

4.141. Riikliku taustaga isiku lähedane kaastöötaja on füüsiline isik, kelle kohta on teada, et ta on juriidilise isiku tegelik kasusaaja koos riikliku taustaga isikuga, tal on lähedased ärisuhted riikliku taustaga isikuga, ta on riikliku taustaga isiku huvides loodud juriidilise isiku tegelik kasusaaja.

4.142. Riikliku taustaga isikuks ei loeta kesk- ja alamastme ametnikke.

4.143. Kui riikliku taustaga isik ei täida enam olulisi avalikke ülesandeid, tuleb vähemalt 12 kuu jooksul arvestada temaga seotud riske ning rakendada asjakohaseid, riskipõhiseid meetmeid seni, kuni on veendutud, et riikliku taustaga isikule omaseid riske enam ei esine.

4.144. **Riikliku taustaga isikuga seotud risk ja selle hindamine**

4.145. Riikliku taustaga isik, tema perekonnaliige või lähedane kaastöötaja on tavapäraselt kõrgema riskiga isik, kelle osas rakendatakse täiendavaid hoolsusmeetmeid. Isik pole kõrge riskiga olukorras, kus kohustatud isiku sisemise riskihinnangu kohaselt on tegemist keskmise või madalama riskiga riikliku taustaga isiku, tema pereliikme või lähedase kaastöötajaga. Näiteks esineb asjaolusid, mis riski vähendavad. Riskipõhisel lähenemisel hinnatakse muu hulgas tõenäosust, et:

4.145.1. isik, tema pereliige või lähedane kaastöötaja võib oma positsiooni kuritarvitada isikliku kasu saamiseks või ebaseadusliku tulu varjamiseks;

4.145.2. isikul on oluline mõju või võimalus kontrollida või suunata vara.

4.146. Riskipõhine lähenemine põhineb kohustatud isiku teadmistel ja kogemusel ning võtab arvesse näiteks:

4.146.1. ametipositsiooni ja selle kestvust;

4.146.2. korruptsioonitaset vastavas riigis või sektoris, millega riikliku taustaga isik on seotud;

4.146.3. majanduslike huvide deklaratsiooni esitamise kohustust;

4.146.4. seoseid riskantsete tegevusvaldkondadega;

4.146.5. negatiivset avalikku teavet isiku kohta;

4.146.6. lisaks arvestatakse muid riskipõhise lähenemise indikaatoreid, mis viitavad kõrgemale riskile.

4.147. **Riikliku taustaga isiku tuvastamine**

4.148. Nii ärisuhte loomisel kui ka ärisuhte seirel ning näiteks kliendi andmete, riskiprofiili või tehingukäitumise olulisel muutusel rakendatakse meetmeid, et tuvastada, kas klient

[28] Abikaasaga samaväärseks peetav isik on isik, kellega riikliku taustaga isik elab püsivas kooselus ja jagab ühiseid majanduslikke või elulisi huve.

või juhuti tehtavat tehingut teostada sooviv isik, nende isikute tegelik kasusaaja või esindaja on riikliku taustaga isik, tema pereliige või lähedane kaastöötaja. Oluline on, et riikliku taustaga isiku staatust ei kontrollitaks vaid ärisuhte loomisel, vaid ka ärisuhte jooksul, et tuvastada, kas klient on saanud selliseks isikuks ärisuhte keskel.

4.149. Riskiga riikliku taustaga isiku tuvastamiseks rakendatavad meetmed:

4.149.1. uute potentsiaalsete ning olemasolevate klientide või juhuti tehtavaid tehinguid soovivate isikute, nende tegelike kasusaajate ja esindajate reaalajas jälgimine vastavatest andmebaasidest (ehk nn nimekontroll andmebaasidest), kes vastavat teenust pakuvad;

4.149.2. riikliku taustaga isiku staatuse küsimine esindajalt (hõlmab nii esindaja ja tegeliku kasusaaja kui ka nende pereliikmete ja lähedaste kaastöötajate vastava staatuse küsimist) või juhuti tehtavat tehingut teostavalt isikult. Samuti vajadusel kliendi või juhuti tehtavat tehingut teostava isiku kutse- või tegevusala küsimine ning eeltoodud andmete uuesti küsimine andmete uuendamise käigus ärisuhte kestel;

4.149.3. avalikult kättesaadavatest ehk kolmandatest allikatest informatsiooni hankimine.

4.150. Riskipõhise lähenemise alusel võib vajadusel rakendada ka täiendavaid meetmeid lisaks eeltoodutele. Neid meetmeid kasutatakse koos ärisuhte või juhuti tehtava tehingu eesmärgi ja olemuse tuvastamisega. Selle käigus kujundab kohustatud isik sisemise veendumuse kliendi kohta ning võib märgata ka kahtlaseid või ebatavalisi asjaolusid, mis võivad viidata riikliku taustaga isiku olemasolule või seosele sellise isikuga.

4.151. Rakendatud meetmed riikliku taustaga isiku tuvastamiseks peavad olema riskipõhised ehk vastama kohustatud isiku suurusele ning tema tegevusega kaasnevatele riskidele. See tähendab, et mida suurem on kliendibaasi risk, et ärisuhe luuakse kõrge riskiga riikliku taustaga isikuga, ning risk, et osutatavate teenuste kaudu võiks kõrge riskiga riikliku taustaga isik soovida kuritegevusest saadud rahalisi vahendeid legaliseerida (ehk pesta) või terrorismi rahastada, seda rohkem või seda ulatuslikumaid meetmeid peab kohustatud isik rakendama.

4.152. Kohustatud isik peab olema valmis pädevale järelevalveasutusele põhjendama, miks kohustatud isik ei ole valinud uute, potentsiaalsete ning olemasolevate klientide või juhuti tehtavaid tehinguid soovivate isikute reaalajas jälgimist andmebaasidest. Samuti seda, miks kohustatud isik leiab, et tema tegevuses puuduvad riikliku taustaga isikutega kaasnevad riskid. Reaalajas riikliku taustaga isikute jälgimine andmebaasides on tõhus meede, millega kohustatud isik saab riske maandada, kuna riikliku taustaga isikutte loetellu kuuluvate isikute ring on lai ning käsitsi iga isiku kontrollimine ei pruugi riski maandada.

4.153. **Riikliku taustaga isiku osas rakendatavad täiendavad hoolsusmeetmed**

4.154. Lisaks üldistele hoolsusmeetmetele tuleb kohaldada riikliku taustaga isiku osas järgmisi hoolsusmeetmeid:

4.154.1. kõrgemalt juhtkonnalt[29] heakskiit selle isikuga ärisuhte loomiseks või jätkamiseks. Heakskiit peab nähtuma juhtkonna vastavas dokumendis (nt juhtkonna koosoleku protokollis või muus dokumendis). Dokumendist peab nähtuma, millistest faktilistest alustest tulenevalt heakskiit otsustati anda;

4.154.2. rakendatakse meetmeid, et teha kindlaks selle isiku rikkuse päritolu või tehingus kasutatud varade päritolu;

4.154.3. tehakse selle ärisuhte seiret tugevdatud korras (juhendi punkti 4.275. ja 4.211.).

4.155. **Rikkuse päritolu tuvastamine**

4.156. Kliendi rikkuse päritolu[30] kohta kogutakse teavet ärisuhte loomisel, kui see on asjakohane.

4.157. Rikkuse päritolu tuleb tuvastada vähemalt järgmistel juhtudel:

4.157.1. kui kohustatud isik puutub majandus- või kutsetegevuse käigus kokku suure riskiga kolmanda riigi isiku või kliendiga;

4.157.2. kui klient on riikliku taustaga isik, riikliku taustaga isiku pereliige või tema lähedaseks kaastöötajaks peetav isik;

4.157.3. kui esineb kahtlus, et tehingud viitavad kuritegevusele, rahapesule või terrorismi rahastamisele;

4.157.4. kui kliendi või tegeliku kasusaaja varaline seisund tundub ebaproportsionaalne;

4.157.5. muudel juhtudel, kui kliendile on määratud kõrge riskiaste.

4.158. Eelnevalt nimetatud juhtudel tuleb tuvastada nii kliendi kui ka tema tegeliku kasusaaja rikkuse päritolu.

4.159. Rikkuse päritolu ja tehingus kasutatud vahendite või vara päritolu[31] on erinevad mõisted. Rikkuse päritolu tuvastamine annab üldise ülevaate kliendi varalise seisundi kujunemisest, sealhulgas sellest, millises mahus võib kliendil olla rahalisi vahendeid ja millistest allikatest need pärinevad. Lisaks teabe kogumisele kliendilt, võib sellist teavet koguda ka usaldusväärsetest avalikest andmebaasidest ning muudest avalikest ja mitteavalikest allikatest, näiteks kinnistusraamatust, maa- vms registritest, majanduslike huvide deklaratsioonidest, äriühingu registritest, sotsiaalmeediast jne.

4.160. Kõrge riskiga juhtudel tuleb rikkuse päritolu kontrollida usaldusväärsete ja sõltumatute andmete või dokumentide alusel. Kohustatud isik ei peaks piirduma kliendi üldiste selgitustega või tegema põhjendamatuid eeldusi (näiteks, et olulisi

[29] Vaata alaviide 17.
[30] Inglise keeles *source of wealth.*
[31] Inglise keeles *source of funds.*

funktsioone omavatel töötajatel ongi suuremad töötasud ja rohkem vara), vaid peab tekkima põhjendatud veendumus kliendi varalise seisundi kujunemise kohta. Kui klient keeldub teabe andmisest, annab ebamääraseid selgitusi või kui esitatud teave ei vasta avalikest või muudest allikatest kättesaadavale teabele, võib see viidata kõrgemale riskile ning nõuda täiendavate hoolsusmeetmete rakendamist. Täiendava hoolsusmeetmena võib küsida kliendilt rikkuse päritolu tõendavaid dokumente. Näiteks kui rikkuse allikana on märgitud pärandus või lotovõit, võib kohustatud isik küsida vastavalt pärimistunnistust või lotovõitu tõendavat dokumenti. Esitatud dokumente ei saa käsitleda pelgalt formaalse nõude täitmisena, vaid neid tuleb ka sisuliselt analüüsida ning vajadusel võrrelda muude kättesaadavate andmetega. Kohustatud isik peab hindama, kas esitatud dokumendid tegelikult kinnitavad väidetud rikkuse päritolu ning kas esitatud teave on kooskõlas muude teadaolevate asjaoludega.

4.161. Kohustatud isik peab oma protseduurireeglites või muudes sisemistes dokumentides selgelt sätestama, millistel juhtudel on vajalik kliendi rikkuse päritolu tuvastamine, milliseid hoolsusmeetmeid rakendatakse ning milliseid tõendeid peetakse piisavaks rikkuse päritolu kinnitamiseks.

4.162. Kogutud teave kliendi rikkuse päritolu kohta ning selle analüüs tuleb kohustatud isikul dokumenteerida kliendifailides või muul viisil kliendikaustas.

Kontrollküsimused rikkuse päritolu tuvastamisel ärisuhte loomisel:

- Kas kliendilt kogutud dokumente rikkuse päritolu tuvastamiseks on sisuliselt analüüsitud ja võimalikud vastuolud on tuvastatud?
- Kas teostatud protsess vastab sisemistes dokumentides ja seaduses sätestatule?
- Kas rikkuse päritolu vastab kliendi üldisele profiilile ja tegevusele? Kui ei, siis kas see on loogiliselt põhjendatav?
- Kas kliendi antud selgitused rikkuse päritolu kohta on piisavad ja põhjendatud?
- Kas tuvastati rikkuse allika päritolu, mitte tehingus kasutatud vara/vahendite päritolu?
- Kas kasutatud makseviis on tavapärane ja põhjendatud ning ei võimalda anonüümsust?
- Virtuaalvääringus tehtavate tehingute ja investeeringute korral: kas on olemas tehnoloogiline lahendus ja võimekus virtuaalvääringu päritolu tuvastamiseks ja hindamiseks?
- Kas kõrgema riskiga klientide või tehingute puhul on rakendatud täiendavaid hoolsusmeetmeid kliendi ja tegeliku kasusaaja osas?

4.163. **Tehingus kasutatud vara päritolu tuvastamine**

4.164. Kohustatud isik tuvastab tehingus kasutatud vara päritolu ärisuhte loomisel eelkõige juhul, kui tehing tehakse väljaspool ärisuhet juhuti tehtava tehinguna. Sel juhul kogub kohustatud isik tehingus kasutatud vara päritolu kohta teavet ärisuhte eesmärgi ja olemuse tuvastamise asemel.

4.165. Ärisuhte olemasolul ei pruugi tehingus kasutatud vara päritolu tuvastamine toimuda ärisuhte loomise etapis, kuid see on kohustuslik ärisuhte seire käigus. Seega peab kohustatud isik arvestama, et tehingus kasutatud vara päritolu kontrollimise kohustus

ei piirdu üksnes juhuti tehtavate tehingutega, vaid kohaldub ka ärisuhte ajal, eelkõige selle seire etapis.

4.166. Lisaks võib kohustatud isik koguda teavet tehingus kasutatud vara päritolu kohta ka juhul, kui tehing on oma olemuselt keerukas, ebatavaline või suure väärtusega ning sellel puudub arusaadav majanduslik või õiguspärane eesmärk.

4.167. Tehingus kasutatud vara päritolu tuvastamine keskendub konkreetse tehingu jaoks kasutatud rahaliste vahendite või muu vara allikale ja selle seaduslikkusele. Eesmärk on veenduda, et tehingus kasutatud vahendid ei pärine kuritegelikest ega ebaseaduslikest allikatest ning tehing ei ole näiline.

4.168. Kohustatud isik sätestab oma protseduurireeglites või muudes sisemistes dokumentides selged kriteeriumid, millistel juhtudel tuleb ärisuhte kestel või juhuti tehtava tehingu puhul tuvastada tehingus kasutatud vara päritolu ning millal rakendada täiendavaid hoolsusmeetmeid, lähtudes riskipõhisest lähenemisest ja õigusaktides sätestatud nõuetest.

4.169. Kogutud teave tehingus kasutatud vara päritolu kohta ning selle analüüs dokumenteeritakse kliendifailis või muus andmete säilitamise süsteemis.

4.170. **Ärisuhte või juhuti tehtava tehingu eesmärgi ja olemuse tuvastamine**

4.171. Ärisuhte loomisel või juhuti tehtava tehingu puhul peab kohustatud isik mõistma ärisuhte või tehingu eesmärki ja olemust. See on tunne-oma-klienti põhimõtte oluline osa ning võimaldab hinnata, kas kliendi tegevus ja soovitud teenus on omavahel kooskõlas.

4.172. Ärisuhte või juhuti tehtava tehingu eesmärgi ja olemuse tuvastamisel tuleb luua süsteem, mis võimaldab eristada, kas kogutav teave puudutab juriidilist isikut, juriidilise isiku esindajat või füüsilist isikut.

4.173. Ärisuhte eesmärgi ja tehingu olemuse mõistmiseks peab vajadusel koguma täiendavat teavet ja rakendama lisameetmeid. Eelkõige juhul, kui tehing on suure väärtusega, ebatavaline või kui kliendi riskiprofiil viitab kõrgemale rahapesu või terrorismi rahastamise riskile.

4.174. Täiendav teave on kliendi või juhuti tehtavas tehingus osaleva isiku püsiv tegevusala, maksetavade, olulisemate tehingupartnerite ja juriidilise isiku puhul ka kogemuse väljaselgitamine. Kohustatud isik peab vajadusel rakendama lisaks täiendavaid meetmeid ärisuhtest arusaamiseks, sealhulgas vajadusel tuvastama rikkuse päritolu või tehingus kasutatud vara päritolu.

4.175. Lisameetmeteks on muu hulgas avalikest allikatest teabe kogumine ja kontrollimine (näiteks Äriregister, ettevõtte koduleht, majandusaasta aruanded, meedikajastused jms).

Täiendavate hoolsusmeetmete rakendamine võib olla vajalik muu hulgas järgmistes olukordades:

- Tehingud ei ole kooskõlas kliendi teadaoleva tegevusega. Näiteks kliendi tavapärane majandustegevus ei ole loogiline planeeritavate või tehingute olemuse või mahu suhtes.

- Tehingud erinevad oluliselt kliendi tavapärasest tehingukäitumisest. Näiteks tehingute maht, sagedus või geograafiline ulatus erineb oluliselt kliendi varasemast tegevusest või kohustatud isikule teadaolevast tehingumustrist.

