VirtualMoney OÜ

VIRTUAALVÄÄRINGU RAHA VASTU VAHETAMISE TEENUSE OSUTAJA PROTSEDUURIREEGLID JA SISEKONTROLLIEESKIRI
Rahapesu ja terrorismi rahastamise tõkestamise seaduse rakendamiseks

ÜLDSÄTTED JA MÕISTED

Käesolevad protseduurireeglid, edaspidi **Juhend**, reguleerivad VirtualMoney OÜ tegevust rahapesu ja terrorismi rahastamise tõkestamise seaduse (RahaPTS) rakendamiseks.
Käesolevas Juhendis on alljärgnevatel mõistetel järgmine tähendus:
Rahapesu- ajakohane kehtiv määratlus vastavalt RahaPTS § 4.
Terrorismi rahastamine- ajakohane kehtiv määratlus vastavalt RahaPTS § 5.
Tegelik kasusaaja – ajakohane kehtiv määratlus vastavalt RahaPTS § 9.
VirtualMoney – virtuaalvääringu raha vastu vahetamise teenuse osutaja, kes on kohustatud isikuks RahaPTS seaduse mõttes.
Ärisuhe – ajakohane kehtiv määratlus vastavalt RahaPTS § 3.
Klient- ajakohane kehtiv määratlus vastavalt RahaPTS § 3.
Personal- VirtualMoney töötaja, VirtualMoney juht, juhatuse liikmed, nõukogu liikmed
Kontaktisik- juhatuse poolt määratud isik, kes on rahapesu andmebüroo kontaktisikuks. Kontaktisikuks võib olla VirtualMoney juhatuse liige või muu Personali liige.

1. RahaPTS RAKENDAMISE KOHUSTUSLIKKUS

VirtualMoney kohustub virutaalvääringu raha vastu vahetamise teenuse pakkujana järgima käesolevaid protseduurireegleid tulenevalt rahapesu ja terrorismi rahastamise tõkestamise seaduse (edaspidi RahaPTS) § 2 lg 1 p 10 .
VirtualMoney juhatus kohustub tagama, et iga Personali liige täidab käesolevas Juhendis, RahaPTS-is ning selle alusel antud õigusaktides sätestatud nõudeid. VirtualMoney Personali liikmed peavad tundma ja täitma õigusakte ja asjaomaseid ametiasutuste juhendeid ning tutvuma iseseisvalt õigusaktide ja juhendite muudatustega.
Personali liige vastutab RahaPTS ja käesolevast Juhendist tulenevate nõuete täitmise eest isiklikult. Nõuete rikkumine võib tuua kaasa töölepingu lõpetamise ja väärteo või kriminaalkorras karistamise.

HOOLSUSMEETMED

1 VirtualMoney kohaldab RahaPTS-is nimetatud hoolsusmeetmeid sobivas ja vajalikus ulatuses, lähtudes VirtualMoney äritegevuse iseloomust ning tehingus osaleva isiku riskiastmest.
2 VirtualMoney pöörab tegevuses kõrgendatud tähelepanu kliendi tegevusele ja asjaoludele, mis viitavad rahapesule või terrorismi rahastamisele või mille seotus rahapesu või terrorismi rahastamisega on tõenäoline.

3 Enne kliendiga ärisuhte loomist, tehingu tegemist ja ärisuhte kestel kohaldab VirtualMoney järgmisi hoolsusmeetmeid:
1 Kliendi isikusamasuse tuvastamine, esitatud teabe kontrollimine, andmete säilitamine ja ajakohastamine;

2 kliendi esindaja isikusamasuse ja esindusõiguse tuvastamine ning kontrollimine. Täpsustada tuleb esindajale antud volituste ulatust, sh kas tegemist on pikemaajalise suhtega või ainult ühekordse tehinguga ning kas esindusõigus võimaldab VirtualMoneyga ärisuhtesse asuda.
3 tegeliku kasusaaja tuvastamine;
4 teabe hankimine ärisuhte ja tehingu eesmärgi ning olemuse kohta;
5 igapäevane hoolsus ja valvsus kliendiga suhtlemisel, sealhulgas ärisuhte vältel teostatud tehingute jälgimine, isikusamasuse tuvastamisel kasutatud andmete regulaarne kontrollimine, asjakohaste dokumentide, andmete ja teabe ajakohastamine ning vajaduse korral tehingus kasutatud vahendite allika ja päritolu tuvastamine;
6 Kontaktisiku teavitamine olukordadest, kui tehingu sisus või kliendi tegevuses võivad esineda rahapesu või terrorismi rahastamise tunnused ning võimalusel selliste tehingute teostamata jätmine.

Hoolsusmeetmete kohaldamisel, kui seda ei tehta infotehnoloogiliste vahendite abil, tehakse tuvastamisele kuuluvad asjaolud kindlaks kliendi poolt esitatud originaaldokumentide alusel. Kui originaaldokumenti ei ole võimalik saada, võib kasutada notariaalselt tõestatud või notariaalselt või ametlikult kinnitatud dokumente, s.h. advokaadi poolt kinnitatud dokumente. Dokumendi koopiale ei tohi tugineda, kui tekib kahtlus koopia vastavuses originaalile.

KLIENDI TUVASTAMINE
1 Isikusamasuse peab tuvastama kõigil isikutel ja nende esindajatel, kes astuvad VirtualMoneyga ärisuhtesse. Kliendi või tema esindaja isiklik tundmine või tema avalik tuntus ei välista Juhendiga kehtestatud tuvastamiskohustuse täitmist.
2 Kliendiga ärisuhtesse asumisel tuleb füüsilisest isikust klient või juriidilisest isikust kliendi esindaja tuvastada infotehnoloogiliste vahendite abil. Isikusamasuse tuvastamiseks ja kontrollimiseks kasutatakse pangalinki, ID-kaarti, mobiil-ID'd, Smart-ID-d vms, kokkulepitud sidevahendeid, millele ligipääs on vaid Kliendil või Klienti esindajal (nt @eesti.ee vm ainukasutatav e-post), või/ja VirtualMoney poolt kehtestatud unikaalseid kasutajatunnuseid ning autentimisvahendeid. Kui nimetatud dokumente või e-identimise vahendeid ei ole, siis peab füüsilise isiku tuvastamisel klient esitama VirtualMoneyle koopia fotoga isikut tõendavast dokumendist. Enne iga tehingu tegemist peab Personali liige veenduma eelnevalt isiku/esindaja isikusamasuses ning esindusõiguse olemasolus.

3 Lisaks punktis 3.2. toodule tuleb kliendil esitada (e-posti teel või vahetusplatvormi ankeedis, kui ei ole allpool märgitud teisiti) järgmised isikuandmed:

1 Füüsilisest isikust resident:
1. ees- ja perekonnanimi;
2. isikukood;
3. isikut tõendava dokumendi nimetus, number, väljaandmise aeg, väljaandja nimetus;
4. elukoha aadress;
5. kutse- või tegevusala;
6. kontakttelefoni number, e-posti aadress.

2 Juriidilisest isikust resident:
1. juriidilise isiku nimi ja registrikood;
2. postiaadress;
3. tegevusala;
4. kontakttelefoni number, e-posti aadress;
5. esindaja ees- ja perekonnanimi, isikukood või sünniaeg (kui ei nähtu registrikaardilt);
6. esindusõiguse alus, volitatud isiku korral notariaalselt kinnitatud volitus
Juriidilise isiku esindaja poolt esitatud andmete õigsust ja esindusõiguse olemasolu kontrollitakse Tartu Maakohtu registriosakonnast .

3 Füüsilisest isikust mitteresident:
1. ees- ja perekonnanimi;
2. isikukood ja sünniaeg ning koht;
3. reisidokumendi nimetus, number, väljaandmise aeg, väljaandja nimetus;
4. elukoha aadress ja postiaadress;
5. asukoha aadress kontakti loomisel;
6. kutse- või tegevusala;
7. teave selle kohta, kas isik täidab või on täitnud avaliku võimu olulisi ülesandeid või on avaliku võimu oluliste ülesannete täitja lähedane kaastöötaja või perekonnaliige (st riikliku taustaga isik RahaPTS mõttes);
8. kontakttelefoni number ja e-posti aadress;
9. notariaalselt kinnitatud koopia reisidokumendi pildiga leheküljest ning vajadusel ka viisast või ajutisest elamisloast. Koopia tuleb saata postiga.

4 Juriidilisest isikust mitteresident:
1. juriidilise isiku nimi ja registrikood;
2. asukoha riik, asukoha riigi registri nimetus ja veebiaadress; vastavad registrite ajakohased väljatrükid,

SRÜ ja offshore riikidest ka maksuameti tõendid;
3. tegeliku kasusaaja andmed;
4. postiaadress;
5. tegevuskoha aadress;
6. tegevusala;
7. pangakonto(de) andmed;
8. kontakttelefoni number ja e-posti aadress;
9. esindaja ees- ja perekonnanimi, isikukood või sünniaeg (kui ei nähtu registrikaardilt);
10. esindusõiguse alus, volitatud isiku korral notariaalselt kinnitatud või sellega võrdväärses korras kinnitatud esindusõigust tõestav dokument, mis on legaliseeritud või kinnitatud legaliseerimist asendava tunnistusega (apostille'iga), kui välislepingust ei tulene teisti. Eelnimetatud dokumentidest tehtud notariaalselt kinnitatud koopiad tuleb saata postiga.

4 Juhul, kui kliendi poolt teostatava tehingu väärtus ületab 15 000 eurot, siis peab klient esitama VirtualMoneyle koopia või väljavõtte tema elukoha/asukoha kommunaalarvest, mis ei või olla vanem kui kolm kuud ja millele on märgitud kliendi nimi ja aadress.

5 Kogutud teabe kontrollimiseks tuleb Personali töötajal kasutada kättesaadavaid registreid ja Internetis sisalduvat teavet. Kõrgema riskiastmega ärisuhte puhul võib nõuda soovitajate andmeid või täiendavaid dokumente. Vajadusel küsib Personali liige üksikasjalikumat teavet äriühingu tegevuse, loodava ärisuhte eesmärgi kohta. Vähimagi kahtluse korral küsitletakse klienti kogutud andmete põhjal kontakttelefoni kaudu.

6 Kestvussuhte korral kontrollitakse ja vajadusel uuendatakse kogutud andmeid vähemalt üks kord kahe aasta jooksul.

7 Isikusamasuse tuvastamiseks saadud isikut paberkandjal tõendava dokumendi koopiale märgib isikut tuvastanud VirtualMoney töötaja oma nime, isikusamasuse tuvastamise kuupäeva ning oma allkirja.

Isikusamasuse tuvastamiseks saadud andmed tuleb registreerida VirtualMoney arvutisüsteemis.

4. FÜÜSILISEST ISIKUST KLIENDI RISKIPROFIILI VÄLJASELGITAMINE, RISKIKATEGOORIA MÄÄRAMINE

Personali liige on kohustatud välja selgitama füüsilisest isikust kliendi profiili ja määrama riskikategooria.

Füüsilisest isikust kliendi riskikategooria määramisel lähtutakse kliendi residentsusest ja tegelikest kasusaajatest. Mitteresidentidest füüsiliste isikute riskikategooria määramisel arvestatakse lisaks, kas klient on riikliku taustaga isik/ tema perekonnaliige/ tema lähedane kaastöötaja. Kui klient on riikliku taustaga isik/ tema perekonnaliige/ tema lähedane kaastöötaja, siis kuulub ta automaatselt III kategooriasse.

4.1 I kategooria - madal riskikategooria:

residendist või mitteresidentist füüsiline isik, kes on ise tegelik kasusaaja;

4.2 II kategooria - keskmine riskikategooria:

mitteresidendist füüsiline isik, kes on ise tegelik kasusaaja ja kes ei ole riikliku taustaga isik/tema perekonnaliige/ tema lähedane kaastöötaja;

residendist füüsiline isik, kes ei ole ise tegelik kasusaaja.

4.3 III kategooria - kõrge riskikategooria:

residendist ja mitteresidendist füüsiline isik, kes on riikliku taustaga isik/tema perekonnaliige/ tema lähedane kaastöötaja;

mitteresidendist füüsiline isik, kes ei ole ise tegelik kasusaaja.

4.4 Riskikategooria määrab Personali liige kliendisuhte alustamisel ning kliendisuhte kestel, lisades vastava kategooria kliendi andmetele.

4.5 Kui klient kuulub III riskikategooriasse, tuleb rakendada tugevdatud hoolsusmeetmeid (p 10)**.**

4.6 Kui luuakse ärisuhe kõrge riskikategooriaga (III kategooria) kliendiga, siis informeerib Personali liige sellest kohe Kontaktisikut Juhatuse poolt määratud e-posti või telefoni teel.

5. JURIIDILISEST ISIKUST KLIENDI TEGEVUSPROFIILI VÄLJASELGITAMINE, RISKIKATEGOORIA MÄÄRAMINE

5.1 VirtualMoney Personali liige on ärisuhte loomisel kohustatud välja selgitama juriidilisest isikust kliendi tegevusprofiili ning määratlema juriidilisest isikust kliendi riskiprofiili.

2 Riskikategooria määramisel lähtutakse juriidilise isiku asukoha maast, tegevusalast ning juhtimisorganite ja juriidilise isiku omanike struktuuri läbipaistvusest.

1 I kategooria - madal riskikategooria:

Eesti Vabariigis registreeritud juriidiline isik, kelle tegevusvaldkond on määratletud (v.a kalatööstus, ehitus ja remont, kütuse hulgikaubandus ja hoiustamine, kütuse jaekaubandus, puidu hulgikaubandus, valuuta-ja /või maksevahendus, hasart-, õnnemängud, kasiino);

Euroopa Liidu liikmesriigis või Norras, Islandil, Šveitsis registreeritud juriidiline isik, kelle aktsiad on avalikult noteeritud ning äriühingu tegevusalaks ei ole kalatööstus, ehitus ja remont, kütuse hulgikaubandus ja hoiustamine, kütuse jaekaubandus, puidu hulgikaubandus, valuuta- ja/või maksevahendus, hasart-, õnnemängud, kasiino;

automaatselt kuuluvad madalasse riskikategooriasse valitsusasutused, kindlustusasutused ja pensionifondid, residendist krediidiasutused, residendist kohalik omavalitsus, residendist keskpank, residendist riiklik sotsiaalkindlustusfond, keskvalitsus mitteresident, kindlustusasutused ja pensionifondid mitteresident, kohalik omavalitsus mitteresident, riiklik sotsiaalkindlustusfond mitteresident, eraettevõte tütar resident, finantsasutus tütar resident/mitteresident, kindlustusasutus ja pensionifondid resident.

2 II kategooria - keskmine riskikategooria:

Euroopa Liidu liikmesriigis või Norras, Islandil, Šveitsis registreeritud juriidiline isik, kelle aktsiad ei ole avalikult noteeritud ning nende tegevusalaks ei ole kalatööstus, ehitus ja remont, kütuse hulgikaubandus ja hoiustamine, kütuse jaekaubandus, puidu hulgikaubandus, valuuta- ja/või maksevahendus, hasart-, õnnemängud, kasiino;

Eestis registreeritud juriidiline isik, kelle tegevusalaks on kalatööstus, ehitus ja remont, kütuse hulgikaubandus ja hoiustamine, kütuse jaekaubandus, puidu hulgikaubandus, valuuta- ja/või maksevahendus, hasart-, õnnemängud, kasiino;

Euroopa Liidu liikmesriigis või Norras, Islandil, Šveitsis registreeritud juriidiline isik, kelle aktsiad on avalikult noteeritud ning äriühingu tegevusalaks on kalatööstus, ehitus ja remont, kütuse hulgikaubandus ja hoiustamine, kütuse jaekaubandus, puidu hulgikaubandus, valuuta- ja/või

maksevahendus, hasart-, õnnemängud, kasiino;
kolmandates riikides ja Liechtensteinis registreeritud juriidiline isik, kelle aktsiad on avalikult noteeritud ja kelle tegevusalaks ei ole kalatööstus, ehitus ja remont, kütuse hulgikaubandus ja hoiustamine, kütuse jaekaubandus, puidu hulgikaubandus, valuuta- ja/või maksevahendus, hasart-, õnnemängud, kasiino.