- Tehingud on seotud jurisdiktsioonidega, millega kliendil puudub ilmne majanduslik seos. Näiteks klient teeb tehinguid riikidega, kus kliendil ei ole teadaolevaid äripartnereid, tegevust või muid majanduslikke seoseid.

- Tehingu maht ei ole kooskõlas kliendi majandusliku profiiliga. Näiteks tehingute suurus või investeeritav summa ei ole vastavuses kliendi teadaoleva tegevusmahu või majandusaasta aruandes esitatud majandusnäitajatega.

- Tehingu majanduslik eesmärk ei ole kohustatud isikule arusaadav. Näiteks ei ole kliendi esitatud teabe põhjal tehingu eesmärk, sisu või piisavalt selge ning kliendi selgitused ei võimalda mõista tehingu tegelikku eesmärki. Eesmärk on ebamäärane, ühe- või üldsõnaline: ärikulud, investeering, äritegevuse laiendamine jmt.

- Kliendi taust või juhtimisstruktuur ei ole vastavuses kohustatud isikule esitatud informatsiooniga. Näiteks juriidilise isiku juhatusel või tegelikel kasusaajatel puudub seos või varasem kogemus ettevõtte deklareeritud tegevusalaga (taotletakse laenu spetsiifilise tegevusala jaoks, kuid puudub varasem kogemus ja seos selle valdkonnaga.

- Tehing või ärisuhe vastab teadaolevatele ja rahvusvaheliste organisatsioonide poolt avaldatud rahapesu või terrorismi rahastamise tüpoloogiatele või riskiskeemidele. Näiteks tasub teenuse eest kolmas isik, kellel puudub ilmne seos kliendi või tehinguga. Sel juhul peab kohustatud isik täiendavalt hindama, kas tegemist võib olla tegeliku kasusaaja varjamise või muu skeemiga, vajadusel täpsustama ärisuhte eesmärki ja osapoolte rolli.

4.176. Ärisuhte või juhuti tehtava tehingu eesmärgi ja olemuse tuvastamine on hoolsusmeetmete kõige olulisem põhimõte. Selle eesmärk on kujundada piisav arusaam kliendist, sealhulgas kliendi tegevusest, isikust, tegelikest kasusaajatest ja kliendiprofiilist, ning selgitada välja põhjus, miks klient soovib vastavat teenust tarbida. Kohustatud isik peab veenduma, et pakutav teenus vastab kliendi tegelikule tahteavalduse sisule, ehk miks ta teenust soovib, ning on kooskõlas konkreetse teenuse, lepingu olemuse ja eesmärkidega. Samuti peab teenuse kasutamine olema kooskõlas kliendile omistatud riskiastmega. Kogutud teave võimaldab kohustatud isikul hinnata kliendi tegevust kogu ärisuhte vältel ning teostada tehingute pidevat seiret, sealhulgas tuvastada tehingutes kasutatud vahendite päritolu ja majanduslikku põhjendatust. Samuti aitab kogutud teavet hinnata, kas klient, tema esindaja ja tegelik kasusaaja on riikliku taustaga isik, kas esitatud tegelik kasusaaja on reaalselt tegelik kasusaaja ning kas klient on võimeline sellise mahuga ja olulisemate äripartneritega selliseid tehinguid teostama.

4.177. Ärisuhte või juhuti tehtava tehingu eesmärgi ja olemuse tuvastamisel tuleb lisaks kliendi esitatud selgitustele hinnata, kas kliendi soovitud teenus ja kavandatav tegevus on kooskõlas kliendi tegeliku tegevuse, majandusliku profiili, võimekuse ja

vajadustega. Seetõttu ei saa ärisuhte eesmärgi ja olemuse tuvastamine piirduda üksnes sõnalise teabe kogumisega. Kliendi tegevusala, maksetavade, olulisemate tehingupartnerite (äripartnerite) ja kogemuse kohta kogutud teavet tuleb hinnata koostoimes. See tähendab, et tegevusala peab olema kooskõlas kliendi maksetavadega ning sellega, millises ulatuses ning mahus klient ärisuhte käigus tehinguid teeb. Samuti peavad kliendi olulisemad tehingupartnerid olema loogiliselt seotud vastava tegevusalaga ja kavandatavate tehingute mahuga. Lisaks tuleb silmas pidada, et kliendil peab olema vastav kogemus konkreetsel tegevusalal, võimekus teostada tehinguid selliste ärimahtudega ning omada vastavaid (äri)suhteid.

4.178. Ärisuhte või juhuti tehtava tehingu eesmärgi ja olemuse tuvastamise eesmärk on muu hulgas tuvastada riiklikus riskihinnangus ning muudes asjakohastes riskihinnangutes ja juhendites kirjeldatud riskidele viitavaid asjaolusid ning rakendada nende ilmnemisel asjakohaseid meetmeid. Sealjuures tuleb arvestada, et teatud tunnused võivad eraldiseisvalt või koos viidata muu hulgas nn riiulifirma kasutamisele või muule ebaharilikule tegevusele, mis ei ole kooskõlas tavapärase ja mõistliku majandustegevusega. Sellisel juhul peab kohustatud isik suutma põhjendada ärisuhte loomist ja jätkamist ning vajadusel tuleb selgitada pädevale järelevalveasutusele, millistele asjaoludele ja hinnangutele tuginedes on vastav ärisuhe loodud või seda jätkatud.

4.179. Sarnaselt teiste hoolsusmeetmetega tuleb ka ärisuhte või juhuti tehtava tehingu eesmärgi ja olemuse tuvastamisel lähtuda riskipõhisest lähenemisest. Mida kõrgem on kliendiga seotud risk, seda põhjalikumalt tuleb koguda ja hinnata teavet kliendi, tema tegevuse ja riskiprofiili kohta. Kohustatud isik peab veenduma, et tunne-oma-klienti põhimõte on täidetud ning on selgelt arusaadav, millist teenust klient soovib kasutada ja mis eesmärgil. Samuti tuleb hinnata, kas kliendi soovitud teenus on kooskõlas kliendi tegeliku tegevuse, majandusliku profiili, võimekuse ja vajadustega. Kõrgema riskiga olukordades ei ole piisav üksnes üldsõnaline teave.

4.180. **Tegevusala**

4.181. Kliendi tegevusala tuvastamiseks peab mõistma, millega klient tegelikult tegeleb ja millega kavatseb ärisuhte käigus tegeleda ning kuidas on see kooskõlas ärisuhte eesmärgi ja olemusega. Samuti tuleb hinnata, kas kliendi kirjeldatud tegevus on mõistlik, arusaadav ja usutav. Tegevusala tuvastamine ei tähenda üksnes registritesse esitatud andmete fikseerimist, vaid sisulise arusaama kujundamist sellest, millega klient tegeleb ning selle teabe dokumenteerimist ja säilitamist.

4.182. Kliendi määratud tegevusala täpsus peab vastama kliendi ärisuhte riskiprofiilile ja kliendi riskiastmele. Tavapärasemast kõrgema riskiga kliendi puhul ei tohi tegevusala majanduslikus mõttes olla liiga üldine või hõlmata omavahel mitteseotud tegevusvaldkondi, mis võimaldaks kliendil sisuliselt tegeleda mis tahes tegevusega ning raskendaks ärisuhte raames tehtavate tehingute asjakohast jälgimist.

4.183. Finantseerimisasutuste puhul tuleb tegevusala tuvastamisel välja selgitada ka see, kas kliendil on osutatava teenuse pakkumiseks vajalik tegevusluba. Samuti tuleb

hinnata, kas finantseerimisasutuse kaudu osutatakse teenuseid kliendi klientidele ehk lõplikult kasusaavatele isikutele, kelle suhtes peaks finantseerimisasutus kohaldama hoolsusmeetmeid, mis on kirjeldatud käesolevas juhendis lõplikult kasusaava isiku osas hoolsusmeetmete kohaldamata jätmise peatükis.

Näited kliendi tegevusala tuvastamisest:

- kui kliendi tegevusala on ehitusmaterjalide tootmine ja paigaldus, siis tema tehingud peavad kajastama reaalset ehitusprojekti või tellimust, mitte suures mahus finantstehinguid, mis ei ole seotud tavapärase tegevusega;

- kui klient tegutseb hulgimüügiga, peavad tehingute maht, sagedus ja tehingupartnerid olema kooskõlas hulgimüügi tavapärase äritegevusega. Ebatavaliselt suured või mitmed riigis toimuvad ühekordsed maksed vajaksid täiendavad selgitust või tõendite esitamist.

4.184. **Maksetavad**

4.185. Maksetavade hindamisel tuleb välja selgitada, kas ja millistel põhjustel ning tingimustel on klient planeeritud tehinguteks võimeline ning kuidas on see kooskõlas kohustatud isiku teadmisega ja tema ärisuhte riskiprofiiliga. Sellise hinnangu andmine eeldab vajadusel ka kliendi rikkuse päritolu või tehingutes kasutatava vara päritolu mõistmist.

4.186. Maksetavade hindamisel tuleb arvestada pakutava teenuse olemust ning kliendi riskiprofiili. Kõikide klientide ja teenuste puhul ei ole maksetavade üksikasjalik hindamine vajalik, kui selleks puudub kohustatud isiku hinnangul otsene vajadus ning võimalus. Otsese vajaduse all peetakse silmas eelkõige seda, et puuduvad pidevad maksed klientide poolt. Sellisel juhul võib kliendi võimekust vastavate tehingute tegemiseks hinnata muu hulgas kliendi varasema maksekäitumise põhjal, näiteks hinnates varasemalt toimunud makseid kliendi arvelduskontol, nende mahtu ja sagedust.

Näited maksetavade hindamise vajaduse ja asjaolude kohta:

- kui ärisuhe eeldab regulaarsete maksete tegemist (näiteks laenumaksed, teenustasud, igakuised renditasud jms), tuleb hinnata, kas kliendi sissetulekud ja majandustegevus võimaldavad selliste kohustuste täitmist;

- kui kliendi maksekäitumises esinevad olulised muudatused, näiteks suureneb järsult maksete maht, sagedus, tehingud toimuvad uutes jurisdiktsioonides ja uute isikutega, võib olla vajadus hinnata selliste muutuste põhjuseid.

4.187. **Olulisemad tehingupartnerid**

4.188. Olulisemate tehingupartnerite tuvastamisel tuleb välja selgitada, kellega kliendid deklareeritud tegevusalal tehinguid teevad või planeerivad teha ning milliste tegevusmahtudega tehinguid teostatakse. Ehk kes on need isikud, kelle kaudu realiseerub ärisuhte loomise majanduslik eesmärk.

4.189. Olulisemate tehingupartnerite all on mõistetakse isikuid, kes teevad võimalikuks sissetulevate ning väljaminevate tehingute teostamise. Seetõttu tuleb olulisemad tehingupartnerid tuvastada kahes eraldi kategoorias: isikud, kellelt laekuvad maksed kliendile ja isikud, kellele klient makseid teeb.

4.190. Mittefinantseerimisasutuste puhul ei pruugi olla võimalik tehingupartnereid tuvastada sama detailselt kui finantseerimisasutustes. Sellisel juhul võib teave olulisemate tehingupartnerite kohta tugineda kliendi selgitustele ning muudele kättesaadavatele andmetele, mida hinnatakse riskipõhiselt. Teave võib hõlmata muu hulgas kliendi kirjeldust peamistest klientidest või tarnijatest (vajadusel sektor, piirkond jms), teavet peamiste turgude või tegevuspiirkondade kohta ning hinnangulisi tehingumahtusid ja -suundi.

4.191. Asjakohasel juhul, eelkõige tavapärasemast kõrgema riski puhul, tuleb hinnata ka seda, kas tuvastatud tehingupartnerid on seotud kliendi deklareeritud tegevusalaga. Selleks võib kontrollida avalikult kättesaadavat teavet, mis kinnitab tehingupartneri tegutsemist vastavas valdkonnas.

4.192. Kui kliendi tegevus hõlmab kaupade ostu või müüki, võib oluliste tehingupartnerite kohta teabe kogumine hõlmata vajadusel (eelkõige kõrgema riski korral) ka kauba transporditeenuse osutajate või muude tehingu täitmisega seotud osapoolte andmete kogumist.

4.193. Eelkõige kõrgema riskiga kliendi puhul tuleb pöörata tähelepanu ka olulisemate tehingupartnerite asukohariikidele ning hinnata, kas need on kooskõlas kliendi varasemalt deklareeritud maksetavadega, sealhulgas riikidega, kust rahalised vahendid eeldatavalt laekuvad või kuhu need suunatakse.

4.194. Kuna tegemist on kliendi olulisemate tehingupartneritega, tuleb ärisuhte loomisel hinnata, kas on põhjendatud eeldada, et tehinguid nende isikutega ka reaalselt tehakse. Seda hinnatakse ja kontrollitakse ärisuhte kestel tehingute seire käigus.

4.195. Olulisemate tehingupartnerite kohta kogutud teavet tuleb arvesse võtta kliendi riskiprofiili hindamisel ning ärisuhte käigus tehtavate tehingute seirel.

Näited olulisemate tehingupartneritega seotud ohumärkidest:

- kliendi majandustegevus toimub peamiselt ühes riigis, kuid olulisemad tehingupartnerid asuvad riikides, millega kliendil puudub ilmne majanduslik seos;
- kliendi olulisemad tehingupartnerid on seotud kliendi juhtkonna, omanike või tegelike kasusaajatega ning selline seos ei ole majanduslikult põhjendatud;
- kliendi oluline tehingupartner on väike või hiljuti asutatud ettevõte, kuid tehingute maht on ebaproportsionaalselt suur;
- kliendi olulisemad tehingupartnerid asuvad *offshore*-jurisdiktsioonides või muudes kõrgema riskiga riikides ning puudub selge majanduslik põhjendus selliste partnerite kasutamiseks või teave on piiratud nende tegeliku majandustegevuse kohta.

4.196. **Finantseerimisasutuste erisus isikusamasuse (kaug)tuvastamisel**

4.197. Finantseerimisasutus peab enne kaugtuvastamise kasutamist kehtestama protseduurireeglid, mis võimaldab maandada kaugtuvastamisega seotud riske ning tagab kogutud andmete ja dokumentide õigsuse ja ajakohasuse. Protseduurireeglites tuleb kirjeldada kasutatavat tuvastamise vahendit või teenust ning vajadusel selle toimimist. Valitud lahendus peab koos teiste rakendatavate meetmetega tagama rahapesu ja terrorismi rahastamise riskide piisava maandamise.

4.198. Isikusamasuse tuvastamise käigus kogutud teabe kontrollimine peab toimuma isikuga samas kohas viibides (ehk näost-näkku) või infotehnoloogilise lahenduse abil (nt video teel tuvastamine), kui esineb vähemalt üks järgmistest asjaoludest:

4.198.1. tehingu või teenuse osutamise lepinguga seotud väljaminevate maksete kogusumma ületab ühes kalendrikuus 15 000 eurot füüsilise isiku puhul või 25 000 eurot juriidilise isiku puhul; või

4.198.2. kliendi elu- või asukoht on Euroopa Majanduspiirkonna välisest riigist.

4.199. Samas kohas viibimine tähendab, et klient või tema esindaja ja finantseerimisasutuse esindaja viibivad eesmärgipärasel kohtumisel samas kohas. See tähendab, et potentsiaalsel kliendil või tema esindajal on finantseerimisasutuse esindajaga vahetu kontakt, mille käigus finantseerimisasutuse esindaja veendub isikusamasuse tuvastamise nõuete täitmises, võrreldes isiku biomeetriat (näokujutist) nõuetekohasel dokumendil oleva või sellelt dokumendilt saadud näokujutisega. Vahetu kontakt eeldab finantseerimisasutuse esindaja otsest suhtlemist kliendi või tema esindajaga, et hinnata tema tahteavalduse sisu ja eesmärgi vastavust tegelikule tahtele. Vahetu kontakti käigus kogetu põhjal on võimalik täpsemalt määrata ka kliendi riskiprofiil. Kontakt võib toimuda ka väljaspool finantseerimisasutuse püsivat tegevuskohta, tingimusel, et selle käigus täidetakse vähemalt samu hoolsusmeetmeid kui tavapärastel juhtudel.