3 III kategooria - kõrge riskikategooria:

kolmandates riikides ja Liechtensteinis registreeritud juriidiline isik (v.a p 5.2.2 alapunkt iv);
Euroopa Liidu liikmesriigis või Norras, Islandil, Šveitsis registreeritud juriidiline isik, kelle aktsiad ei ole avalikult noteeritud ning nende tegevusalaks on kalatööstus, ehitus ja remont, kütuse hulgikaubandus ja hoiustamine, kütuse jaekaubandus, puidu hulgikaubandus, valuuta- ja/või maksevahendus, hasart-, õnnemängud, kasiino.

4 Kui klient kuulub III riskikategooriasse tuleb rakendada tugevdatud hoolsusmeetmeid (p 10).
5 Riskikategooria määrab VirtualMoney Personali liige kliendisuhte alustamisel ning kliendisuhete kestel, lisades vastava kategooria kliendi andmetele.
6 Kui luuakse ärisuhe kõrge riskikategooriaga (III kategooria) kliendiga, siis informeerib töötaja sellest kohe Kontaktisikut Juhatuse poolt määratud e-posti või telefoni teel. Lisaks tuleb informeerida Kontaktisikut, kui äriühingu tegevusala on seotud relvatööstuse, relvade müügi või vahendamisega.

KLIENDISUHTE KESTEL ISIKU TUVASTAMINE

1 Kliendisuhte ajal on nõutav kliendi isikusamasuse tuvastamine.
2 VirtualMoneyl on õigus tehingute teostamine peatada või lõpetada, kui ärisuhte kestuse ajal ilmnenud rahapesu kahtluse puhul ei esita klient dokumente või andmeid, mis sellise kahtluse ümber lükkaksid. Hinnangu rahapesu kahtluse osas annab ja otsuse tehingute peatamiseks või lõpetamiseks teeb VirtualMoney juhatus või Kontaktisik.

RIIKLIKU TAUSTAGA ISIKU TUVASTAMINE JA TEHINGUTE TEGEMINE

1 Riikliku taustaga isikuteks on RahaPTS § 3 p-s 11 loetletud isikud, kes jagunevad siseriiklikke ja rahvusvaheliste organisatsioonide poolt antud ülesandeid täitvateks riikliku taustaga isikuteks.
2 Riikliku taustaga isikute kindlakstegemise eest VirtualMoney klientide ja potentsiaalsete klientide seast vastutab Kontaktisik, kui VirtualMoney juhatus ei ole määranud selleks muud isikut.
3 Riikliku taustaga isiku tuvastamine on võimalik:
1 klienti küsitledes;
2 olemasolevaid avalikke või tasulisi andmebaase2 ja interneti otsingumootoreid kasutades; või
3 tehes päringu või kontrollides andmeid kliendi asukohamaa ametiasutuste veebilehtede kaudu.
4 Riikliku taustaga isikuga ärisuhte loomise peab otsustama VirtualMoney juhatus või Kontaktisik. Kui kliendiga on ärisuhe loodud ja klient osutub hiljem või muutub riikliku taustaga isikuks, siis on vajalik Kontaktisiku kirjalik või kirjalikku taasesitamist võimaldavas vormis informeerimine.

VÄIKESE JA KÕRGE RISKIASTMEGA TEHINGUD

1 Tehingu teostamisel peab VirtualMoney Personali liige hindama rahapesu ja terrorismi rahastamise riski ning valima kohased hoolsusmeetmed vastavalt Juhendile ning neid rakendama.
2 Rahapesu ja terrorismi rahastamise riski hindamisel võetakse arvesse kliendi riski ja tehingu riski.
3 Tehinguga seotud riski käsitletakse väikesena, kui samaaegselt esinevad järgmised asjaolud:
1 tehingust saadav kasu ei ole kliendi poolt realiseeritav enne ühe aasta möödumist tehingu tegemisest;
2 tehing ei toimu kiirmaksena;
3 sõlmitud leping ei sätesta kliendi tagasiostuklauslit.
4 Väikese riski kriteeriumitena «Rahapesu ja terrorismi rahastamise tõkestamise seaduse» § 34 lõike 2 punktides 1 kuni 6 nimetatud isikute või klientide isikusamasuse tuvastamisel ja kontrollimisel käsitletakse järgnevaid samaaegselt esinevaid asjaolusid:
1 kliendi isikusamasuse tuvastamine on võimalik avalikult kättesaadava teabe alusel;
2 kliendi omandi- ja kontrollistruktuur on läbipaistev ja püsiv;
3 kliendi tegevus ja tema raamatupidamistavad on läbipaistvad;
4 klient on aruandekohustuslik ja kontrollitav Eesti või Euroopa Majanduspiirkonna lepinguriigi täidesaatva riigivõimu asutuse, muu avalikke ülesandeid täitva asutuse või Euroopa Ühenduse asutuse poolt.

5 Kliendi riski käsitletakse kõrgena, kui klient on:
1 kantud ÜRO või Euroopa Liidu nimekirja, mida peetakse isikute kohta, kelle suhtes kehtivad rahvusvahelised finantssanktsioonid3;
2 isik, kelle suhtes on VirtualMoneyle elnevalt teada kahtlus, et isik võib olla seotud rahapesu või terrorismi rahastamisega.

6 Tehinguga seotud riski käsitletakse kõrgena, kui:
1 Tehingut soovib teha kliendi esindaja, kes ei suuda piisavalt veenvalt selgitada raha päritolu;
2 Tehingut soovib teha klient, kelle suhtes on VirtualMoneyle eelnevalt teada kahtlus, et ta võib olla seotud rahapesu või terrorismi rahastamisega;
3 tehingut soovitakse teha sularahalise tasumise teel;
4 tehingu tegemisel taotletakse rahakande tegemist kolmandale isikule või kolmanda isiku kaudu;
5 esinevad tehingud või toimingud, mis vastavad käesoleva Juhendi lisas 2 ja 3 nimetatud tunnustele.
7 Kõrge riskiastmega tehingute osas tuleb rakendada hoolsusmeetmeid tugevdatud korras.
8 Ebahariliku tehingu, toimingu või asjaolu ilmnemisel on Personali liikmel kohustus analüüsida ja võrrelda tehingu asjaolusid rahapesu ja terrorismi rahastamise kahtlusega tehingute tunnustega. Personali liikmel on kohustus kontrollida vara legaalset päritolu enne tehingu sooritamist vähemalt juhul, kui tehing on senist kliendisuhet arvestades ebaharilik rahapesu või terrorismi rahastamise kahtlusega.
9 Hoolsusmeetmeid tuleb rakendada tugevdatud korras samuti siis, kui madala riskiga tehingute või klientide osas tekib kahtlus rahapesus või terrorismi rahastamises.