4.200. Kaugtuvastamisel täidab finantseerimisasutus RahaPTS-i §-s 31 sätestatud nõudeid ning arvestab pädeva järelevalveasutuse ja Euroopa Pangandusjärelevalve Asutuse asjakohastes juhendites ja suunistes sätestatuga.

4.201. Kaugtuvastamisel tuleb kasutada usaldusväärset elektroonilise tuvastamise süsteemi või teenust, näiteks eIDAS määruse nõuetele vastavat e-identimise vahendit või kvalifitseeritud usaldusteenust. Kaugtuvastamise käigus kogutud kujutise-, heli- ja muud andmed peavad olema piisava kvaliteediga, et võimaldada isiku üheselt tuvastamist, ning need tuleb säilitada vastavalt kehtivatele nõuetele. Tehniliste probleemide või ühenduse katkemisel loetakse isikusamasuse tuvastamine ebaõnnestunuks.

4.202. Kaugtuvastuse eesmärgiks on muu hulgas võrrelda sessiooni käigus saadud isiku biomeetriat (näokujutist) dokumendil oleva või sellelt dokumendilt saadud näokujutisega.

4.203. Rahapesu Andmebüroo on avaldanud isikusamasuse kaugtuvastamise märgukirja.

4.204. **Lõplikult kasusaava isiku osas hoolsusmeetmete kohaldamata jätmine korrespondentsuhetes finantseerimisasutuste puhul**

4.205. Korrespondentsuhteks peetakse finantseerimisasutuste vahelist ärisuhet, mille raames üks finantseerimisasutus (korrespondentasutus) osutab teisele finantseerimisasutusele (respondentasutus) finantsteenuseid, võimaldades viimasel teha tehinguid oma klientide nimel või kasuks. Sellises suhtes on oluline arvestada, et teenusest võivad kasu saada respondentasutuse kliendid (lõplikult kasusaavad kliendid), kelle riskiprofiil võib mõjutada kogu ärisuhte riski.

4.206. Juhul, kui finantseerimisasutus pakub teisele krediidi- või finantseerimisasutusele teenuseid korrespondentsuhte raames, kus teenusest saavad kasu teenust saava krediidi- või finantseerimisasutuse kliendid (edaspidi lõplikult kasusaav klient), ei pea finantseerimisasutus kohaldama lõplikult kasusaava isiku osas hoolsusmeetmeid RahaPTS-i ja selle juhendi mõttes, kui kõik järgmised tingimused on täietud samaaegselt:

4.206.1. kliendiks olev finantseerimisasutus on finantsjärelevalve all ja rakendab tegelikkuses RahaPTS-is sätestatud nõuetega võrdväärseid hoolsusmeetmeid, sealhulgas hoolsusmeetmete kohaldamise, riikliku taustaga isiku tuvastamise ja andmete säilitamise nõudeid;

4.206.2. finantseerimisasutus hindab ja dokumenteerib lõplikult kasusaavate klientide riskistruktuuri (sealhulgas klientide geograafiline asukoht, kõrge riskiga klientide osakaal ja tegevusalad) ning tagab, et korrespondentsuhtega kaasnev risk on kooskõlas finantseerimisasutuse enda riskiisuga;

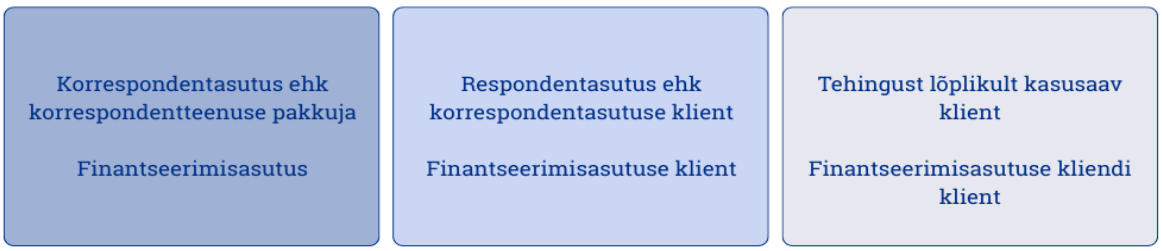
4.206.3. lepinguga on tagatud kohustuslik juurdepääs andmetele ja dokumentidele, mis võimaldavad vajadusel viivitamata tuvastada lõplikult kasusaava isiku.

4.207. Kui ülaltoodud tingimused ei ole täidetud või korrespondentasutus on asutatud suure riskiga kolmandas riigis, kohaldab finantseerimisasutus (korrespondentasutus) lõplikult kasusaavate klientide suhtes ise kõiki RahaPTS-i § 20 lg 1 hoolsusmeetmeid.

4.208. Finantseerimisasutus dokumenteerib korrespondentsuhete riskihinnangu ja rakendatud meetmed, sealhulgas hinnangu lõplikult kasusaavate klientide riskidele, kogutud andmete ulatuse ja allikad.

4.209. RahaPTS-i ja käesoleva juhendi nõuete täitmise eest vastutab alati korrespondentasutus, sõltumata sellest, kas hoolsusmeetmeid kohaldab tema või teenust saav finantseerimisasutus.

Korrespondentsuhte osapooled:



4.210. Korrespondentsuhtega kaasnevad kõrgendatud rahapesu ja terrorismi rahastamise riskid, kuna:

4.210.1. korrespondentasutusel puudub üldjuhul otsene ärisuhe tehingust lõplikult kasusaavate klientidega ning piiratud on info nende isikute, tehingute eesmärgi ja majandusliku sisu kohta, mis raskendab kahtlaste tehingute tuvastamist;

4.210.2. korrespondentasutus ei kohalda tavapäraselt lõplikult kasusaavate klientide suhtes vahetult hoolsusmeetmeid, vaid tugineb respondentasutuse rakendatavatele meetmetele, mille piisavus ja tõhusus ei pruugi olla tagatud;

4.210.3. tegelike kasusaajate ning tehingutes kasutatavate vahendite allika ja päritolu tuvastamine on keerukam, kuna tehinguahelas on täiendav osapool, mis vähendab tehingute läbipaistvust;

4.210.4. tehingud võivad toimuda mitme jurisdiktsiooni ja osapoole kaudu, mis raskendab järelevalvet ning suurendab regulatiivsete nõuete eiramise riski;

4.210.5. korrespondentsuhte kaudu võib suureneda risk, et teenuseid kasutatakse kaudselt kõrge riskiga klientide või tegevuste teenindamiseks, ilma et korrespondentasutus omaks nende üle piisavat kontrolli.

Näited olukordadest, kus võib tekkida korrespondentsuhe:

- valuutavahetaja osutab valuutavahetusteenust teisele valuutavahetajale, kes omakorda teenindab oma kliente;
- laenuandja kliendiks on teine finantseerimisasutus (näiteks teine laenuandja), kes vahendab teenuseid või laene lõppklientidele;
- finantseerimisasutus kasutab teist finantseerimisasutust maksete vahendamiseks (nt rahvusvahelised ülekanded), kus tehingu lõplik kasusaaja on esimese asutuse klient.

4.211. **Hoolsusmeetmed ärisuhte kestel**

4.212. **Rakendatavad hoolsusmeetmed ärisuhte seirel ja kestel**

4.213. Ärisuhte kestel ja seirel rakendatakse järgmiseid hoolsusmeetmeid:

4.213.1. ärisuhtes tehtud tehingute kontroll, tagamaks, et need on kooskõlas olemasolevate teadmistega kliendist, tema (äri)tegevusest ja riskiprofiilist (juhendi punktid 4.232., 4.242. ja 4.250);

4.213.2. hoolsusmeetmete rakendamisel kogutud dokumentide, andmete või muu teabe regulaarne ajakohastamine (juhendi punkt 4.216.);

4.213.3. tehingus kasutatud vahendite allika ja päritolu tuvastamine (juhendi punkt 4.253.);

4.213.4. suurema tähelepanu pööramine ärisuhtes tehtavatele tehingutele, kliendi tegevusele ja asjaoludele, mis võivad viidata kuritegevusele, rahapesule või terrorismi rahastamisele, sealhulgas:

4.213.4.1. keerukatele, suure väärtusega ja ebatavalistele tehingutele;

4.213.4.2. tehingumustritele, millel puudub mõistlik või nähtav majanduslik või õiguspärane eesmärk;

4.213.4.3. tehingutele, mis ei ole konkreetsele ärispetsiifikale iseloomulik[32];

4.213.5. suurema tähelepanu pööramine ärisuhtele või tehingule, kui klient:

4.213.5.1. on pärit suure riskiga kolmandast riigist või RahaPTS § 37 lõikes 4 nimetatud riigist või territooriumilt; või

4.213.5.2. omab nimetatud riigi kodakondsust, elu- või asukohta; või

4.213.5.3. makse saaja makseteenuse pakkuja asukoht on nimetatud riigis või territooriumil.

4.214. Ärisuhte seire käigus rakendatavate hoolsusmeetmete eesmärk on hinnata ja tagada, et ärisuhte käigus tehtavad tehingud ja kliendi (äri)tegevus vastab ärisuhte loomisel kogutud teabele ja tunne-oma-klienti põhimõttele. Selline hindamine võimaldab mõista, millistel eesmärkidel ja millistes majandus- või õigussuhete raames teeb klient tehinguid ärisuhte kestel või saab rahalisi vahendeid. Samuti peab kohustatud isik veenduma, et kliendi tegevus ja asjaolud ei viita rahapesule, terrorismi rahastamisele ega muudele ebatavalistele tehingutele.

4.215. Kohustatud isik peab kohaldama kõiki hoolsusmeetmeid ja ei tohi jätta kohaldamata ühtegi hoolsusmeedet üheski etapis. Hoolsusmeetmete rakendamise ulatuse võib valida lähtuvalt kliendi ning kliendi ja kohustatud isiku vahelise ärisuhtega kaasnevast riskist. See tähendab, et hoolsusmeetmeid kohaldatakse riskipõhiselt ning lähtutakse äristrateegiale sobivatest põhimõtetest. Seejuures rakendatakse hoolsusmeetmeid ulatuses, mis vastab eelnevale riskihinnangule. Kui kliendi või tehingus osaleva isikuga seotud risk on madal, võib rakendada hoolsusmeetmeid lihtsustatud korras, kuid hoolsusmeetmeid ei tohi jätta täielikult rakendamata. Kui kliendi või tehingus osaleva isikuga seotud risk on tavapärasest kõrgem, tuleb kohaldada hoolsusmeetmeid suuremas ulatuses ehk tugevdatud korras.

4.216. **Andmete uuendamine**

4.217. Kohustatud isik tagab hoolsusmeetmete kohaldamise käigus kogutud dokumentide, andmete ja teabe regulaarse ning sündmuspõhise ajakohastamise. Eelkõige hõlmab see kliendi, tema esindaja (sealhulgas esindusõiguse) ja tegeliku kasusaaja ning ärisuhte eesmärki ja olemust selgitavate andmete ajakohastamist.

4.218. Tavapärasest kõrgema riskiga klientide ja ärisuhete puhul tuleb olemasolevaid andmeid kontrollida ja ajakohastada sagedamini kui madalama riskiga klientide puhul. Üldjuhul ajakohastatakse tavapärasest kõrgema riskiga klientide ja ärisuhete andmeid vähemalt kord aastas, kui riskihinnangust ei tulene vajadust sagedasemaks kontrolliks.

[32] Selle kohustuse täitmisel tuleb muu hulgas välja selgitada nende tehingute olemus, põhjus ja taust, samuti muu teave tehingute sisu mõistmiseks, ning pöörata nendele tehingutele suuremat tähelepanu.

4.219. Lisaks tuleb kõrgema riskiga kliendi riskiprofiil esmakordselt üle vaadata hiljemalt kuue kuu jooksul pärast ärisuhte loomist, et hinnata, kas kliendile esialgselt omistatud riskiaste on jätkuvalt asjakohane.

4.220. Andmete ajakohastamise viisi ja ulatuse määrab kohustatud isik ise, lähtudes kliendi ja ärisuhte riskiastmest ning võimalusest kasutada otseseid või kaudseid meetodeid viisil, mis ei häiri põhjendamatult kliendisuhte tavapärast toimimist.

4.221. Muu hulgas võib andmeid uuendada küsides kliendilt täiendavat teavet või dokumente (näiteks isikut tõendavat dokumenti, esindusõigust tõendavaid dokumente või teavet tegevusala kohta), avalike registrite ja andmebaaside kontrollimise kaudu (nt äriregister) ning kliendi varasema käitumise ja tehingute analüüsi põhjal ärisuhte seire käigus.

Näited andmete uuendamise vajadusest:

- kui kliendi juhatuse koosseis muutub, tuleb kontrollida uute juhatuse liikmete andmeid ja esindusõigust;
- kui kliendi tehingumustrid muutuvad oluliselt, võib olla vajalik ajakohastada teavet kliendi tegevusala või ärisuhte eesmärgi kohta;
- kõrgema riskiga kliendi puhul võib andmete ajakohastamine hõlmata regulaarset kontrolli nii kliendilt saadud teabe kui ka avalike allikate põhjal;
- kui kliendi tuvastamiseks või andmete kontrollimiseks kasutatud dokumendi kehtivusaeg lõppeb või tekib kahtlus selle kehtivuses, tuleb ajakohastada vastavad andmed ning vajadusel koguda kliendilt uue kehtiva dokumendi andmed.

4.222. **Ärisuhte seire**

4.223. Ärisuhet seiratakse pidevalt, mis hõlmab ärisuhtes tehtud tehingute jälgimist ja kontrolli, tagamaks, et tehingud on kooskõlas teadmistega kliendist, tema (äri)tegevusest ja riskiprofiilist. Ärisuhte seire hõlmab kogu ärisuhte elutsüklit, sealhulgas sissetulevaid ja väljaminevaid tehinguid, millele kehtib nõue tuvastada tehingus kasutatud vahendite allikas ja päritolu.

4.224. Ärisuhte seire käigus tuleb hinnata, kas kliendi tehingud vastavad kliendi kohta eelnevalt teadaolevale informatsioonile, sealhulgas ärisuhte loomisel deklareeritud eesmärgile, tegevusalale ja tehingumahule. Samuti tuleb tuvastada tehingud ja tegevused, mis võivad viidata kuritegelikule tegevusele, rahapesule või terrorismi rahastamisele, sealhulgas ebatavalised, keerukad või suure väärtusega tehingud ja tehingumustrid, millel puudub mõistlik majanduslik või õiguspärane eesmärk.

4.225. Ärisuhte seire käigus hinnatakse regulaarselt ka kliendi riskiprofiili, mis tuleb üle vaadata tervikuna, arvestades nii kliendiga kui ka tehingutega seonduvaid riske. Samuti tuleb pidevalt hinnata kliendi tegevuse muutumist, mis võib tõsta kliendi ja ärisuhtega kaasnevat riskiastet ning tuua kaasa vajaduse kohaldada täiendavaid või tugevdatud hoolsusmeetmeid.

4.226. Seire käigus tuleb hinnata ka üksikute tehingute eesmärki ja olemust ning nende vastavust kliendi profiilile. Selleks kogutakse vajadusel täiendavaid andmeid ja dokumente, et mõista tehingu majanduslikku sisu, selle tegemise põhjust ning tehingu seost kliendi tegevuse ja riskiprofiiliga, võimaldades hinnata selle vastavust kliendi kohta eelnevalt teadaolevale informatsioonile.

4.227. Ärisuhte seire teostamisel lähtutakse riskipõhisest lähenemisest. Mida suurem on kliendiga kaasnev risk, seda ulatuslikum ja põhjalikum peab olema seire ning kogutav informatsioon ei tohi piirduda üldsõnalise teabega.

4.228. Kui ärisuhte seire käigus kogutud andmed on ebapiisavad, vastuolulised või nende usaldusväärsuses on põhjust kahelda, tuleb rakendada täiendavaid hoolsusmeetmeid, sealhulgas vajadusel koguda täiendavat teavet või kohaldada hoolsusmeetmeid uuesti.

4.229. Tehingute jälgimise meetmed jagunevad kaheks: reaalajas teostatav kontroll ja jälgimine (skriinimine) ja järelkontroll (monitoorimine).

4.229.1. Reaalajas teostatav kontroll tähendab tehingute kontrollimist nende tegemise hetkel eelnevalt määratud tunnuste, parameetrite või riskikriteeriumite alusel. Selleks võib kasutada infotehnoloogilisi lahendusi, teostada manuaalset kontrolli või kasutada nende kombineeritud versiooni. Reaalajas tehingute kontrollimise eesmärk on tuvastada viivitamata tehingud, mis võivad olla seotud sanktsioonide rikkumise, rahapesu või terrorismi rahastamise riskiga, ning vajadusel takistada selliste tehingute teostamist. Mittefinantseerimisasutuste vaatest kontrollitakse reaalajas eelkõige klienti, tehingut või dokumentatsiooni teenuse osutamise käigus enne toimingu või tehingu tegemist, näiteks hinnatakse kliendi tausta, kontrollitakse tegeliku kasusaaja andmeid jne.

4.229.2. Järelkontroll tähendab tehingute hilisemat analüüsi, mille käigus hinnatakse tehingute mustreid, mahtusid ja sagedust ning nende vastavust kliendi profiilile, tegevusalale ja varasemalt hinnatud riskile, sealhulgas hinnatakse, kas need on kooskõlas kliendi kohta eelnevalt teadaoleva informatsiooniga. Järelkontrolli eesmärk on tuvastada ebatavalisi või kahtlaseid tehinguid ja tehingumustreid, mis ei pruugi olla üksiktehingu tasandil tuvastatavad.

4.230. Ärisuhte seire eesmärk on muu hulgas tuvastada riskidele viitavaid asjaolusid, mis on kirjeldatud riiklikus riskihinnangus ja muudes juhendites. Mitme riskitunnuse koosmõju või ka üksikud tunnused võivad viidata kahtlasele või ebaharilikule majandustegevusele (näiteks riiulifirma kasutamine), mille puhul peab kohustatud isik suutma põhjendada ärisuhte loomist ja jätkamist.

4.231. Ärisuhte seire teostamine tuleb dokumenteerida viisil, mis võimaldab hiljem tuvastada seire tegemise aja, ulatuse ja tulemused.

Näited ja ohumärgid ärisuhte seire puhul:

- kliendi tehingud ei vasta deklareeritud tegevusalale või tehingumahule, näiteks esineb mitmeid suure väärtusega makseid, mis ei ole kohane tavapärasele äritegevusele;

- klient teostab ülekandeid kõrge riskiga või tema äritegevusega mitteseotud jurisdiktsioonidesse, millega kliendil puudub majanduslik seos;

- klient soovib ärisuhte käigus kasutada teenuseid, mis ei olnud ärisuhte loomisel ärisuhte eesmärgi osa. Näiteks CSP klient soovib ärisuhte loomisel kontaktaadressi teenust ning lühikese aja jooksul peale ärisuhte loomist, soovitakse ka äriühingu asutamise teenust. Sellisel juhul tuleks kaaluda, kas esineb suuremat riski iseloomustavaid asjaolusid (nt loodava äriühingu asukoht on seotud suure riskiga riigiga, struktuur on ebaselge, arvet soovitakse kolmanda isiku nimele vms);

- esinevad ebatavalised või keerukad tehingumustrid. Näiteks saab klient raha ja kannab selle kohe tagasi samale saatjale või kolmandale isikule, ilma nähtava majandusliku põhjenduseta, või klient kannab raha oma ettevõtte kontolt teise riigi kontole, sealt kolmandasse ettevõttesse ja lõpuks kasutatakse summa väikestes osades eri teenuste eest maksmiseks, ilma et sellel oleks majanduslik põhjendus;

- klient teostab tehinguid läbi ettevõtete, millel tegelikult puudub majandustegevus, töötajad või reaalne kontor ning mis ei osale kliendi põhitegevuses. Näiteks klient kannab suuri summasid *offshore*-ettevõtte kontole, kuid see ettevõte ei müü ega osta tegelikke kaupu ega teenuseid ning puuduvad arved või tehingud, mis põhjendaksid raha liikumist ning sel viisil on võimalik varjata raha tegelikku päritolu või lõplikku kasusaajat.

4.232. **Reaalajas jälgimine**

4.233. Ärisuhte reaalajas jälgimise eesmärgiks on tuvastada kahtlaseid ja ebaharilikke tehinguid ning tehingumustreid, etteantud piirmäärasid ületavaid tehinguid, riikliku taustaga isikuid, sanktsioneeritud isikuid, negatiivset meediainfot vms informatsiooni, mis on oluline kliendi kohta ning mis võib mõjutada riskipõhist lähenemist tema suhtes.

4.234. Keerukate, suure väärtusega ja ebatavaliste tehingute ja tehingumustrite jälgimine on oluline osa kõikidest rakendatavatest hoolsusmeetmetest. Sellistel tehingutel ei pruugi olla mõistlikku või nähtavat majanduslikku ega õiguspärast eesmärki või need pole konkreetsele ärispetsiifikale iseloomulikud. Jälgimine võimaldab klientide majandustegevuses tuvastada asjaolusid, mis võivad viidata rahapesule või terrorismi rahastamisele. Ärisuhete jälgimine ülaltoodud eesmärkidel omab samuti rolli, et tuvastada riikliku taustaga isikuid.

4.235. Ärisuhte ja tehingute reaalajas jälgimiseks kasutatavad meetmed peavad olema riskipõhised ehk vastama kohustatud isiku suurusele ning tema tegevuse ja teenuste olemusele, ulatusele, keerukusastmele, sealhulgas riskiisule ja tegevusega kaasnevatele riskidele.

Mida suurem on kliendibaas ning risk, et teenuste kaudu võidakse kuritegelikul teel saadud rahalisi vahendeid legaliseerida (ehk pesta) ja terrorismi rahastada, seda rohkem või seda ulatuslikumaid meetmeid tuleb rakendad. Näiteks, kui tehingute ja klientide maht on nii

suur, et sellise info manuaalne reaalajas jälgimine ei ole tõhus, siis tuleks kasutata täisautomaatseid või poolautomaatseid süsteeme.

4.236. Kohustatud isik võib proportsionaalsuse põhimõttest lähtudes kasutada reaalajas tehingute jälgimiseks ja klientide kontrollimiseks:

4.236.1. automaatseid IT-süsteeme;

4.236.2. manuaalset kontrolli;

4.236.3. nende kahe meetodi kombineeritud versiooni.

4.237. Kui kasutatakse manuaalset kontrolli, peab see tagama vähemalt samaväärse kontrollitaseme kui automaatsed süsteemid ning hõlmama käesolevas juhendis kirjeldatud riskistsenaariume (punktis 4.240.).

4.238. Kohustatud isik peab olema valmis pädevale järelevalveasutusele põhjendama, miks valiti konkreetne reaalajas kontrollimise ja jälgimise lahendus ning miks see on tema tegevuse ja riskide seisukohast sobiv.

4.239. Kui ärisuhte reaalajas jälgimiseks kasutatakse automaatseid süsteeme konkreetsete ärisuhete raames tehtavate kahtlaste ja ebaharilike tehingute tuvastamiseks, siis tuleb samuti tagada, et need süsteemid on eesmärgipärased ja proportsionaalsed.

4.240. Ärisuhte reaalajas jälgimise eesmärgiks on tuvastada kahtlaseid ja ebaharilikke tehinguid ning tehingumustreid, etteantud piirmäärasid ületavaid tehinguid või riikliku taustaga isikuid või sanktsioneeritud isikuid. Sellest tulenevalt peavad automaatsed IT-süsteemi parameetrid/stsenaariumid vastama proportsionaalsuse põhimõttele ning arvestama ka kohustatud isiku riskihinnangut. Parameetrid/stsenaariumid peavad muu hulgas:

4.240.1. hõlmama kahtlaste ja ebaharilike tehingute (ning võimalusel tehingumustrite) tuvastamiseks riske ja ohte, millega oma tegevuses eelkõige kokku puututakse (näiteks ebaharilikult suured tehingud, sagedased väiksed tehingud, kiire tehingute tegemine, tehingu majandusliku eesmärgi ebaselgus, keerukad omandi- ja tehingustruktuurid, kolmandate isikute kaasamine ilma selge põhjuseta);

4.240.2. võimaldama tuvastada tehinguid, mis teostatakse, edastatakse või laekuvad riikidest, millel on kõrge rahapesu või terrorismi rahastamise risk, sealhulgas konfliktipiirkondadest, ning vajadusel ka nende riikidega seotud riikidest ja naaberriikidest, kui see on põhjendatud kohustatud isiku riskihinnangu ja täiendavate riskitegurite alusel;

4.240.3. katma ka tehingute kirjeldusi ja selles olevat informatsiooni, sealhulgas ka seda kas arvete eest tasub klient või keegi kolmas;

4.240.4. kontrollima nii kliendi, tema esindaja kui ka tegeliku kasusaaja andmete vastavust;

4.240.5. peavad võimaldama tuvastada riikliku taustaga isikuid, kontrollides nii kliendi, tema esindaja kui ka tegeliku kasusaaja andmete vastavust;

4.240.6. tagama isikute tuvastamise (hõlmab isikut ennast, tema esindajat ja tegelikku kasusaajat), kelle osas on eelnev kahtlus või kellega on ärisuhte loomisest keeldutud või ärisuhe erakorraliselt üles öeldud (sealhulgas juhul, kui see on tehniliselt võimalik ja ei ole liiga koormav, võimalusel kontrollida kasutatud IP-aadresse). Eesmärgiks on, et rakendataks kohaseid meetmeid, kui samad isikud soovivad luua uuesti ärisuhet;

4.240.7. tagama võimalused, et suudetakse tuvastada varjatud või nähtavad (äri)sidemed erinevate klientide vahel (nn ühte gruppi kuuluvus, sama tegelik kasusaaja, samad sidevahendite andmed, samad IP-aadressid jne).

4.241. Kehtestatud parameetreid/stsenaariume tuleb ka regulaarselt üle hinnata, et veenduda, kas need parameetrid/stsenaariumid on veel vastavuses kohustatud isiku tegevuse, suuruse ja riskidega.

4.242. **Järelkontroll**

4.243. Tehingute järelkontrolli käigus analüüsitakse tehinguid, mis on eelnevalt määratud parameetrite alusel tehingute kogumist eraldatud. Tehingute järelkontrollimise viisid ja ulatus tuleb kehtestada vastavalt ettevõtte teenustega kaasnevatele riskidele.

4.244. Kui reaalajas jälgimine aitab muu hulgas tuvastada ilmsemaid riske ja kõrvalekaldeid, siis tagantjärgi tehingute jälgimine võimaldab analüüsida kliendi tehinguid terviklikult ajas. See võimaldab kohustatud isikul kujundada ja pidevalt ajakohastada kliendiprofiili, lähtudes tema ajaloolisest tegevusest. Näiteks, kui kliendi hoiuste maht järsult suureneb, peaks kohustatud isik kindlaks tegema tehingute eesmärgi ja sissetulevate vahendite allika ning tagama, et sellisele kasvule on olemas majanduslikult mõistlik selgitus.

4.245. Tehingute järelkontrolli käigus jälgivad töötajad klientide käitumist ja tehinguid, et tuvastada asjaolud, mida ei olnud võimalik reaalajas hinnata. See hõlmab muu hulgas juhtumeid, mis tehingu iseloomu tõttu ei kajastunud reaalajas jälgimise parameetrites või manuaalse jälgimise käigus (nt suuremahulised tehingud summade, valuutade või klienditüüpide lõikes).

4.246. Alljärgnevalt on lisatud näiteid mõnedest tüüpilisematest parameetritest, mille alusel võib tehinguid järelkontrollida:

4.246.1. vaadeldava perioodi suurema käibega (nii füüsilised kui juriidilised) kliendid, teenuse kasutajad, fondiosakute ostjad jne (nii füüsilised kui juriidilised isikud);

4.246.2. vaadeldava perioodi (nii füüsilised kui juriidilised isikud) suuremad tehingud (nii füüsiliste kui juriidiliste isikute) valuutade ja teenuste kaupa;

4.246.3. vaadeldava perioodi jooksul teatud piirmäära ületavad tehingud;

4.246.4. teatud piirmäära ületavad sularahatehingud (nii füüsiliste kui juriidiliste isikute lõikes) jne.

Näited järelkontrolli stsenaariumitest:

- tehingud riikidega, mis on rahapesu või terrorismi rahastamise seisukohalt kõrgema riskiga;
- sularaha tehingud;
- struktureeritud tehingud;
- kliendi tehingute maht;
- tehingud, mis ei ole kooskõlas kliendi tavapärase majandustegevuse või varasema tehingukäitumisega;
- mitme kliendi vahelised korduvad tehingud, mis võivad viidata omavahel seotud isikutele või ettevõtetele;
- tehingud, mille puhul toimub raha kiire edasikandmine mitmele kontole või mitme vahendaja kaudu;
- tehingud, mille puhul kasutatakse ebatavalisi makseselgitusi või puudub tehingu majanduslik sisu.

4.247. Tehingute järelkontroll erinevate kriteeriumite järgi, võimaldab kohustatud isikutel saada terviklikku ülevaadet oma klientide tehingumustritest ning hõlbustab ebatavaliste ja kahtlaste tehingute avastamist, sest kohustatud isikul on teadmine, milline on tavapärane tegevus tema kliendibaasis ning milline on sellest hälbiv käitumine. Tehingute järgne järelkontroll võimaldab muuta ka reaalajas toimuvat kontrolli sihipärasemaks ehk kohustatud isik saab keskenduda tehingute reaalajas kontrollimisel kõrgema riskiga asjaoludele.

4.248. Kohustatud isik peab lisaks kliendipõhisele järelkontrollile vajadusel analüüsima ka oma kliendibaasi tervikuna, et tuvastada riskimustreid, trende ja süsteemseid kõrvalekaldeid. Selline analüüs võimaldab hinnata, kas kohustatud isiku riskihinnang on ajakohane ning kas rakendatavad hoolsusmeetmed on piisavad.

4.249. Järelkontrolli reegleid ja parameetreid tuleb regulaarselt uuendada ja kohandada vastavalt kohustatud isiku tegevusele.

Kogu kliendibaasi analüüsimisel on võimalik tuvastada näiteks:

- kõrge riskiga klientide osakaal (kas tõusnud või langenud, kas vastab riskiisule);
- teatud riikidega seotud klientide või tehingute kasv (kas riskiriikide osakaal on suurenenud, kas on vastavuses riskiisuga);
- sagedased sarnased kahtlased mustrid erinevate klientide lõikes;
- korduvad probleemid (nt sama tüüpi kahtlased tehingud).

4.250. **Reaalajas tehingute ja klientide kontrollimine ja järelkontroll mittefinantssektoris**

4.251. Mittefinantssektori kohustatud isikud (nt kinnisvaramaaklerid, raamatupidamisteenuse pakkujad ja äriühingute teenuse pakkujad jne) ei pruugi jälgida

tehinguid samas mahus või sama automatiseeritult kui finantseerimisasutused. Sellest hoolimata peavad nad riskipõhiselt:

4.251.1. jälgima kliendi tegevust ja tehinguid ulatuses, mis on seotud nende poolt osutatava teenusega;

4.251.2. hindama, kas tehingud või toimingud on kooskõlas kliendi teadaoleva tegevuse, profiili ja ärieesmärgiga;

4.251.3. tuvastama ebaharilikke või kahtlaseid asjaolusid nii üksiktehingute kui ka ärisuhte käigus tervikuna;

4.251.4. vajadusel koguma täiendavat teavet tehingu eesmärgi ja rahaliste vahendite päritolu kohta;

4.251.5. teostama kliendibaasi ja ärisuhete perioodilist järelkontrolli riskipõhiselt.

4.252. Kohustatud isik, kelle kliendibaas on väike, ei pea kasutama keerukaid IT-süsteeme, kuigi automatiseeritud lahendused on efektiivsemad ja tõhusamad. Kui IT-süsteeme ei kasutada siis peab kohustatud isiku suutma selgitada:

4.252.1. kuidas ta oma töös kahtlasi olukordi tuvastab;

4.252.2. millistele riskitunnustele ja asjaoludele ta tähelepanu pöörab;

4.252.3. kuidas ta dokumenteerib tehtud kontrollid, hinnangud ja järeldused;

4.252.4. kuidas on tagatud piisav töökorraldus ja ressurss nõuete täitmiseks.

4.253. **Tehingus kasutatud vahendite allika ja päritolu tuvastamine**

4.254. Ärisuhte seire käigus peab kohustatud isik tuvastama kõikide tehingute vahendite allika ja päritolu, tagamaks, et tehingud on kooskõlas kliendi äriprofiili, tegevusala ja riskihinnanguga.