HOOLSUSMEETMETE KOHALDAMINE LIHTSUSTATUD KORRAS
1 Hoolsusmeetmeid võib kohaldada lihtsustatud korras järgmistel tingimustel:
1 RahaPTS § 34 lg 2 p 1-6 nimetatud isikute suhtes; või
2 kui kliendiga on sõlmitud kirjalik kestvusleping; või
3 kui Personalil ei teki kahtlust kliendi esitatud andmete õigsuses või kliendi teovõimes või õigusvõimes; ja
4 kui Personalil ei teki tehinguga seonduvalt rahapesu või terrorismi rahastamise kahtlust; ja
5 kui tehingu või kliendi riski saab käsitleda madalana; ja
6 kui kliendiga on varasem ärisuhe, mis on loodud enne käesoleva Juhendi kehtestamist või klient on identifitseeritud pärast käesoleva Juhendi kehtestamist vastavalt Juhendile

2 Lihtsustatud hoolsusmeetmete kohaldamisel:
1 Isikud tuvastatakse vastavalt käesoleva Juhendi punktile 3;
3 Kui Personali liikmel tekib lihtsustatud hoolsusmeetmete kohaldamisel siiski kahtlus kliendi esitatud andmete õigsuses, siis teostab Personal täiendava kontrolli. Täiendava kontrolli käigus helistab VirtualMoney töötaja kliendile ja täpsustab kliendi andmeid ning võib küsida muid kontrollküsimusi4.Kui kontrolli ei ole võimalik läbi viia või kontrolli käigus selgub, et klient ei oska kontrollküsimustele vastata, siis tehingut kliendiga ei tehta.
4 Keelatud on hoolsusmeetmete kohaldamine lihtsustatud korras juhul, kui ükskõik millises kliendiga suhtlemise etapis on tekkinud rahapesu või terrorismi rahastamise kahtlus. Kui lihtsustatud hoolsusmeetme kohaldamise käigus tekib Personali liikmel rahapesu või terrorismi rahastamise kahtlus, teatab Personali liige sellest Kontaktisikule telefoni teel või e-posti teel.

HOOLSUSMEETMETE KOHALDAMINE TUGEVDATUD KORRAS
1 VirtualMoney Personali liige kohaldab hoolsusmeetmeid tugevdatud korras, kui olukorra olemusega kaasneb suur rahapesu või terrorismi rahastamise risk. Tugevdatud hoolsusmeetmeid peab kohaldama, kui:
tehingus osaleva kliendi isikusamasus on tuvastatud ja esitatud teave kontrollitud temaga samas kohas viibimata; ja
isikusamasuse tuvastamisel või esitatud teabe kontrollimisel tekib kahtlus esitatud andmete tõelevastavuses või dokumentide ehtsuses või tegeliku kasusaaja või tegelike kasusaajate tuvastamises; ja
Tehingus osalev klient on teise Euroopa Majanduspiirkonna lepinguriigi või kolmanda riigi riikliku taustaga isik, tema perekonnaliige või lähedane kaastöötaja; ja

esinevad kõrgema riskiastmega tehingute tunnused.

Tugevdatud hooldusmeetme kohaldamise kohustuse korral kohaldatakse lisaks tavapärastele hoolsusmeetmetele vähemalt ühte järgmistest tugevdatud hoolsusmeetmetest:
isikusamasuse tuvastamine ja esitatud teabe kontrollimine lisadokumentide, andmete või teabe põhjal, mis pärinevad usaldusväärsest ja sõltumatust allikast või Eestis äriregistrisse kantud krediidiasutuselt või välisriigi krediidiasutuse filiaalilt või krediidiasutuselt, kes on registreeritud või kellel on tegevuskoht Euroopa Majanduspiirkonna lepinguriigis või riigis, kus kehtivad võrdväärsed nõuded rahapesu ja terrorismi rahastamise tõkestamise seadusega, ja kui selles krediidiasutuses on isiku isikusamasus tuvastatud isikuga samas kohas viibides; ii) lisameetmete võtmine esitatud dokumentide ehtsuses ja nendes sisalduvate andmete õigsuses veendumiseks, muu hulgas nende notariaalse või ametliku kinnitamise nõudmine või andmete õigsuse kinnitamine dokumendi välja andnud punktis i) nimetatud krediidiasutuse poolt; iii) tehinguga seotud esimese makse tegemine konto kaudu, mis on avatud tehingus osaleva isiku nimel krediidiasutuses, kes on registreeritud või kelle tegevuskoht on Euroopa Majanduspiirkonna lepinguriigis või riigis, kus kehtivad võrdväärsed nõuded rahapesu ja terrorismi rahastamise tõkestamise seadusega.
2 Ebahariliku tehingu, toimingu või asjaolu ilmnemisel on Personali liikmel kohustus analüüsida ja võrrelda tehingu asjaolusid rahapesu ja terrorismi rahastamise kahtlusega tehingute tunnustega. Personali liikmel on kohustus kontrollida vara legaalselt päritolu enne tehingu sooritamist vähemalt juhul, kui tehing on senist kliendisuhet arvestades ebaharilik rahapesu või terrorismi rahastamise kahtlusega.
3 Kõrgema riskiastmetega tehingute osas tuleb võrrelda tehingu kohta ilmnenud asjaolusid rahapesu või terrorismi rahastamise kahtlusega tehingute tunnustega ning teavitada rahapesu ja terrorismi rahastamise kahtlusest Kontaktisikut.

ÄRISUHTE JÄLGIMINE

12.1. VirtualMoney juhatuse poolt määratud Personali liige kohustub regulaarselt kliendiga ärisuhet jälgima, kindlustamaks, et teostatavad tehingud vastavad tema äri- ja riskiprofiilile. Selleks kohustub Personali liige:
Regulaarselt jälgima tehingus kasutatavate rahasummade suurust ning tehingute sagedust ning vajadusel välja selgitama ärisuhtes ja/või tehingutes kasutava vara päritolu; regulaarselt kontrollima kliendi juriidilist staatust (õigusvõime olemasolu), finantsolukorda, tegevusala, omandikuuluvust puudutavat informatsiooni (tegelikke kasusaajaid).
12.2. Täiendavalt jälgib Personali liige vähemalt üks kord aastas:
Kliendi riski hindamist;
Kliendi asukoha riigi riski hindamist;
liitriski ehk kombineeritud riski hindamist.

Kliendiriski (riskifaktorid tulenevad kliendi isikust) puhul tuleb arvestada:
isiku õiguslikku vormi, juhtimisstruktuuri (sh usaldusfondid, seltsingud või muud sellised lepingulised õiguslikud üksused, juriidilised isikud, millel on esitajaaktsiad);
äriühingu omandistruktuuri, eriti neid, millel puudub ilmselge äriline põhjendus ja mis võib lõpliku kasusaaja varjamise lihtsamaks muuta;
isiku tegevuse valdkonda (kliendid, kes on seotud äritegevusega, mis hõlmab suurte sularahasummade käitlemist nagu valuutavahetuspunktid, rahaveoga tegelejad, kõrge väärtusega kaupade vahendajad, kasiinod, kihlveo ja muud hasartmängu tegevustega seotud äriühingud, kes saavad regulaarselt makseid sularahas);
kas tegemist on riikliku taustaga isikuga/ tema perekonnaliikme või lähedase kaastöötajaga (klient või tegelik kasusaaja);
1) kas isiku esindajaks on juriidiline isik;
isiku residentsust, sh kas tegemist on *offshore* piirkonnas registreeritud isikuga (maksuvabad ja madala maksumääraga territooriumid, näiteks Maksu- ja Tolliameti veebilehel toodud vastavate andmete alusel http://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest ;
kliendi, tema koostööpartnerite, omanike, esindajate jms isikutega suhtlemise kogemusest tulenevad

asjaolusid (nt varasema ärisuhte käigus tuvastatud kahtlased tehingud, kliendi kahtlane käitumine, nõutud dokumentide mitteesitamine);
2) tegevuse kestvus, ärisuhete iseloom.

Riigirisk, mille riskifaktorid tulenevad erinevate riikide õiguskeskkonna erinevustest, kuritegevuse tasemest ning sellest, kas selle riigi või selle riigi isikute suhtes on rakendatud või rakendatakse rahvusvahelisi sanktsioone.
Riskantsemad on sealhulgas riigid :
kelle suhtes on kehtestatud rahvusvahelised sanktsioonid või embargod;
kellel puuduvad piisavad rahvusvaheliste standarditega kooskõlas olevad rahapesualased seadused ja määrused;
kelle puhul on kindlaks tehtud terrorismi rahastamine või toetamine;
kelle puhul on kindlaks tehtud märkimisväärne korruptsiooni või organiseeritud kuritegevuse või muu kuritegevuse (sh narkokuritegevuse) tase;
mis on maksuvabad ja madala maksumääraga, *offshore* finantskeskused.

Liitriskid ehk kombineeritud riskid
Erilist tähelepanu tuleb Personali liikmel pöörata olukordadele, mis viitavad kõrgemale riskile mitmes ülalnimetatud riskigrupis.
1 Eelnimetatud analüüsi tulemused edastab Personali liige kirjalikult kontaktisikule.

ANDMETE KOGUMINE, KONTROLLIMINE, SÄILITAMINE JA UUENDAMINE
1 Andmete kogumine
1 Kliendi esmakordne tuvastamine toimub vastavalt Juhendi punktis 3 sätestatud korrale.
2 Kliendi igakordsel tuvastamisel registreerib VirtualMoney arvutisüsteemis/vahetusplatvormis:
1 kliendi nime, isikukoodi, elukoha5, tegevus- või kutseala; ja
2 informatsiooni kliendi esitatud andmete ja Juhendiga nõutud muude andmete ning dokumentide kontrollimise kohta.
2 Andmete kontrollimine
1 Isikut tõendava dokumendi kehtivust tuleb kahtluse korral kontrollida Politsei- ja Piirivalveameti kodulehelt http://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/index.dot.
3 Andmete säilitamine
1 Kliendi ja tema esindaja esitatud andmeid, kliendi ja tema esindaja isikut tõendava dokumendi koopiat, Juhendi ja RahaPTS alusel kliendilt nõutud muid dokumente säilitatakse digitaalselt VirtualMoney arvutisüsteemis(serveris) või paberkandjal VirtualMoney juhatuse asukohas või muus Juhatuse poolt määratud kohas vähemalt 5 aastat pärast kliendiga lepinguliste suhete lõppemist.
2 Tehinguandmeid, mis on seotud rahapesu või terrorismi rahastamise kahtlusega6, säilitatakse Kontaktisiku poolt viisil, et teistel VirtualMoney teistel Personali liikmetel puudub neile Kontaktisiku loata ligipääs.
3 Andmeid, mis on seotud rahapesu või terrorismi rahastamise kahtlusega, säilitatakse punktis 14.4.1. toodud tähtaja lõpuni, v.a. juhul kui tehinguga seotud asjaolude uurimine ei ole selleks ajaks lõpetatud, millisel juhul säilitatakse kliendi- ja tehinguandmeid kuni kinnituse saamiseni uurimise lõpetamise kohta.
4 Andmete ja dokumentide uuendamine, sisekontrolli meetmed
1 Vähemalt kord kahe aasta jooksul tuleb läbi viia andmete uuendamine. Andmete uuendamise käigus koostatakse Juhatuse poolt määratud Personali liikme poolt raport, mis peab sisaldama riske, mis seoses äritegevusega on kindlaks tehtud, riskide maandamiseks kehtestatud kontrollimeetmete kirjeldust ja puuduste korral seda, kuidas neid käsitleda. Raport esitatakse Kontaktisikule ja Juhatusele.
2 Personali liige, kes vastutab kliendisuhete eest (kliendihaldur) pöörab oluliselt suuremat tähelepanu riskianalüüsi tulemusena tuvastatud kõrge riskikategooriaga (III kategooria) klientide andmete kontrollimisele ja äritegevuse tundmisele. Lisaks iga-aastasele analüüsile peab kliendihaldur pidevalt hindama klientide äritegevusega seotud võimalikke rahapesu ja terrorismi rahastamise riske ning on kohustatud koheselt teavitama riskiprofiili muutumisest Kontaktisikut.
3 Kontaktisik koostab raporti tulemustele tuginedes üksikasjaliku monitooringu plaani, mille alusel Kontaktisik monitoorib riskantsemaid tehinguid ja jälgib kliendiprofiili.

4 Uuendatud andmed sisestab Kontaktisik koheselt VirtualMoney arvutisüsteemi, milles olevad andmed on kättesaadavad kõigile teistele Personali liikmetele. Kontaktisik korraldab juhtkonna kaasamise andmete uuendamise ja analüüsi protsessi ja võtab raporti tulemused aluseks kogu riskide hindamise protsessis, tegevusplaanide koostamisel ja juhtide nõustamisel riskide vähendamiseks.

PIIRANGUD TEHINGUTE TEOSTAMISEL

1 VirtualMoneyl ega Personali liikmel ei ole lubatud:
1 Arveldada sularahas;
2 Teha tehingut kliendiga, kelle isikusamasus ei ole tuvastatud Juhendi kohaselt;
3 Teha tehinguid anonüümsete või fiktiivsete isikutega, kes kasutavad teisi nimesid või valenime.

2 VirtualMoney ja Personali liige keelduvad tehingu tegemisest kliendiga:
1 kelle esitatud dokumentide või muu informatsiooni alusel tekib kahtlus dokumentide või andmete õigsuses ning klient ei selgita adekvaatselt kahtlusi tekitanud asjaolusid;
2 kelle isikusamasust või esindaja volituste õigsust ei ole võimalik tuvastada või kontrollida;
3 kelle elukohta või kutse- või tegevusala või tegevusprofiili ei ole võimalik tuvastada;
4 kes osutuvad olevat rahvusvaheliste sanktsioonide rakendamise nimekirjas või keda on rahapesu andmebüroo poolt tuvastatud kui rahapesu või terrorismi rahastamise kahtlusega tehingute sooritajat, juhul kui selline informatsioon rahapesu andmebüroo poolt avalikustatakse;
5 kelle puhul tekib muudest asjaoludest tulenevalt kahtlus, et isik võib olla seotud rahapesuga või terrorismi rahastamisega.

3 Tehingu tegemisest keeldumine registreeritakse VirtualMoney arvutisüsteemis.

TEHINGUTE JÄLGIMINE JA ANALÜÜSIMINE

1 VirtualMoney Personal peab tehingute teostamisel jälgima ning analüüsima, kas tehing või Klient ei ole seotud rahapesu või terrorismi rahastamisega. Rahapesu või terrorismi rahastamise kahtlusega ning ebaharilike tehingute tunnuste loetelu on toodud käesoleva Juhendi lisades 2 ja 3 (Rahapesu andmebüroo juhend „**Rahapesu andmebüroo soovituslik juhend rahapesu kahtlusega tehingute tunnuste kohta**“ ja Rahapesu andmebüroo juhend „**Rahapesu andmebüroo soovituslik juhend terrorismi rahastamise kahtlusega tehingute tunnuste kohta**“).
2 Kui kliendi tegevus viitab rahapesule või terrorismi rahastamisele, tuleb kliendilt küsida lisainformatsiooni selgitamaks välja raha päritolu. Lisainformatsiooni võib küsida suuliselt ja/või kirjalikult, kuid saadud teave tuleb registreerida ja siduda VirtualMoney arvutisüsteemis kliendi nimega.
3 Kontaktisik analüüsib vajadusel klientide tehinguid, selgitamaks tehingu võimalikku seotust rahapesuga või võimalust raha mittelegaalseks päritoluks.
4 Rahapesu ja terrorismi rahastamise riskihindamise juhtimise eest on vastutav Kontaktisik, kes peab regulaarselt analüüsima, kas VirtualMoney äritegevuses võib esineda Juhendis käsitlemata rahapesu ja terrorismi rahastamise riskifaktoreid.
5 Uute riskifaktorite tuvastamisel peab Kontaktisik koostama:
1 selgituse, kuidas VirtualMoneyi äritegevuses tuleb uute riskifaktoritega arvestada ja riske maandada; ning
2 ettepaneku Juhendi täiendamiseks ning uue Juhendi projekti.