4.255. Tehingus kasutatud vahendite allika ja päritolu kontroll on ärisuhte seire osa, kuid keskendub peamiselt sissetulevatele tehingutele.

4.256. Kohustatud isik hindab ja dokumenteerib tehingutes kasutatavate rahaliste vahendite ja muu vara päritolu, sealhulgas nende liikumise kliendini ning tehingute kaudu, mis hõlmavad kolmandate osapoolte kontosid või kui teenuste eest tasub kolmas isik. Muu vara tähendab lisaks sularahale ja pangamaksetele kõiki tehinguvahendeid, mille kaudu väärtust kantakse või tehinguid sooritatakse, näiteks virtuaalvääringud, väärtpaberid, kuld ja muud väärismetallid, kalliskivid, kunstiesemed, luksuskaupade objektid jmt.

4.257. Seire käigus tuleb tuvastada ebatavalised, keerukad või mitmekihilised tehingud, samuti raha liikumine läbi ettevõtete, millel puudub tegelik majandustegevus või mis ei kajastu kliendi põhitegevuses.

4.258. Vajadusel tuleb, eelkõige kui kogutud andmed on ebapiisavad või vastuolulised, rakendada täiendavaid meetmeid, sealhulgas koguda täiendavaid dokumente või tõendeid, et selgitada tehingu allikat, majanduslikku eesmärki ja seost kliendi tegevuse ning riskiprofiiliga.

4.259. Kõik tuvastatud andmed ja hinnangud tuleb dokumenteerida viisil, mis võimaldab hiljem tuvastada kontrolli tegemise aja, ulatuse ja tulemused.

Kohustatud isik peab hindama iga tehingu konteksti ning vajadusel koguma ka muid tõendeid või dokumente, mis kinnitavad tehingus kasutatud vahendite allikat ja päritolu.

Näidisloetelu dokumentidest ja tõenditest, mida hinnata tehingus kasutatud vahendite allika ja päritolu tuvastamiseks:

- pangadokumendid, näiteks arvelduskonto väljavõtted, maksekorraldused, maksesüsteemide väljavõtted;
- lepingud ja arved, näiteks kaupade või teenuste ostu-müügilepingud, teenuse osutamise arved, töölepingud, mis selgitavad tehingu majanduslikku eesmärki;
- kui vahendid liiguvad läbi kolmanda osapoole kontode, siis selle osapoole isiku või ettevõtte andmed, juhatuse andmed, konto kasutamise põhjendused;
- virtuaalvääringute puhul rahakoti aadressid, tehingute logid, tehingu räsi jne;
- registreeritud ettevõtete andmed, sealhulgas äriregistri väljavõtted, tegevusload ja nende olemasolu kinnitavad tõendid;
- täiendavad analüüsid, näiteks majandusaasta aruannete või muude andmete analüüs, kus on finantsvõimekuse, -mustrite ja riskiprofiilide analüüsid.

4.260. **Kõrgemale riskile viitavad tehingud**

4.261. Kõrgendatud tähelepanu tuleb pöörata ehk tugevdatud hoolsusmeetmeid tuleb kohaldada keerukatele, suure väärtusega ja ebatavalistele tehingutele ja tehingumustritele, millel ei ole mõistlikku või nähtavat majanduslikku või õiguspärast eesmärki või mis ei ole konkreetsele ärispetsiifikale iseloomulik.

4.262. Lisaks tugevdatud hoolsusmeetmete kohaldamisele tuleb uurida iga üksiku tehingu tausta nii palju, kui see on mõistlikult vajalik, sealhulgas tuleb fikseerida tehingu üksikasjad ning analüüsida ilmnenud asjaolusid, et selgitada välja sagedamini esinevate tehingute tüüpilisemad tunnused. Need andmed tuleb säilitada. Seejuures peamised asjaolud, millele tuleb selliste tehingute analüüsimisel tähelepanu pöörata, on järgmised:

4.262.1. milline on kahtlustäratav asjaolu toimingute, tehingute või muude asjaolude juures;

4.262.2. kas ollakse veendunud, et klienti tuntakse vajalikul määral ja kas kliendi tegevus vastab temast eelnevalt teadaolevale informatsioonile või on tema kohta vaja koguda lisaandmeid ning kasutada mõistlikke ja piisavaid meetmeid, et mõista tehingu tausta ja eesmärki. Näiteks selgitada välja rahaliste vahendite allikas ja sihtkoht või otsida rohkem teavet kliendi tegevuse kohta, et teha kindlaks sellise tehingu tõesus;

4.262.3. kas on esinenud korduvaid kahtlaste toimingute ja tehingute ilminguid (sealhulgas sarnaste olukordade või asjaolude osas);

4.262.4. kas kliendi tegevusele ja ärisuhtele üldiselt on vajalik edaspidi pöörata suuremat tähelepanu, sealhulgas üksikasjadele;

4.262.5. kas on vaja täita Rahapesu Andmebüroole teatamiskohustust juhendi punkti 7 mõttes.

4.263. **Lihtsustatud hoolsusmeetmed**

4.264. Lihtsustatud hoolsusmeetmeid võib kohaldada üksnes juhul, kui kohustatud isik on nii üldise riskihinnangu kui ka konkreetse kliendi või tehingu hindamise põhjal veendunud, et klient, tegevus, valdkond või olukord on tavapärasest vähem riskantne.

4.265. Lihtsustatud hoolsusmeetmete kohaldamine on lubatud üksnes ulatuses, milles kohustatud isik suudab jätkuvalt jälgida piisavalt ja riskipõhiselt tehinguid, toiminguid ja ärisuhteid, et tuvastada ebatavalised tehingud ja täita teatamiskohustust.

4.266. Lihtsustatud hoolsusmeetmete rakendamisel võib kliendi või tema esindaja isikusamasust kontrollida usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal ka ärisuhte loomise ajal, kui seda on vaja, et äritegevuse tavapärast käiku mitte häirida. Sellisel juhul tuleb isikusamasuse kontrollimine lõpule viia võimalikult kiiresti ning enne siduvate toimingute tegemist.

4.267. Lihtsustatud korras tegeliku kasusaaja, riikliku taustaga isiku ja ärisuhte eesmärgi tuvastamisel võib kohustatud isik valida kohustuse täitmise ulatuse ning selleks kasutatud allika ja andmete usaldusväärsest ja sõltumatust allikast kontrollimise vajaduse.

4.268. Ärisuhte seiret võib lihtsustatud korras kohaldada (st harvemini ja väiksema intensiivsusega), kui on tuvastatud madalam risk ja on arvestatud nii kliendi riskiprofiili, kui ka kohustatud isiku riskihinnangut ning täidetud on vähemalt järgmised tingimused:

4.268.1. kliendiga on sõlmitud leping kirjalikus, elektroonilises või muus kirjalikku taasesitamist võimaldavas vormis;

4.268.2. maksete liikumine usaldusväärse finantssüsteemi kaudu[33];

4.268.3. tehingutele on kehtestatud sissetulevate ja väljaminevate maksete koguväärtuse piirangud.

4.269. Lihtsustatud hoolsusmeetmete rakendamisel kliendile peab kogutud teave andma kindluse, et põhjendatud on hinnang kliendi või ärisuhtega seotud tavapärasest väiksema riski osas.

4.270. Igasuguse hoolsusmeetme kohaldamisel tuleb arvestada Eestile omaseid rahapesu ja terrorismi rahastamise riske ja meetodeid.

[33] Konto, mis asub Eestis äriregistrisse kantud krediidiasutuses või välisriigi krediidiasutuse filiaalis või krediidiasutuses, mis on asutatud või mille tegevuskoht on Euroopa Majanduspiirkonna lepinguriigis või riigis, kus kohaldatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849 nõuet ega võrdväärseid nõudeid.

4.271. Kohustatud isik dokumenteerib ning järelevalveasutuse nõudmisel näitab, miks, millises osas ja milliseid hoolsusmeetmeid on kliendi suhtes ärisuhte loomisel või ärisuhte kestel tehingutes rakendanud ning miks need on piisavad.

4.272. Lihtsustatud hoolsusmeetmete valikul tuleb arvestada väiksemat riski iseloomustavate ajaoludega.

4.273. Kliendi isikuga seotud riske vähendavad asjaolud:

4.273.1. klient on reguleeritud turul noteeritud äriühing, kellele kohaldatakse avalikustamiskohustust, mis nõuab, et tegelik kasusaaja oleks piisavalt läbipaistev. Suure läbipaistvusega ettevõte, kelle omaniku- ja finantsandmed on reguleeritud turu ja seadusega avalikult nähtavad. Selline klient on madalama riskiga, sest on lihtne tuvastada, kes tegelikult ettevõttest kasu saab;

4.273.2. klient on Eestis asutatud avalik-õiguslik juriidiline isik, näiteks riigiasutus, kohalik omavalitsus või muu avalikke ülesandeid täitev organisatsioon;

4.273.3. klient on Eesti või Euroopa Majanduspiirkonna lepinguriigi valitsusasutus või muu avalikke ülesandeid täitev asutus;

4.273.4. klient on Euroopa Liidu asutus;

4.273.5. klient on enda nimel tegutsev krediidiasutus või finantseerimisasutus, Euroopa Majanduspiirkonna lepinguriigis või kolmandas riigis asuv krediidiasutus või finantseerimisasutus, kelle kohta kehtivad tema asukohariigis Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849 nõuetega võrdväärsed nõuded, mille täitmise üle tehakse riiklikku järelevalvet;

4.273.6. klient on sellise riigi või piirkonna resident, mida iseloomustab madalam rahapesu ja terrorismi rahastamise risk.

4.274. Geograafilist riski vähendavateks asjaoludeks võib lugeda olukordi, kus klient on pärit järgmisest riigist või tema elu- või asukoht on järgmises riigis:

4.274.1. Euroopa Majanduspiirkonna lepinguriigis;

4.274.2. kolmandas riigis, kus on tõhusad rahapesu ja terrorismi rahastamise tõkestamise süsteemid;

4.274.3. kolmandas riigis, kus usaldusväärsete allikate kohaselt on korruptsiooni ja muu kuritegeliku tegevuse tase madal;

4.274.4. kolmandas riigis, kus usaldusväärsete allikate, nagu vastastikuste hindamiste, aruannete või avaldatud järelaruannete kohaselt on kehtestatud rahapesu ja terrorismi rahastamise tõkestamise nõuded, mis on kooskõlas FATF-i muudetud soovitustega, ning kus neid nõudeid tõhusalt rakendatakse.

4.275. **Tugevdatud hoolsusmeetmed**

4.276. Tugevdatud hoolsusmeetmeid peab kohaldama, kui on tuvastatud, et kliendi ja temaga seotud tegevuse näol on tavapärasest kõrgem rahapesu ja terrorismi rahastamise

risk. Tugevdatud hoolsusmeetmeid kohaldatakse selleks, et asjakohaselt juhtida ja maandada tavapärasest kõrgemat rahapesu ja terrorismi rahastamise riski.

4.277. Tugevdatud hoolsusmeede tähendab, et lisaks tavapärastele hoolsusmeetmetele kohaldatakse täiendavaid meetmeid, et kõrgemaid riske maandada.

4.278. Tugevdatud hoolsusmeetmeid saab kohaldada kliendile ärisuhte loomisel või kliendi teostatud tehingule ärisuhte kestel või juhuti tehtava tehingu puhul.

4.279. Kohustatud isik kirjeldab protseduurireeglites, millised on tugevdatud hoolsusmeetmed ja millises olukorras vastavaid meetmeid kohaldatakse.

4.280. **Hoolsusmeetmeid tuleb tugevdatud korras rakendada alati, kui:**

4.280.1. isikusamasuse või esitatud teabe kontrollimisel tekib kahtlus andmete tõele vastavuse, dokumentide ehtsuse või tegeliku kasusaaja tuvastamise osas;

4.280.2. tehingus või toimingus osalev isik on riikliku taustaga isik, va juhul kui riikliku taustaga isiku osas esineb väiksemat riski iseloomustav asjaolu, mis vähendab riski (juhendi punkt 4.144.). Kliendiriskiprofiili määramisel tuleb arvestada, et riikliku taustaga isiku puhul kohaldatakse üldjuhul alati tugevdatud hoolsusmeetmeid, sõltumata kliendi üldisest riskiskoorist. Kui klient jääb riskimudeli kohaselt madala riskiga vahemikku, kuid esineb vähemalt üks kõrgemale riskile viitav asjaolu, tuleb rakendada tugevdatud hoolsusmeetmeid ka juhul, kui asjaolude kogusumma ei anna kõrget riskiskoori. Erandina võib jätta tugevdatud hoolsusmeetmed kohaldamata, kui kõik asjaolud viitavad madalale riskile;

4.280.3. tehingus või toimingus osalev isik on pärit (sünniriik ja kodakondsus) suure riskiga kolmandast riigist või on seotud suure riskiga riigi makseteenuse pakkujaga. Näiteks, kui kinnisvaramaaklerite puhul on ostja pärit suure riskiga riigist või kui müüja pangakonto, kuhu kantakse ostuhind, on suure riskiga riigist, siis tuleb rakendada tugevdatud hoolsusmeetmeid;

4.280.4. klient, tehing või tehingus osalev isik on pärit, tema elu- või asukoht on riigist või territooriumilt, kus rahapesu ja terrorismi rahastamise tõkestamise süsteemid ei ole tõhusad või mis on Euroopa Liidu maksualast koostööd mittetegevate jurisdiktsioonide loetelus;

4.280.5. klient, tehing või tehingus osalev isik on seotud riigiga, kus on märkimisväärne korruptsioon või kuritegelik tegevus, või mille suhtes on kehtestatud sanktsioonid, embargod või sarnased meetmed ning kohustatud isik ei kohalda kaugtuvastamisel ja andmete kontrollimiseks usaldusväärsel tasemel e-identimise süsteemi ja kvalifitseeritud usaldusteenust (juhendi punkt 4.196.);

4.280.6. Tehingud virtuaalvääringutega, mis on suunatud isehallatavale aadressile või pärinevad selliselt aadressilt. Isehallatava rahakoti omaniku tuvastamine on keerulisem või peaaegu võimatu, kuna see võimaldab privaatsust. Isehallatavate rahakottidega seotud tehinguid võivad olla kõrgema riskiga, kuna puudub

võimalus tuvastada rahakoti omanikku ning puuduvad tunne oma klienti ning rahapesu ja terrorismi rahastamise tõkestamise protseduurid.

4.280.7. Kohustatud isiku riskihinnangust tulenevalt esineb majandus- või kutsetegevuses, valdkonnas või konkreetsetes asjaoludes tavapärasest kõrgem rahapesu või terrorismi rahastamise risk.

4.281. Tugevdatud ja täiendavateks hoolsusmeetmeteks on näiteks:

4.281.1. ärisuhte loomisel kõigi kliendi tegelike kasusaajate isikusamasuse tuvastamine, sealhulgas ka nende, kelle osalus on alla 25%;

4.281.2. ärisuhte loomisel kliendile sõltumatu kontrolli läbiviimine ja vajadusel kõrgema juhtkonna heakskiidu taotlemine uute ja olemasolevate klientide riskitundlikkuse alusel;

4.281.3. põhjenduste ja asjaolude tuvastamine, miks klient kasutab keerukaid omandistruktuure ja/või on registreerinud äriühingu just konkreetsesse riiki;

4.281.4. isikusamasuse tuvastamisel ja esitatud andmete täiendav kontroll. Esitatud andmete õigsuse kontrollimine täiendavate dokumentide või usaldusväärsetest ja sõltumatutest allikatest pärineva teabe alusel;

4.281.5. täiendava isikut tõendava dokumendi, elukohatõendi ja kommunaalarve vms esitamine;

4.281.6. täiendava teabe kogumine tehingu või ärisuhte eesmärgi ja olemuse kohta ning selle kontrollimine usaldusväärsete allikate abil;

4.281.7. täiendavate andmete ja dokumentide kogumine, et veenduda tehingute tegelikus toimumises ning välistada näilikkus;

4.281.8. täiendava teabe ja dokumentide kogumine, et selgitada tehingus kasutatavate vahendite päritolu;

4.281.9. esimese makse tegemine kliendi nimel avatud konto kaudu krediidiasutuses, mis asub Euroopa Majanduspiirkonnas või riigis, kus kehtivad võrreldavad rahapesu ja terrorismi rahastamise nõuded;

4.281.10. hoolsusmeetmete rakendamine kliendi või tema esindajaga samas kohas viibides;

4.281.11. virtuaalvääringutes tehtud tehingute täiendav kontroll.