KONTAKTISIK

1 Kontaktisik on aruandekohustuslik juhatuse ees. Kontaktisiku kontaktandmetest ja nende muutumisest teavitab VirtualMoney juhatus rahapesu andmebürood viivitamatult. Kontaktisikuks on VirtualMoney juhatuse liige, kui VirtualMoney ei ole määranud Kontaktisikuks muud Personali liiget. Kui Kontaktisikuks on juhatuse liige, kes on ainus juhatuse liige, on Kontaktisik aruandekohustuslik osanike ees.

2 Kontaktisikul on õigus nõuda kõigilt Personali liikmetelt Juhendis sätestatud kohustuste täitmist ja võimaliku rikkumise viivitamatut lõpetamist.

3 Kontaktisiku ülesanneteks on:

1 ebaharilikele või rahapesu või terrorismi rahastamise kahtlusega tehingutele viitava teabe kogumise korraldamine, teabe analüüsimine ja arhiveerimine;
2 teabe edastamine rahapesu andmebüroole rahapesu või terrorismi rahastamise kahtluse korral;
3 ÜRO ja Euroopa Liidu finantssanktsioonide nimekirjas olevate isikute nimede kontrollimine VirtualMoney klientide ning potentsiaalsete klientide hulgast;
4 Juhendi RahaPTS-ile ja muudele õigusaktidele vastavuse kontrollimine vähemalt 1 kord aastas ning vajadusel muudatusettepanekute tegemine juhatusele Juhendi muutmiseks;
5 Juhendi täitmiseks ning informatsiooni õigeaegseks edastamiseks vajalike tehniliste vahendite olemasolu kontrollimine;
6 Juhendi ning õigusaktidest tulenevate rahapesu ja terrorismi rahastamise tõkestamise alaste nõuete täitmise kontrollimine ning kontrolli tulemuste analüüsimine ja juhatuse teavitamine Juhendi täitmisest;
7 ettepanekute tegemine rahapesu ja terrorismi rahastamise riski hindamise ja juhtimise kohta;
8 töötajate rahapesu ja terrorismi rahastamise tõkestamise alase koolitusvajaduse väljaselgitamine ja Personali koolitamine;
9 rahapesu andmebüroo teavitamine kliendi isikusamasuse tuvastamise kohustuse kolmandale isikule edasiandmisest ;
10 rahapesu andmebüroo ja teiste ametiasutuste poolt tehtud ettekirjutuste täitmise tagamine VirtualMoney poolt;
11 riikliku taustaga isikute kindlakstegemine klientide seast;
12 muude kohustuste täitmine, mis on seotud RahaPTS nõuete täitmisega.
4 Kontaktisikul on oma ülesannete täitmiseks õigus tutvuda ärisuhte loomise aluseks või eelduseks olevate dokumentide ja muu informatsiooniga.

SISEKONTROLLI MEETMED
1 VirtualMoney poolt rahapesu ja terrorismi rahastamise tõkestamise meetmete täitmist kontrollib Kontaktisik käesolevas Juhendis ja selle lisades, samuti õigusaktides sätestatud ülesandeid täites.
2 Täiendavalt viib Kontaktisik vähemalt üks kord aastas läbi sisekontrolli, mille käigus kontrollib:
Hoolsuskohustuse täitmise toimingute nõuetele vastavust käesolevale juhendile;
registreeringute nõuetele vastavust käesolevale Juhendile;
rahapesu ja terrorismi rahastamise tõkestamise muude nõuete täitmist;
Juhendi alusel läbi viidavate ärisuhte jälgimise toimingute vastavust käesolevale Juhendile,
Juhendi vastavust õigusaktidele ja pädevate ametiasutuste juhenditele;
Töötajate koolitusvajadust;
3 Sisekontrolli läbiviimise kohta koostab Kontaktisik kirjaliku raporti. Raportis märgitakse:
Kontrolli eesmärk;
Kontrolli teostamise aeg
Kontrolli teostaja nimi ja ametinimetus
Läbiviidud kontrolli kirjeldus
Kontrollimise tulemuste analüüs või teostatud kontrolli üldised järeldused ja analüüs
Puuduste esinemisel puuduste kirjelduse ja sellega seotud riskid.
Puuduste kõrvaldamise aeg, puuduste kõrvaldamise soovitatavad meetmed ja järelkontrolli teostamise aja. Järelkontrolli teostamisel lisab Kontaktisik kontrolliaruande juurde järelkontrolli tulemuste analüüsi ning puuduste kõrvaldamiseks kasutatud meetmete loetelu, näidates ära puuduste kõrvaldamiseks kulunud tegeliku aja.
4 Jooksva ja iga-aastase täiendava kontrolli läbiviimisel on Kontaktisikul õigus:
jälgida Personali tööd ja saada selleks vajalike tehnilisi vahendeid;
Nõuda kohest rahapesu ja terrorismi rahastamise tõkestamise alaste nõuete rikkumise lõpetamist;
Teha ettepanekuid kontrollimise käigus ilmnenud puuduste kõrvaldamiseks, s.h. protseduurireeglite muutmiseks ja täiendamiseks.

TEAVITAMISKOHUSTUSE TÄITMINE
1 Personali liige teavitab Kontaktisikut iga järgmise olukorra esinemisest:
1 igast tehingust, kus rahaline kohustus üle 32 000 euro või võrdväärne summa muus vääringus täidetakse sularahas, sõltumata sellest, kas tehing tehakse ühe maksena või mitme omavahel seotud maksena;

2 rahapesu või terrorismi rahastamise kahtlusega tehingust. Rahapesu või terrorismi rahastamise kahtlusega ning ebaharilike tehingute tunnuste loetelu on toodud käesoleva Juhendi lisades 2 ja 3 (Rahapesu andmebüroo juhend „**Rahapesu andmebüroo soovituslik juhend rahapesu kahtlusega tehingute tunnuste kohta**“ ja Rahapesu andmebüroo juhend „**Rahapesu andmebüroo soovituslik juhend terrorismi rahastamise kahtlusega tehingute tunnuste kohta**“);
3 juhtumitest, mis viitavad VirtualMoney poolt Juhendi rikkumisele;
4 kui klient ei esita vaatamata nõudmisele isikut tõendavat dokumenti, andmeid oma elukoha ja tegevusala kohta ning esinduse korral esindusõiguse aluseks olevat dokumenti.
2 Rahapesu või terrorismi rahastamise kahtlusega tehingu avastamisest ei tohi teatada ühelegi isikule (kaasa arvatud kolleegile) peale Kontaktisiku või VirtualMoney juhatuse. Kliendi informeerimine tema kohta rahapesu andmebüroole edastatud teatisest rahapesu või terrorismi rahastamise kahtluse kohta on keelatud.
3 Rahapesu või terrorismi rahastamise kahtlusega tehingust teada saades analüüsib Kontaktisik laekunud teabe sisu seoses kliendi seniste tehingutega ja muu teadaoleva teabega ning konsulteerib vajadusel VirtualMoney juhatuse liikmega, kas tegemist võib olla rahapesu või terrorismi rahastamise tunnustustele viitava tehinguga.
4 Andmeid rahapesu või terrorismi rahastamise kahtlusega tehingu kohta säilitatakse Kontaktisiku poolt sellisel viisil, et VirtualMoney teistel töötajatel puudub neile Kontaktisiku kirjaliku loata ligipääs.

5 Tuvastades tehingu sooritamisel olukorra, mille tunnused viitavad rahapesule või terrorismi rahastamisele:
1 edastab Kontaktisik rahapesu andmebüroole viivitamatult teate7 kahtlasest tehingust suuliselt, kirjalikult või kirjalikku taasesitamist võimaldavas vormis. Kui teade on edastatud suuliselt, kordab Kontaktisik seda hiljemalt järgmise tööpäeva jooksul kirjalikult;
2 annab Kontaktisik VirtualMoney töötajale loa pooleliolev tehing sooritada pärast:
rahapesu andmebüroo poolt saadud kirjalikku luba tehingu sooritamiseks; või
VirtualMoney juhatuse liikmega konsulteerimist, kui tehingu edasilükkamine võib tekitada olulist kahju, millisel juhul edastatakse kirjalik teade rahapesu andmebüroole viivitamatult pärast tehingu sooritamist.