4.282. Tugevdatud hoolsusmeetmete kohaldamisel tuleb tavapärasest sagedamini ärisuhet seirata. Oluline on, et esmane ärisuhte seire teostatakse hiljemalt kuue kuu jooksul pärast ärisuhte loomist ning selle käigus hinnatakse uuesti kliendi riskiprofiili.

4.283. Finantseerimisasutused arvestavad hoolsusmeetme valikul ja kohaldamisel ka Euroopa Pangandusjärelevalve Asutuse asjakohaste suunistega.

4.284. Tugevdatud hoolsusmeetmete valikul tuleb lähtuda konkreetsest riskist, arvestada Eesti-spetsiifilisi riske ning tagada, et rakendatavad meetmed on asjakohased, tõhusad ja proportsionaalsed. Selleks tuleb lähtuda kehtivast riiklikust riskihinnangust ning

Rahapesu Andmebüroo esitatud uuringutest, märgukirjadest vms avaldatud materjalidest, mis käsitlevad aktuaalseid riske Eesti finantssüsteemis.

4.285. Kohustatud isik dokumenteerib ning järelevalveasutuse nõudmisel näitab, miks, millises osas ja milliseid tugevdatud hoolsusmeetmeid on finantseerimisasutus kliendile ärisuhte loomisel või ärisuhte seirel tehingutes rakendanud.

4.286. **Suuremat riski iseloomustavad asjaolud**

4.287. Selleks, et hinnata, kas klient tehing või tehingus osalev isik on kõrgema riskiga, tuleb lähtuda kõrgemat riski iseloomustavatest asjaoludest. Kohustatud isik määrab oma protseduurides kindlaks, kas suuremat riski iseloomustavad asjaolud võetakse arvesse kogumis, osaliselt või eraldi ning millised tugevdatud hoolsusmeetmeid rakendatakse.

4.288. **Kliendiga seotud suurema rahapesu või terrorismi rahastamise riski hindamisel tuleb eelkõige arvestada järgmiste asjaoludega:**

4.288.1. Ärisuhe toimub ebatavalistel asjaoludel, sealhulgas esinevad keerukad, ebatavaliselt suuremahulised või ebaharilikud tehingud ja tehingumustrid, millel puudub selge majanduslik või õiguspärane eesmärk või mis ei ole konkreetsele ärivaldkonnale iseloomulik.

4.288.2. Seos suurema riskiga geograafilise piirkonnaga.

4.288.3. Personaalse varahaldusega tegelev klient.

4.288.4. Sularahamahukas tegevus.

4.288.5. Varjatud omandistruktuuri tunnused. Kliendiga seotud äriühingul on variaktsionärid või esitajaaktsiad.

4.288.6. Ebatavaline või keerukas omandistruktuur. Kliendi äriühingu omandistruktuur on ebaproportsionaalselt keeruline või ei ole tema tegevuse seisukohast loogiline.

4.288.7. Investeeringu alusel elamisõiguse või kodakondsuse taotlemine (nt kapitalisiirete, vara, riigivõlakirjade või äriühingutesse investeerimise).

4.289. **Toote, teenuse, tehingu või edastamiskanaliga seotud riski suurendava asjaoluna käsitletakse olukorda, kus on tegemist eeskätt:**

4.289.1. anonüümsust soodustavate toodete või tehingutega;

4.289.2. kolmandate isikute maksetega;

4.289.3. kaugtuvastamise teel loodud ärisuhted ilma täiendavate kaitsemeetmeteta. Ärisuhe või tehing algatatakse ilma osapoolte füüsilise kohalolekuta ning ei rakendata täiendavaid turvameetmeid;

4.289.4. uute toodete ja tehnoloogiatega, ärimudelite või tehnoloogiate kasutamine, eriti kui nendega seotud riskid ei ole veel täielikult hinnatud;

4.289.5. kõrgema riskiga kaupadega, näiteks nafta, relvad, väärismetallid või tubakatooted;

4.289.6. kultuuriväärtustega seotud tehingutega, mis hõlmavad arheoloogilise, ajaloolise, kultuurilise või usulise väärtusega esemeid.

4.289.7. kaitstud liikidega seotud tehingutega, mille esemeks on elevandiluu või muud kaitstud liigid.

4.290. **Kõrgem rahapesu või terrorismi rahastamise risk võib tuleneda kliendi, tehingu või tehingus osaleva isiku seotusest riigi või jurisdiktsiooniga, kus esinevad järgmised asjaolud:**

4.290.1. riigis ei ole usaldusväärsete allikate (nt vastastikused hindamised või aruanded) kohaselt kehtestatud tõhusaid rahapesu ja terrorismi rahastamise tõkestamise meetmeid;

4.290.2. riigis on märkimisväärne korruptsioon või muu kuritegelik tegevus;

4.290.3. riigi suhtes on kehtestatud sanktsioonid, embargo või muud sarnased meetmed (nt Euroopa Liidu või ÜRO poolt);

4.290.4. riik toetab terrorismi või selle territooriumil tegutsevad Euroopa Liidu või ÜRO määratletud terroristlikud organisatsioonid.

4.291. **Tehingud suure riskiga kolmandas riigis tegutsevate füüsiliste ja juriidiliste isikutega, sealhulgas FATF-i kõrge riskiga või koostööd mittetegevate riikidega**

4.292. Kui kohustatud isik puutub oma majandustegevuses tehingu või kliendi kaudu kokku suure riskiga kolmanda riigiga, tuleb kohaldada lisaks tavapärastele hoolsusmeetmetele järgmisi tugevdatud hoolsusmeetmeid:

4.292.1. hankida lisateavet kliendi ja tema tegeliku kasusaaja kohta;

4.292.2. hankida lisateavet ärisuhte eesmärgi ja planeeritava sisu kohta;

4.292.3. hankida teavet kliendi ja tema tegeliku kasusaaja rahaliste vahendite ning rikkuse päritolu kohta;

4.292.4. hankida teavet planeeritud või teostatud tehingute eesmärgi ja põhjuste kohta;

4.292.5. saada kõrgema juhtkonna luba ärisuhte loomiseks või selle jätkamiseks;

4.292.6. tõhustada ärisuhte seiret, suurendades kohaldatavate kontrollimeetmete arvu ja sagedust ning valida täiendavad tehingute näitajad ja mustrid, mida kontrollitakse.

4.293. Lisaks ülaltoodule kohaldatakse vajadusel täiendavalt ka tugevdatud hoolsusmeetmeid, mis käsitleti juhendi punktis 4.275.

4.294. Kohustatud isik jälgib pidevalt, kas tema tegevuskohariigi või tema esinduse, filiaali või tütarettevõtte tegevuskohariigi pädevad asutused või FATF on kehtestanud suure riskiga kolmandate riikide, sealhulgas FATF-i kõrge riskiga või koostööd mittetegevate riikide, suhtes täiendavaid vastumeetmeid. Kohustatud isik kohaldab neid vastumeetmeid ning tagab, et need meetmed on võetavate riskide suhtes asjakohased, efektiivsed ja proportsionaalsed.

4.295. Kohustatud isik peab pöörama kõrgendatud tähelepanu muu hulgas järgmistele asjaoludele:

4.295.1. kliendi, tegeliku kasusaaja või tehingu osapoole seosoele riigiga, mis on määratletud suure riskiga kolmanda riigina (sealhulgas FATF-i nimekirjad);

4.295.2. tehingutele, kus raha liigub läbi suure riskiga kolmanda riigi, kuigi kliendi tavapärane majandustegevus ei ole selle riigiga seotud;

4.295.3. keerukatele tehingustruktuuridele, kus kasutatakse suure riskiga riikides registreeritud ettevõtteid ilma nähtava majandusliku põhjuseta;

4.295.4. olukordadele, kus kliendi esitatud teave suure riskiga riigiga seotud tehingute kohta on puudulik, vastuoluline või raskesti kontrollitav;

4.295.5. tehingutele jurisdiktsioonidega, kus on teadaolevalt nõrk rahapesu ja terrorismi rahastamise tõkestamise raamistik või vähene järelevalve.

4.296. Kohustatud isik on kohustatud pidevalt jälgima Euroopa Liidu suure riskiga kolmandate riikide nimekirja ning FATF avaldatavaid kõrge riskiga ja koostööd mittetegevate riikide nimekirju ning tagama, et nimetatud nimekirjade muudatused kajastuvad viivitamata tema riskihinnangus, protseduurireeglites ja kontrollisüsteemides.

4.297. **Teise isiku kogutud andmetele tuginemine ja hoolsusmeetmete kohaldamise edasiandmine**

4.298. Kohustatud isik saab teatud tingimustel ühe või mitme hoolsusmeetme osalisel või täielikul täitmisel tugineda teise isiku kogutud andmete ja dokumentidele. Samuti on kohustatud isikul võimalik hoolsusmeetmete täitmisega (välja arvatud ärisuhte seire) seotud tegevused edasi anda kolmandale isikule.

4.299. Kohustatud isikul on keelatud tugineda teisele isikule või tegevusi edasi anda sellisele isikule, kes on asutatud suure riskiga kolmandas riigis.

4.300. Kui kohustatud isik otsustab tugineda teise isiku kogutud andmetele ja dokumentidele või anda tegevuse edasi, siis vastutab ikkagi kohustatud isik ise selle eest, et kõik RahaPTS-i nõuded oleks täidetud. Kui RahaPTS-i nõudeid on rikutud, siis vastutab selle eest kohustatud isik, kes tugines kolmanda isiku kogutud andmetele ja dokumentidele või andis tegevuse edasi.

4.301. **Teise isiku kogutud andmetele tuginemine**

4.302. Kohustatud isik võib tugineda teise isiku kogutud andmetele ja dokumentidele, et vältida topeltkontrolli, vähendada ressursikasutust ning lihtsustada ärisuhete loomist ja tehingute läbiviimist.

4.303. Teise isiku kogutud andmetele tuginemisel peab kohustatud isikul olema selgelt kirjeldatud ja dokumenteeritud protsess, mis sätestab, millistel juhtudel ja tingimustel sellistele andmetele tuginetakse, kuidas hinnatakse nende usaldusväärsust ning kuidas tehakse nende andmete pinnalt otsuseid.

Näiteks kaks kohustatud isikut kuuluvad samasse ettevõtete gruppi, nende tegevusalad on erinevad, kuid mõlemad täidavad rahapesu ja terrorismi rahastamise tõkestamise nõudeid ning teenindavad sama klienti. Sellisel juhul võivad kaks isikut tugineda üksteise kogutud andmetele.

4.304. Teise isiku kogutud andmetele ja dokumentidele saab tugineda, kui on täidetud järgmised tingimused:

4.304.1. teiselt isikult saadakse piisavalt teavet, et teada ärisuhet loova või tehingut tegeva isiku, tema esindaja ja tegeliku kasusaaja identiteeti ning ärisuhte või tehingu eesmärki ja olemust;

4.304.2. on tagatud, et vajadusel saab viivitamata kätte kõik andmed ja dokumendid, mille puhul tugineti teise isiku kogutud andmetele;

4.304.3. on tehtud kindlaks, et teine isik, kellele tuginetakse, on ise kohustatud täitma ning täidab Euroopa Parlamendi ja nõukogu asjakohastes direktiivides sätestatuga võrdväärseid nõudeid, sealhulgas hoolsusmeetmete kohaldamise, riikliku taustaga isiku tuvastamise ja andmete säilitamise nõudeid, ning on või on valmis olema nõuete täitmisel riikliku järelevalve all. Kohustatud isik peab võtma seejuures kasutusele piisavad meetmed, et täita selles punktis kirjeldatud tingimused.

4.305. Kohustatud isikud peavad arvestama, et klient ei pruugi neile kujutada sama tasemega riski kui isikule, kelle andmetele tuginetakse. See tähendab, et kui teine isik, kelle andmetele tuginetakse, on määranud kliendile madala riskiastme, aga kohustatud isiku jaoks on tegemist kõrge riskiastmega kliendiga, siis ei pruugi piisata teise isiku andmetest kohustatud isiku riskide maandamiseks. Kliendi riskiprofiil ja riskiaste tuleb määrata kohustatud isikul endal. Kohustatud isik peab veenduma, et teise isiku rakendatavad meetmed on kooskõlas tema sisemiste protsessidega ja on piisavad ning sellised hinnangud tuleb kirjalikult dokumenteerida.

4.306. Teise isiku andmetele tuginedes tuleb jälgida ka, et andmed, millele tuginetakse, on kogutud selle konkreetse teise isiku poolt. See tähendab, et hoolsusmeetmete kohaldamisel kogutud andmete kogumisel ei tohi tekkida nö jada, kus kohustatud isik tugineb teise isiku andmete, mis on omakorda saadud kolmandalt isikult. Sellises jadas võivad riskid jääda maandamata, sest kohustatud isik ei saa kontrollida tingimusi, mille alusel eelnevates etappides andmeid koguti.

4.307. Kui kohustatud isik kasutab teenuse osutamiseks agente, siis kohustatud isik ei saa tugineda agendi kogutud andmetele, sest agent ei ole sõltumatu teine isik. Agent on nö vahend, mille kaudu kliendile teenust osutatakse.

4.308. Teise isiku andmetele tuginemise tingimused, sealhulgas andmete väljastamise protsess, tähtajad jne, on soovituslik fikseerida lepingus.

4.309. **Tegevuste edasiandmine**

4.310. Kohustatud isikul on õigus, arvestades õigusaktides sätestatud erinõudeid ja piiranguid, kasutada lepingu alusel teise isiku teenuseid selliste tegevuste ja toimingute tegemiseks, mis on vajalikud teenuste osutamiseks ning mida tavapäraselt teeks kohustatud isik ise. Teiseks isikuks käesoleva punkti tähenduses on nt teenusepakkujad, alltöövõtjad jt isikud, kellele antakse üle nende teenuste osutamisega seotud tegevus, mida tehtaks reeglina ise oma majandustegevuses.

4.311. Tegevus antakse edasi olukorras, kus kohustatud isiku nimel ning eest kohaldab RahaPTS-ist ja/või antud juhendist tulenevaid nõudeid teine isik. Selline kohustus erineb teisele isikule tuginemisest, kus teine isik kohaldab RahaPTS-i ja/või selle juhendi nõudeid seadusest tuleneva enda kohustuse täitmiseks, misjärel kasutab kohustatud isik neid enda kohustuste täitmisel ja tugineb nendele andmetele.

4.312. Teisele isikule ei saa edasi anda ärisuhte seire kohustust.

4.313. Kohustusi saab edasi anda:

4.313.1. teisele kohustatud isikule;

4.313.2. organisatsioonile, ühendusele või liidule, mille liikmeks on kohustatud isikud;

4.313.3. muule isikule, kes rakendab seaduses sätestatud hoolsusmeetmeid ja säilitab andmeid ning kellel on lepinguline kohustus neid andmeid järelevalveasutusele kättesaadavaks teha.

4.314. Tegevuse edasi andmisel tuleb sõlmida kirjalik leping, kus tagatakse, et:

4.314.1. tegevuse edasiandmine ei takista kohustatud isiku tegevust ega seadusest tulenevate kohustuste täitmist;

4.314.2. teine isik täidab kõiki edasiandmisega seotud kohustusi;

4.314.3. tegevuse edasiandmine ei takista kohustatud isiku üle järelevalve tegemist;

4.314.4. pädev järelevalveasutus saab vajadusel kontrollida kolmanda osapoole tegevust;

4.314.5. kolmandal isikul on vajalikud teadmised ja oskused seadusest tulenevate nõuete täitmiseks;

4.314.6. kohustatud isikul on piiranguteta õigus kontrollida nõuete täitmist;

4.314.7. vajalikud dokumendid ja andmed säilitatakse ning kohustuslikud koopiad antakse koheselt kohustatud isiku või järelevalveasutuse nõudmisel. Lepinguga peab tagama, et asjakohane teave hoolsusmeetmete kohaldamisel antakse üle kohustatud isikule ja/või vastavad andmed ja dokumendid arhiveeritakse tema protseduurireeglitega ettenähtud korras;

4.314.8. oleks fikseeritud edasi antud tegevuste ulatus, õiguste ja kohustuste jaotus, sealhulgas andmete säilitamine, Rahapesu Andmebüroo teavitamine jne;

4.314.9. oleks õigus vajadusel tegevuse edasiandmise leping teise isikuga lõpetada, kui viimane on jätnud lepingujärgsed kohustused täitmata või ei ole neid kohaselt täitnud.

4.315. Teenuse edasi andmisel sõlmitud leping tuleb esitada vajadusel ka pädevale järelevalveasutusele.

4.316. Teise isiku poolt teenus(t)e osutamisel tuleb vältida olukorda, kus vajalikus ulatuses hoolsusmeetmete rakendamine ei ole piisaval määral võimalik või see on muudetud võimatuks. Teisel isikul peab olema võimalik vajalikke hoolsusmeetmeid rakendada täies ulatuses, muu hulgas peab tal olema võimalus kontaktisikut koheselt informeerida ja tehingust keelduda.

4.317. **Hoolsusmeetmete kohaldamine kokkuvõtlikult**

5. Ärisuhte loomisest või juhuti tehingu tegemisest keeldumine ning ärisuhte (erakorraline) lõpetamine

5.1. **Ärisuhte loomisest või tehingu tegemisest keeldumine**

5.2. Kohustatud isikul on keelatud luua ärisuhet või võimaldada tehingu tegemist, kui esineb mõni järgmistest olukordadest:

5.2.1. rahapesu või terrorismi rahastamise kahtlus või kohustuslikke hoolsusmeetmeid ei saa täielikult rakendada. Näiteks klient ei esita vajalikke dokumente ja teavet või esitatud andmed ei võimalda veenduda kogutud info piisavuses;

5.2.2. ärisuhet või tehingut soovib isik, kelle kapitalist üle 10% moodustavad esitajaväärtpaberid. Selline olukord võib varjata tegelikku kasusaajat, muutes hoolsusmeetmete rakendamise võimatuks ning suurendades rahapesu, terrorismi rahastamise ja sanktsioonide rikkumise riski;

5.2.3. ärisuhet või tehingut soovib isik, kellel puudub vastav tegevusluba, kuid kelle peamine ja püsiv majandustegevus sarnaneb litsentseeritud finantsteenuse osutamisele;

5.2.4. ärisuhe või tehing looks anonüümse konto või konto vale isiku nimele;

5.2.5. ärisuhte loomisel või tehingu tegemisel on variisiku esinemise kahtlus.

5.3. Kohustust ärisuhte loomise või tehingu tegemise keeldumise kohta ei kohaldata, kui kohustatud isik on teavitanud Rahapesu Andmebürood ja saanud juhise jätkata ärisuhet või tehingut.

5.4. **Tehingu edasilükkamine**

5.5. Kohustatud isikul on õigus lükata tehing edasi, kuni tehingus osalev isik või klient on esitanud kõik hoolsusmeetmete rakendamiseks vajalikud dokumendid ja teabe, sealhulgas tehingu objektiks oleva vara päritolu tõendamiseks ja ärisuhte seireks vajaliku teabe.

5.6. Tehingu tegemist võib jätkata vaid erandjuhtudel, kui selle edasilükkamine takistaks kahtlasest tehingust kasusaajate tuvastamist. Sellisel juhul peab kohustatud isik:

5.6.1. tegema tihedat koostööd Rahapesu Andmebürooga,

5.6.2. dokumenteerima tehtud meetmed ja otsused, sealhulgas põhjenduse, miks tehingu edasilükkamine oleks takistanud kasusaajate tuvastamist.

5.7. Kui mõistliku aja jooksul ei ole võimalik rakendada piisavaid hoolsusmeetmeid, et koguda vajalikku teavet ja veenduda andmete õigsuses või kõrvaldada rahapesu või terrorismi rahastamise kahtlus, peab kohustatud isik ärisuhte erakorraliselt lõpetama.

5.8. **Ärisuhte (erakorraline) lõpetamine**

5.9. Kohustatud isikul on õigus ärisuhte aluseks olev leping lõpetada kas korraliselt või erakorraliselt. Korraline lõpetamine toimub vastavalt lepingu tingimustele. Erakorraline lõpetamine võib toimuda juhul, kui ärisuhte lõpetamine on kohustatud isiku otsustada

või kui klient rikub oluliselt lepingutingimusi, näiteks keeldub hoolsusmeetmete rakendamiseks vajaliku teabe või dokumentide esitamisest.

5.10. Kohustatud isik võib ärisuhte erakorraliselt lõpetada ilma etteteatamistähtaegadeta, kui e-residendist kliendi digitaalne isikutunnistus on kehtetuks tunnistatud, peatatud või väljaandmisest keeldutud või kui klient rikub oluliselt hoolsusmeetmete kohustust, näiteks ei esita vajalikku teavet või dokumente rahapesu ja terrorismi rahastamise tõkestamiseks.

5.11. Erakorralisel lõpetamisel peab kohustatud isik tagastama kliendi vara mõistliku aja jooksul, soovitatavalt mitte hiljem kui ühe kuu jooksul. Vara kantakse kontole Eestis registreeritud krediidiasutuses või välisriigi krediidiasutuses/filiaalis, mis tegutseb Euroopa Majanduspiirkonnas või jurisdiktsioonis, kus kehtivad Euroopa Parlamendi ja nõukogu direktiividega võrdväärsed regulatsioonid.

5.12. Erandjuhul võib vara kanda muule kui kliendi kontole, mis vastab eeltoodud tingimustele, teavitades sellest vähemalt 7 tööpäeva ette Rahapesu Andmebürood, tingimusel, et büroo ei ole kehtestanud käsutuspiirangut vara suhtes. Kõik maksed tuleb dokumenteerida, märkides inglise keeles, et tegu on kliendisuhte erakorralise lõpetamisega.

5.13. Kohustatud isik võib erandjuhul tehingu siiski teha või ärisuhtega ajutiselt jätkata, kui tehingu tegemata jätmine või ärisuhte lõpetamine võib takistada kahtlasest tehingust kasusaajate tuvastamist. Sellisel juhul peab kohustatud isik teavitama Rahapesu Andmebürood viivitamata pärast tehingu tegemist või otsust jätkata ärisuhet ning dokumenteerima kõik asjakohased otsused ja põhjendused

5.14. Kohustatud isik peab teatama Rahapesu Andmebüroole erakorralise lõpetamise asjaoludest ja säilitama kogu dokumentatsiooni vastavalt sisekontrolli nõuetele.

6. Andmete registreerimine ja säilitamine

6.1. Kohustatud isik peab registreerima ja säilitama kõik andmed, mis on seotud hoolsusmeetmete kohaldamise, tehingute tegemise ning RahaPTS-i kohustuste täitmisega.

6.2. Kohustatud isik peab muu hulgas registreerima ja säilitama järgmised andmed ja dokumendid:

6.2.1. Ärisuhte ja tehingutega, sealhulgas juhuti tehingutega seotud otsused:

6.2.1.1. teave ärisuhte loomisest või juhuti tehtava tehingu tegemisest keeldumise kohta;

6.2.1.2. teave olukordade kohta, kus infotehnoloogiliste vahendite abil ei ole võimalik hoolsusmeetmeid kohaldada;

6.2.1.3. teave juhtudest, kus klient loobub ärisuhte loomisest või tehingu tegemisest, sealhulgas juhuti tehingu tegemisest, seoses hoolsusmeetmete kohaldamisega;

6.2.1.4. teave ärisuhte lõpetamise asjaolude kohta, kui hoolsusmeetmeid pole võimalik kohaldada.

6.2.2. Isikusamasuse tuvastamise ja kontrollimise andmed:

6.2.2.1. isikusamasuse tuvastamise ja kontrollimise aluseks olevad dokumendid, originaalid või koopiad;

6.2.2.2. isikusamasuse tuvastamisel digitaalselt ehk isikuga samas kohas viibimata:

6.2.2.3. digitaalseks isikutuvastamiseks kasutatud dokumendi andmed;

6.2.2.4. teave elektrooniliste päringute kohta riiklikesse registritesse;

6.2.2.5. isikusamasuse tuvastamise ja kontrollimise protsessi andmed koos ajatempliga;

6.2.2.6. muud kontrolli tõendavad andmed (näiteks logid), sealhulgas kahe sõltumatu allika kasutamise tõendid.

6.2.3. Ärisuhte loomise ja seirega seotud dokumendid:

6.2.3.1. ärisuhte loomise aluseks olevad dokumendid, välja arvatud juhendi eelmises punktis nimetatud dokumendid;

6.2.3.2. ärisuhte käigus kogutud andmed ja dokumendid, sealhulgas kliendi tegevuse ja tehingute analüüsid, tehingute tausta ja eesmärgi selgitamisega seotud andmed ning keerukate, ebatavaliste või suure väärtusega tehingute analüüsid.

6.2.4. Tehingute andmed:

6.2.4.1. tehingu tegemise kuupäev või ajavahemik;

6.2.4.2. tehingu sisu kirjeldus;

6.2.4.3. tehingu summa, vääring ja seotud konto andmed;

6.2.4.4. erijuhtudel täiendavad andmed, näiteks juriidilise isiku staatust mitteomava ühenduse või usaldusfondi esindaja staatus ja registriandmed või vara hoiule võtmisel deponeerimisnumber, turuhind või vara kirjeldus, muu tehingu puhul summa, vääring ja konto number.

6.2.5. Muud andmed ja teatamiskohustusega seotud teave:

6.2.5.1. kogu RahaPTS-ist ja juhendist tulenevate kohustuste täitmisega seotud kirjavahetus;

6.2.5.2. Rahapesu Andmebüroole teatamiskohustuse täitmise aluseks olev teave;

6.2.5.3. andmed kahtlaste või ebatavaliste tehingute kohta ka juhul, kui neist ei teatatud. Soovituslik on säilitada dokumentatsioon, mis sisaldaks ka asjaolude hindamist, kogutud tõendeid, kahtluse välistamise põhjuseid ning otsuse teinud isiku või struktuuriüksuse. Selline dokumenteerimine võimaldab otsustusprotsessi jälgida ning seda hiljem kontrollida.

6.3. Käesolevas peatükis nimetatud andmeid säilitatakse 5 aastat pärast ärisuhte lõppemist või juhuti tehtud tehingu tegemist.

6.4. Rahapesu Andmebüroole teatamisega seotud andmeid säilitatakse 5 aastat pärast teatamiskohustuse täitmist.

6.5. Andmeid ei pea registreerima ega säilitama ulatuses, milles kohustatud isik on võimeline neid usaldusväärselt reprodutseerima kogu 5-aastase säilitamistähtaja jooksul. Samas peab kohustatud isik igal ajal olema võimeline tõendama, et isikusamasuse tuvastamise käigus kogutud andmeid on kontrollitud, ning esitama teabe kontrollitud andmete päritolu, nende usaldusväärsuse ja sõltumatute allikate kohta, sealhulgas tõendama vähemalt kahe sõltumatu allika kasutamist.

6.6. Kui hoolsusmeetmete kohaldamiseks tehakse päring riigi infosüsteemi andmekogusse, loetakse andmete säilitamise kohustus täidetuks, kui päringu tegemise fakt ning kuupäev on taasesitatav 5 aasta jooksul pärast ärisuhte lõppemist või juhuti tehtud tehingu tegemist. Samas tuleb registreerida ja säilitada andmed kuupäeva osas, millal vastav päring teostati.

6.7. Finantseerimisasutus säilitab RahaPTS § 31 rakendamisel digitaalseks isiku tõendamiseks ette nähtud dokumendi andmed, teabe elektroonilise päringu tegemise kohta isikut tõendavate dokumentide andmekogusse ning isikusamasuse tuvastamise ja kontrollimise protseduuri andmeid koos ajatempliga viis aastat pärast ärisuhte lõppemist.

6.8. **Andmete säilitamise ja kustutamise põhimõtted**

6.9. Säilitatud andmed tuleb kustutada pärast säilitamistähtaja möödumist, kui õigusaktidest ei tulene teisiti.

6.10. Pädeva järelevalveasutuse ettekirjutuse alusel võib rahapesu või terrorismi rahastamise tõkestamise, avastamise või uurimise seisukohast olulisi andmeid säilitada kauem, kuid mitte rohkem kui 5 aastat pärast esmase tähtaja möödumist.

6.11. **Andmete kättesaadavus ja säilitamise viis**

6.12. Dokumente ja andmeid tuleb säilitada viisil, mis võimaldab viivitamata ja ammendavalt vastata Rahapesu Andmebüroo või vastavalt õigusaktidele teiste järelevalveasutuste, uurimisasutuste või kohtu päringutele.

6.13. Kohustatud isik peab muu hulgas suutma tuvastada, kas tal on päringus nimetatud isikuga olnud ärisuhe viimase 5 aasta jooksul ning milline on või oli selle ärisuhte olemus.

6.14. Dokumente ja andmeid tuleb säilitada süstemaatiliselt ja kronoloogiliselt, tagades selge struktuuri, dokumentide loogilise jaotuse (näiteks dokumentide pealkirjastamise) ja hoolsusmeetmete rakendamise jälgitavuse kogu ärisuhte vältel.

7. Teatamiskohustus

7.1. Kohustatud isik on kohustatud teavitama Rahapesu Andmebürood tegevustest või asjaoludest, mis on tuvastatud majandustegevuse käigus ja mille puhul:

7.1.1. esinevad tunnused, mis viitavad kuritegelikust tegevusest saadud tulu kasutamisele või sellega seotud kuritegude toimepanemisele (esitada eelkõige kahtlase või ebahariliku tehingu või tegevuse teade ehk UTR või UAR);

7.1.2. kohustatud isikul on kahtlus või teadmine või esinevad tunnused, mis viitavad rahapesule või sellega seotud kuritegude toimepanemisele (esitada rahapesu kahtlusega tehingu teade ehk STR);

7.1.3. kohustatud isikul on kahtlus või teadmine või esinevad tunnused, mis viitavad terrorismi rahastamisele või sellega seotud kuritegude toimepanemisele (esitada terrorismi rahastamise teade ehk TFR);

7.1.4. tegemist on eeltoodud tegevuste või asjaolude katsega;

7.1.5. kohustatud isik on keeldunud ärisuhte loomisest või tehingu tegemisest või on ärisuhte erakorraliselt lõpetanud ning keeldumise või lõpetamise aluseks on kahtlased või ebaharilikud asjaolud;

7.1.6. kohustatud isik saab teatavaks tehingust, mille puhul täidetakse sularahas rahaline kohustus summas üle 32 000 euro (või sellega võrdväärne summa muus vääringus), sõltumata sellest, kas tehing tehakse ühe maksena või mitme omavahel seotud maksena kuni ühe aasta jooksul (esitada summapõhine teade ehk CTR).

7.1.6.1. Seotud tehinguteks tuleb pidada tehinguid, mis on omavahel sisuliselt seotud ning moodustavad ühtse terviku, sõltumata sellest, kas need tehakse ühekordselt või mitme eraldiseisva tehinguna teatud ajavahemiku jooksul. Seotud tehingute tuvastamisel ei ole piisav üksnes asjaolu, et tehingud on teinud sama klient või et need on toimunud kuni ühe aasta jooksul. Hinnata tuleb tehingute omavahelist loogilist ja sisulist seost. Seotud tehingutele võivad viidata näiteks sama või sarnane eesmärk, samad või omavahel seotud osapooled, raha liikumine samasse sihtkohta või samast allikast, tehingute tegemine ajaliselt lähestikku või tehingute jagamine väiksemateks osadeks. Seotud tehingute hindamisel tuleb lähtuda kohustatud isikule teadaolevast või mõistlikult kättesaadavast teabest.

7.2. Täiendavad kahtlaste tegevuste ja asjaolude tunnused, mis vajaksid teate esitamist Rahapesu Andmebüroole, on toodud Rahapesu Andmebüroo juhendis „Juhend kahtlaste tehingute tunnuste kohta“ (leitav kodulehelt https://www.fiu.ee/ juhendite rubriigist).

7.3. **Teate esitamise aeg ja kord**

7.4. Teade tuleb esitada enne tehingu tegemist, kui kahtlus või teadmine rahapesu või terrorismi rahastamise kohta tekib enne tehingu tegemist.

7.5. Kui tehingu edasilükkamine ei ole võimalik, võib põhjustada olulist kahju või võib takistada kahtlase tehingu kasusaajate tuvastamist, võib tehingu erandjuhul teostada. Sellisel juhul tuleb teade esitada viivitamata pärast tehingu tegemist ning teha koostööd Rahapesu Andmebürooga.