6 Kontaktisik teavitab rahapesu andmebüroole esitatud igast teatest VirtualMoney juhatust kolme tööpäeva jooksul alates teate saatmisest.
7 Rahapesu andmebüroo nõudmisel esitab Kontaktisik rahapesu andmebüroole täiendavat teavet rahapesu või terrorismi rahastamise kahtlusega tehingu asjaolude ja klienti kohta, kui selline teave on VirtualMoneyl olemas.
8 Rahapesu ja terrorismi rahastamise kahtluse korral teatamiskohustuse täitmise täiendavad nõuded võivad tuleneda rahapesu andmebüroo juhenditest, millega Kontaktisik peab iseseisvalt vähemalt kord aastas tutvuma.
9 VirtualMoney säilitab kõik töötajatelt laekunud teated kahtlaste ja ebaharilike tehingute kohta vähemalt 5 aastat alates teate saamisest, samuti nende teadete analüüsimiseks kogutud informatsiooni ja muud seonduvad dokumendid ning rahapesu andmebüroole edastatavad teated, koos teate edastamise aja ja edastanud töötaja andmetega.
10 Vastavalt RahaPTS § 52 lg 2 ei loeta kohustatud isiku poolt rahapesu ja terrorismi rahastamise kahtluse korral heas usus teavitamiskohustuse täitmist ning asjakohase teabe edastamist rahapesu andmebüroole seaduse või lepinguga pandud konfidentsiaalsusnõude rikkumiseks ning teatamiskohustust täitnud isikute suhtes ei kohaldata vastavate andmete avaldamise eest õigusakti või lepinguga ettenähtud vastutust.

KOOLITUS JA TÖÖTAJATE TEAVITAMINE
1 Kontaktisik viib läbi perioodiliselt VirtualMoney Personali koolitust ja teavitamist, et tõsta töötajate teadlikkust:
1 seonduvalt kahtlaste ja ebaharilike tehingute tüüpilistest juhtumitest ja rakendatavatest ennetusmeetmetest.
2 Õigusaktide nõuete täitmisel;
3 Õigusaktide nõuete rikkumisega kaasnevatest sanktsioonidest.

2 Uue töötaja tööle asumisel tutvustab Kontaktisik või selleks volitatud VirtualMoney töötaja uuele töötajale Juhendit ning teavitab töötajat hoolsusmeetmete rakendamise ja rahapesu kahtlusest Kontaktisiku teavitamise nõuetest.
3 Töötaja võib nõuda Kontaktisikult rahapesu ja terrorismi rahastamise tõkestamise alase (täiend)koolituse saamist või selgitusi, kuidas vältida rahapesu ja terrorismi rahastamise tõkestamist VirtualMoney äritegevuses.
4 Kontaktisik hindab regulaarselt töötajate rahapesu ja terrorismi rahastamise tõkestamise alast koolitusvajadust ning esitab selle kohta juhatusele aruande.

JÄRELEVALVE
1 Reeglite täitmise üle teostab järelevalvet Kontaktisik. Kontaktisiku tegevuse üle teostab järelevalvet Juhatus kui käesolevast juhendist ei tulene teisiti.
2 Kontaktisik peab eelkõige teostama järelevalvet riskide hindamine ja juhtimise, andmete kogumise ja säilitamise ning teatamiskohutuste täitmise osas. Juhatuse informeerimise kohustuse täitmise üle teostab järelevalvet juhatus.
3 Kontaktisikul on õigus tutvuda oma ülesannete täitmiseks VirtualMoney arvutisüsteemiga, dokumentide ja muu teabega.
4 Kontaktisikul on õigus kontrollida, kas VirtualMoney Personali liikmed täidavad rahapesu ja terrorismi rahastamise tõkestamise alaseid nõudeid ning nõuda rikkumiste viivitamatut lõpetamist.
5 VirtualMoney juhatus ja Kontaktisik teeb koostööd rahapesu andmebürooga esitades eelnimetatud asutusele teavet Juhendi rakendamise ja muude seonduvate asjaolude kohta nende nõudmisel.

Lisa 1 Rahapesu andmebüroo soovituslik juhend rahapesu kahtlusega tehingute tunnuste kohta

Lisa 2 Rahapesu andmebüroo soovituslik juhend terrorismi rahastamise kahtlusega tehingute tunnuste kohta

Lisa 3 Juhendiga tutvumine
Olen tutvunud VirtualMoney OÜ rahapesu ja terrorismi rahastamise tõkestamise Juhendiga ning kohustun neid täitma.

Ees- ja perekonnanimi Kuupäev Allkiri

Virtual Money, Ltd.

THE PROCEDURAL RULES AND INTERNAL CONTROLS OF DIGITAL CURRENCY FINANCIAL SERVICE PROVIDERS

Act on Detecting and Preventing Money Laundering and Terrorist Financing

GENERAL PROVISIONS AND DEFINITIONS

The present rules of procedure hereinafter referred to as the "Guide," regulate the activity of Virtual Money, Ltd. pursuant to the Act on Detecting and Preventing Money Laundering and Terrorist Financing. The following words and terms, wherever mentioned throughout this Act, shall have the meanings hereby assigned for them:

- Money laundering implies a valid definition pursuant to § 4 of The Act on Detecting and Preventing Money Laundering and Terrorist Financing;
- Terrorist financing implies a valid definition pursuant to § 5 of The Act on Detecting and Preventing Money Laundering and Terrorist Financing;
- Actual beneficiary implies a valid definition pursuant to § 9 of The Act on Detecting and Preventing Money Laundering and Terrorist Financing;
- Virtual Money means a digital currency provider, who pursuant to The Act on Detecting and Preventing Money Laundering and Terrorist Financing is required to be a natural person.
- Business relationship implies a valid definition pursuant to§ 3 of The Act on Detecting and Preventing Money Laundering and Terrorist Financing;
- Client implies a valid definition pursuant to§ 3 of The Act on Detecting and Preventing Money Laundering and Terrorist Financing;
- Administrative staff means the employees, managers, board members;
- Contact person means the natural person, who is appointed by the management board of Financial Intelligence Unit and may be contacted. The definition “Contact person” may be applied with respect to the members of Virtual Money Board or with respect to the other staff.

THE IMPLEMENTATION OF THE OBLIGATIONS PURSUANT TO THE ACT ON DETECTING AND PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

Virtual Money as a service provider shall comply with the exchange rates. These rules of procedure are the result of the Act on Detecting and Preventing Money Laundering and Terrorist Financing (hereinafter referred to as Act) § 2 (1) (10).

Virtual Money Board shall ensure that each staff member will comply with this Guide, Act and the requirements set out in the legislation on the basis thereof. The administrative staff of Virtual Money shall know and comply with the legislation and relevant instruction, issued by the authorities and study independently the legislation and the Guide. The staff member is personally responsible for fulfilling the requirements arising from the Act and the Guide. The violation of the requirements may result in the termination of the employment agreement and misdemeanor or criminal punishment.

DUE DILIGENCE MEASURES

1. Virtual Money shall apply the due diligence measures, described in the Act or to the extent, based on the nature of the business of Virtual Money and to the extent necessary of the risk level, involved in the transaction.
2. Virtual Money shall pay a great attention to the activities and the circumstances of the client, which refer to money laundering or terrorist financing or the circumstances, upon which the client is definitely linked with money laundering or terrorist financing.
3. Prior to establishing a business relationship with a client, making a transaction, and applying for a business relationship, Virtual Money shall apply the following due diligence measures:
    1. Client identification, the verification of the submitted information, data retention and the update of an information;
    2. The identification and the verification of the identity of the client's representative, including his representation rights. The scope of powers, granted to the representative of the client shall be specified, whether there is a long-term business-relationship or one-time transaction, and whether the right of the representation allows Virtual Money to enter into business-relationship;
    3. The identification of the actual beneficiary;
    4. Obtaining an information regarding business-relationship, including the information about the nature and the purpose of the transaction;
    5. Daily maintenance and vigilance in dealing with the client, including transactions performed during the business relationship, monitoring, regular checking of the data used to identify the person, the updates of the relevant documentation, data and information and, if necessary, the resources used in the transaction source and person identification.