7.6. Teatamiskohustus tuleb täita viivitamata, kuid hiljemalt kahe tööpäeva jooksul alates hetkest, mil tuvastatakse kahtlane tegevus või asjaolu või tekib põhjendatud kahtlus, mida ei ole võimalik ümber lükata. Viivitamatu teatamise eesmärk on võimaldada

Rahapesu Andmebürool rakendada vajalikke meetmeid, arvestades rahaliste vahendite kiiret liikumist erinevate riikide ja finantssüsteemide vahel.

7.7. Teatamiskohustus ei välista ega asenda hoolsusmeetmete kohaldamist. Kahtluse korral tuleb jätkata asjakohaste hoolsusmeetmete rakendamist kuni kahtluse kõrvaldamiseni või otsuse tegemiseni edasiste meetmete osas.

7.8. Kui teatamiskohustus on täidetud, tuleb enne ärisuhte loomisest keeldumist või ärisuhte erakorralist lõpetamist vajadusel ära oodata Rahapesu Andmebüroo juhised, välja arvatud juhul, kui viivitus ei ole võimalik või ei ole asjakohane.

7.9. Kui summapõhise teate või ärisuhte keeldumise/lõpetamisega kaasnevad ka rahapesu või terrorismi rahastamise kahtluse tunnused, tuleb esitada vastav kahtlusepõhine teade. Sellisel juhul võib teabe esitada ühe teatena, kuid tuleb selgelt viidata erinevatele alustele ja indikaatoritele.

7.10. Kui kohustatud isik tuvastab korduvalt kahtlasi või ebaharilikke tehinguid, mille puhul esialgu ei ole võimalik tuvastada rahapesu või terrorismi rahastamise kahtlust, peab selliste juhtumite kuhjumisel kujunema põhjendatud kahtlus. Sellisel juhul tuleb esitada vastav teade Rahapesu Andmebüroole, kohaldada täiendavaid hoolsusmeetmeid ning hinnata ärisuhte jätkamise või tehingu tegemise lubatavust.

8. Rahapesu Andmebüroo pädevus

8.1. Rahapesu Andmebüroo põhimääruse alusel on Rahapesu Andmebüroo ülesandeks muu hulgas järelevalve teostamine RahaPTS-i täitmise osas.

8.2. Rahapesu Andmebüroo ülesandeks on ka rahvusvahelise sanktsiooni seadusest tulenevate ülesannete täitmine. Rahapesu Andmebüroo koostanud juhendi Rahapesu Andmebüroo järelevalvatavatele erikohustustega isikutele ja juhendi finantssanktsioonide kohaldamiseks. Mainitud juhendid on leitavad Rahapesu Andmebüroo kodulehelt www.fiu.ee juhendite rubriigist.

8.3. RahaPTS-i § 64 lõikes 1 sätestatu kohaselt teostab Rahapesu Andmebüroo järelevalvet RahaPTS-i ja selle alusel kehtestatud õigusaktide nõuete täitmise üle nende kohustatud isikute suhtes, kes ei ole Finantsinspektsiooni järelevalve all.

8.4. RahaPTS § 56 lõike 1 kohaselt on Rahapesu Andmebürool õigus välja anda soovituslikke juhendeid rahapesu ja terrorismi rahastamise tõkestamist käsitlevate õigusaktide selgitamiseks.

8.5. Juhendis kasutatud mõisted on defineeritud RahaPTS-i 1. peatüki 2. jaos, Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849 (AMLD 4)[34] I peatüki 1. jaos, Euroopa Parlamendi ja nõukogu direktiivis (EL) 2018/843 (AMLD

[34] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

5)[35], FATF-i 2012. aasta soovitustes[36] ja 2013. aasta metodoloogia sõnastikus[37] ning muudes juhendites[38].

8.6. Rahapesu ja terrorismi rahastamise tõkestamise nõuete täitmise all on juhendi mõistes peetud silmas kõiki tegevusi, mida FATF eeldab liikmesriikidelt ja Rahapesu Andmebüroo järelevalve all olevatelt kohustatud isikutelt ennetavate meetmete kohaldamisel, sealhulgas korruptsiooni tõkestamist.

[35] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32018L0843
[36] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
[37] https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/fatfissuesnewmechanismtostrengthenmoneylaunderingandterroristfinancingcompliance.html
[38] Nii Rahapesu Andmebüroo kui ka Finantsinspektsiooni poolt välja antud juhendid.

9. Lisad

Lisa 1. Riskikategooriatega seotud märksõnad kohustatud isiku ülese riskihinnangu koostamiseks

1. Klientidega, sealhulgas tegeliku kasusaajaga seonduv risk.
- Juriidilised isikud ja füüsilised isikud. - Resident/mitteresident (mis jurisdiktsiooniga on isik seotud). - Juriidilisest isiku puhul juriidilise isiku vorm (seltsing, mittetulundusühing, sihtasutus vms). - Nominaaldirektorite kasutamine tehingutes. - Kliendi omandistruktuur (keerulised, läbipaistmatud, lihtsad). - Keeruliste omandistruktuuride vms läbi tegeliku kasusaaja tuvastamine – keeruline, lihtne. - Omandistruktuuris kliendi omanik välisriigi juriidiline isik. - Kliendi või tegeliku kasusaaja seotud sanktsioonidega. - Kas klient või tegelik kasusaaja on riikliku taustaga isik, tema pereliige või tema lähedaseks kaastöötajaks peetav isik. - Kas kliendisuhetes esineb nominaaldirektoreid või aktsionäre? - Milline on kliendi tegevusala? Kas tegutsetakse kõrgema riskiga sektoris? Hinnata kõrgema riskiga sektoreid, sealhulgas valdkondi, millega seonduvad suured sularahatehingud. - Tehingus esindajate kasutamine. - Teave, mis kogutud tunne-oma-klienti meetmete rakendamisel (planeeritavad mahud, varade ja rikkuse päritolu jne) jne. - Kliendi ja tema tegeliku kasusaaja olemus ja käitumine (hoidub kohtumistest, raskesti kättesaadav, ei vasta tähtaegselt kirjadele, ei esita dokumente, kiirustab tehinguid, muudab korduvalt tehingute andmeid jne). Raamatupidajad: - Kas kliendi rahavood on kooskõlas deklareeritud tegevusega? - Raamatupidamisdokumentide puudulik esitamine. - Äriühingud, millel puudub reaalne majandustegevus. Usaldushalduse ja äriühingute teenuse pakkujad: - Nominaalaktsionäri või nominaaldirektori kasutamine ilma selge põhjuseta. - Keerulised omandistruktuurid, mis seotud mitmete jurisdiktsioonidega. - Keeruline tegeliku kasusaaja tuvastamine. - Riiulifirmade ostmine. Valuutavahetusteenus: - Tehingute struktureerimine, väikses mahus tehingute tegemine. - Teadlikult erinevate valuutavahetuspunktide kasutamine isikusamasuse tuvastamise vältimiseks. - Suured sularahatehingud. Kinnisvaramaaklerid: - Kinnisvara ost läbi *offshore*-ettevõtte. - Püüdlused varjata kliendi tegelikku kasusaajat. - Kliendi ebatavaliselt suured püüdlused tehingu kiirendamiseks. - Kinnisvara ostavad välisriigi juriidilised isikud.
2. Toodete, teenuste või tehingutega, sealhulgas uute ja/või tulevikus pakutavate toodete, teenuste või tehingutega seonduv risk.
- Kas ja mis ulatuses pakutav toode või teenus võimaldab anonüümsust? - Makseviisid (sularaha, pangaülekanne, virtuaalvääringud, virtuaalvääringute rahakotid, muud ebatavalised makseviisid nagu väärismetallid jne). - Laekumised kolmandate isikute poolt. - Tähtajalised vs tähtajatud lepingud. - Lepingu tingimused (nt laenulepingute puhul laenu tagasimakse graafik). - Tehingute keerukus, tehingute maht ja sagedus. - Tehingutes kasutatud vahendite päritolu.

- Korrespondentsuhted. - Anonüümsust võimaldavad teenused. - Ebaharilikud esindusõigused/volitused. - Kliendi tehingutes ebakõlad jne.
3. Suhtlus- või vahenduskanalitega või toodete, teenuste või tehingute edastamis- ja müügikanalitega, sealhulgas selliste uute ja/või tulevikus pakutavate kanalitega seonduv risk.
- Riskid suhtluskanalite lõikes, nt e-posti teel suhtlemine, suhtlusrakenduste kaudu suhtlemine. - Igapäevaselt kasutatavad andmebaasid, IT-süsteemid (nii enda kui ka kolmandate isikute pakutavad). - Integreeritud infrastruktuur (erinevad makselingid). - Erinevad platvormid teenuse osutamiseks (koduleht, mobiilirakendus, veebikeskkonnad) jne. - E-identifitseerimine. - Automatiseeritud süsteemide kasutamine. - CSP-del agentide kasutamise risk.
4. Riikide või geograafiliste piirkondade või jurisdiktsioonidega seonduv risk.
- Kõrge riskiga piirkonnad. - Suure riskiga kolmandad riigid. - Riigid, kus ei ole kehtestatud rahapesu ja terrorismi rahastamise tõkestamise tõhusaid süsteeme. - Maksualast koostööd mittetegevad riigid. - Erinevad rahvusvahelised nimekirjad, määrused ja resolutsioonid (nt FATF, Rahapesu Andmebüroo juhendid/nimekirjad, ÜRO, EU jne).

Lisa 2. Näide kliendi riskiprofiili lihtsustatud mudelist

Järgnev on näide ning iga kohustatud isik peab kliendi riskiprofiili määramise mudeli koostama vastavalt organisatsiooni suurusele, tegevusele, osutatavate teenuste olemusele, ulatusele, keerukusastmele, tegevusega kaasnevatele riskidele ning riskiisule.

Kliendi riskiprofiil määratakse ettevõtteüleses riskihinnangus tuvastatud riskikategooriate alusel. Iga riskitegur hinnatakse tavapäraselt numbriliselt. Numbriline skaala ning väärtused sõltuvad kohustatud isiku riskide hindamise metoodikast.

Riskikategooriad ja riskinäitajad			
Kliendirisk			
Riskitegur	**Madal (1p)**	**Keskmine (2p)**	**Kõrge (3p)**
Kliendi tüüp	eraisik või lihtne kohalik ettevõte	rahvusvahelise tegevusega ettevõte	keeruline omandistruktuur
Tegelik kasusaaja	selgelt tuvastatav	mitme tasandiga omandistruktuur	tegelik kasusaaja raskesti tuvastatav
Kliendi taust ja maine	negatiivne info puudub	piiratud avalik info	negatiivne meediainfo
PEP staatus	ei ole PEP	PEP-iga seotud isik	PEP
Geograafiline risk			
Riskitegur	**Madal (1p)**	**Keskmine (2p)**	**Kõrge (3p)**
Kliendi asukohariik	EL või EMP riik	mõõduka riskiga riik	kõrge riskiga jurisdiktsioon
Tehingute geograafia	ainult EL riigid	EL ja muud riigid	kõrge riskiga riigid
Toote ja teenuse risk			
Riskitegur	**Madal (1p)**	**Keskmine (2p)**	**Kõrge (3p)**
Kasutatavad teenused	lihtsad ja läbipaistvad teenused	rahvusvahelised maksed	keerulised või anonüümsust võimaldavad teenused
Tehingute maht	väikesed ja regulaarsed	keskmise suurusega	väga suured või ebaharilikud
Tarnekanali risk			
Riskitegur	**Madal (1p)**	**Keskmine (2p)**	**Kõrge (3p)**
Kliendisuhtluse viis	otsene kontakt	osaliselt vahendatud	täielikult kaugteel
Kliendi tuvastamine	isiklik tuvastamine	elektrooniline tuvastamine	vahendaja kaudu

Riskiprofiili määramisel liidetakse kõigi riskitegurite punktid ning punktide summa tulemusel leitakse kliendi riskiaste.

10–14 punkti	Madal risk
15–22 punkti	Keskmine risk
23–30 punkti	Kõrge risk

Lisa 3. Kohustatud isiku poolt kehtestatavad dokumendid

Käesolevas lisas on esitatud dokumentide kontrollnimekiri, mis tuleb RahaPTS-i nõuete täitmiseks koostada igal RahaPTS-i mõistes kohustatud isikul. Kontrollnimekiri on abivahend kohustatud isikule, et hinnata, kas organisatsioonis on kehtestatud ja rakendatud vajalikud sisemised reeglid, protseduurid ja riskijuhtimise meetmed. Kohustatud isik peab tagama, et tabelis toodud dokumendid on ajakohased ning vastavad kohustatud isiku tegevuse iseloomule, mahule ja keerukusele. Dokumente tuleb vajaduse korral regulaarselt üle vaadata ja ajakohastada.

Dokumentide loetelu ei ole ammendav ning kohustatud isik peab vajaduse korral kehtestama täiendavaid protseduure ja dokumente, lähtudes oma tegevuse iseloomust, mahust, keerukusest ning tuvastatud rahapesu ja terrorismi rahastamise riskidest.

Kontrollnimekirjas toodud dokumendid ja protseduurid peavad olema ajakohased, töötajatele kättesaadavad ning praktikas rakendatavad. Kohustatud isik peab regulaarselt hindama nende asjakohasust ning vajadusel neid ajakohastama.

Nimetatud dokumendid/protseduurid võivad olla koondatud ühte põhidokumenti (näiteks protseduurireeglitesse), kuid erinevad sisemised dokumendid ja protsessid võib kehtestada ka eraldiseisvalt.

Dokument/protsess/kord	Kontrollküsimused
Rahapesu ja terrorismi rahastamise riskihinnang	• Kas riskihinnang on dokumenteeritud? • Kas see katab vähemalt kliendi-, toote-, geograafilisi ja kanaliriske? • Kas see on ajakohane? • Kas riskihinnang lähtub ettevõtte tegevusvaldkonnast? • Millise regulaarsusega riskihinnangut uuendatakse?
Rahapesu ja terrorismi rahastamise riskiisu	• Kas riskiisu on dokumenteeritud? • Kas riskiisu on koostatud lähtudes ettevõtte ärimudelist, toodetest/teenustest ja klientidest? • Millist riski on ettevõte valmis kandma? • Millise regulaarsusega riskiisu uuendatakse? • Kas riskiisus on määratud riskid kvalitatiivsel ehk kirjeldaval ja kvantitatiivsel ehk mõõdetaval tasemel?
Protseduurireeglid	• Kas protseduurireeglid sisaldavad kliendi suhtes rakendatavate hoolsusmeetmete korda, sealhulgas lihtsustatud ja tugevdatud hoolsusmeetmete rakendamist? • Kas on kirjeldatud, kuidas tuvastatakse füüsiline ja kuidas juriidiline isik? • Kas on kehtestatud isikusamasuse tuvastamise koht nii näost-näkku kui ka kaugtuvastamise puhul (sealhulgas kaugtuvastamisel kasutatavad vahendid)?

	• Kas protseduur kirjeldab, kuidas tuvastada tegelik kasusaaja nii füüsilise isiku kui ka juriidilise isiku puhul? • Kas on kirjeldatud riikliku taustaga isiku tuvastamise protseduurid? • Kas on sätestatud klientidega seotud riskide hindamine? • Kas on kirjeldatud kliendile riskiprofiili määramine? • Kas on kirjeldatud, milliseid tehinguid jälgitakse ja kuidas? • Kas on kehtestatud teatamiskohustuse täitmise juhend? • Kas on kehtestatud detailne käitumisjuhis/kord teatamiskohustuse täitmiseks? • Kas on määratletud, kuidas kontrollitakse sanktsioonide nimekirju? • Kas on kirjeldatud dokumentide ja andmete säilitamise kord ja tähtajad? • Kas on kirjeldatud töötajatele tehtavad koolitused ja nende regulaarsus?
Sisekontrollieeskiri	• Kas sisekontrollieeskiri on dokumenteeritud? • Kas see sisaldab siseauditi ja vastavuskontrolli rakendamise korda ning vajadust? • Kas see sisaldab töötajate kontrollimise korda?
Kontaktisiku ülesanded	• Kas kohustatud isik on kirjeldanud RahaPTS-i kontaktisiku ülesanded? • Kas kontaktisik on teadlik talle kohalduvatest õigustest ja kohustustest?