6. To inform the contact person about the situations, when the transaction content or client's activities may contribute money laundering or terrorist financing and, if possible, to stop carrying out such kind transactions.

The due diligence measures may be applied not only upon the use of IT instruments, but also based on the facts identified pursuant to the original documents, which the client submitted. The original document cannot be obtained; the notarized or officially certified by the lawyer copies may be applied. Any other copies cannot be used, even if there is any doubt, that they may be compared against the original.

CONSIDERING CLIENT'S IDENTITY

All persons and their representatives, who are applying to establish any business-relationship with Virtual Money, shall verify the client's identity. The personal recognition or the publicity of the client or his representative does not exclude the compliance with the Guide's obligation to detect money laundering or terrorist financing.

Upon establishing a business-relationship with a client, whether he/she is a sole proprietor or the representative of the client's legal person, he/she shall be identified by means of IT instruments. The identification and control of a person's identity shall be carried out upon the use of a bank link, ID-card, mobile-ID, Smart-ID, etc. In addition, the communication means, which are accessible only to the client or the client's representative (e.g., @ Eesti.ee or other exclusive mail) or/and the unique user ID of Virtual Money, including the authentication tools shall be applied. If these documents or e-identification tools are unavailable, then the client shall identify his/her person with a photocopy of the identifying document copy of Virtual Money. Prior to each transaction, the staff member shall ensure that the person / representative was previously identified and has a representation right.

In addition to point 3.2. The client shall submit the following personal data (by e-mail or in the form of an exchange platform, unless otherwise noted below).

1. Resident:
2. First and last name;
3. Personal identification code;
4. The name, the number, the issue date, the issuer name of the identity document;
5. Residence address;
6. Occupation or type of activity;
7. Contact phone number, e-mail address.

2. Legal person:
1. The name and registry code of the legal entity;

2. Postal address;
3. Type of activity;
4. Contact phone number, e-mail address;
5. The name, surname, personal identification code or date of birth of the representative (in case, when it is not indicated on the register card);
6. The reason for the application of the representation right, in case of an authorized person or notary authorization.

The accuracy of the information provided by the representative of a legal person and the existence of the right of representation is checked by Tartu County Court Registry Office.

3. Non-resident natural person:
1. First and last name;
2. Personal identification code, the date of birth and the place of birth;
3. The name of the travel document, the number, the issue date, the name of the issuer;
4. Postal address of the place of residence;
5. Local address, when creating a contact;
6. Occupation or type of activity;
7. Information concerning the fact, whether the person fulfills or has fulfilled the essential functions of the public authority or is a close associate or a family member (i.e. national background pursuant to the Act).
8. Contact phone number and e-mail address;
9. Notarized copy of the travel document and if necessary the visa or a temporary residence permit. A copy shall be sent via post.

4. Non-resident legal person:
1. The name and the registry code of the legal entity;
2. Country of location, web country code, the current corresponding printouts of the registers, the tax authorities of CIS and offshore countries, updated printouts;
3. The actual information of the beneficiary;
4. Postal address;
5. Business address;
6. Type of activity;
7. Information of the bank account;
8. Contact phone number and e-mail address;
9. Name, surname, the personal identification code and date of birth of the representative (in case, when it is not indicated on the register card);
10. The ground for the representation right in the case of an authorized person, the document, certifying the representation right notarial or through other equally authorized procedure, which is legalized or approved by a certificate replacing

organization (apostille), unless otherwise is provided by an international agreement. Notarized copies of the aforementioned documents shall be sent via post.

4. In case, when the amount of the transaction, carried out by the client exceeds 15000 EUR, the client shall submit a copy of his Virtual Money account or an extract from his/her local government account, which may not be older than three months and indicates the name and address of the client.

5. To verify the information gathered, the member of the administrative staff shall use the available registers and the information contained on the Internet. In case of a business-relationship with a higher risk profile the information and the supporting documents from the submitters may be required. In case of doubts, the client shall be questioned on the grounds of the data gathered via the contact phone talk.

5. In case of a long-term relationship the data gathered shall be checked and updated at least every two years, if it is necessary.

7. A copy of the document, which certifies the identity of a person, shall indicate the identity of the staff member of Virtual Money, who identified the person, including his identification date and his signature.

Data gathered to identify the person shall be registered in the computer system of Virtual Money.

4. DISCLOSURE OF THE RISK PROFILE OF THE CLIENTS, WHO ARE NATURAL PERSONS; DETERMINATION OF THE RISK CATEGORY

An administrative staff member shall identify the client's personal profile and determine the risk category.

The determination of the client's risk category is based on the client's country of residence and actual beneficiaries. In the process of determination of the risk category of non-resident natural persons, it shall be considered the national background of a client and his/her family member or close associate. If the client, his/her family member or his/her close associate is a nationally honored person, he/she will automatically fall into the Category III.

4.1 Category I – Low risk category:

Resident or non-resident natural person, who is the beneficial owner himself;

4.2 Category II – Medium risk category:

Non-resident natural person, who is actually the beneficial owner and who has not a national background, including his/her family member, his/her close associate; resident natural person, who is not the actual beneficial owner.

4.3 Category III – High-risk category:

Resident and non-resident natural person, who has a national background, including his/her family member, his/her close associate; resident natural person, who is not the actual beneficial owner.

4.4 The Risk Category is determined by an administrative staff member, while entering into client relationship and during the client relationship by adding the relevant category to the data of the client.

4.5 If the client relates to the Category III, an administrative staff member shall apply enhanced vigilance measures. (p.10).

4.6 While entering into business-relationship with the clients from High-risk category (Category III), an administrative staff member shall inform the contact person immediately via e-mail or via phone, specified by the Management Board.

5. DEPLOYMENT OF THE CLIENTS ACTIVITY PROFILE OF THE LEGAL PERSONS; DETERMINATION OF THE RISK CATEGORY

5.1 An administrative staff of Virtual Money shall establish a business-relationship with a legal person and define a client risk profile for the legal person.

2. The grounds for the determination of the risk category are the location of the legal person, the type of activity, the transparency of the management structure and the ownership of the legal entity.

1. Category I - Low risk category:

A legal entity registered in the Republic of Estonia, whose type of activity is defined (except for the fishing industry, construction and repair services, fuel wholesale and storage, fuel retail trade, wholesale trade of wood, currency exchange, gambling, casino);

A legal entity registered in the Member State of the European Union or Norway, Iceland, Switzerland, whose shares are publically listed and the company does not deal with a fishing industry, construction and repair services, fuel wholesale trade and storage, fuel retail trade, wholesale trade of wood, currency exchange, gambling, casino);

Automatically belong to a low risk category the government agencies, the insurance companies and the pension funds, the residential credit institutions, the residential local government, the residential central bank, the residential national social security fund, the non-residential central government, the non-residential insurance institutions and the non-residential pension funds, the non-residential local government, the non-residential state social insurance fund, the residential daughter private company, the residential and non-residential daughter financial institution, the residential insurance institution and the residential pension funds.

2. Category II - Medium risk category:

A legal entity registered in a Member State of the European Union or Norway, Iceland, Switzerland, whose shares are publically listed and the company does not deal with a fishing industry, construction and repair services, fuel wholesale trade and storage, fuel retail trade, wholesale trade of wood, currency exchange, gambling, casino);

A legal entity registered in Estonia, whose type of activity belongs to a fishing industry, construction and repair services, fuel wholesale trade and storage, fuel retail trade, wholesale trade of wood, currency exchange, gambling, casino).

A legal entity registered in a Member State of the European Union or Norway, Iceland, Switzerland, whose shares are publically listed and the company deals with a fishing industry, construction and repair services, fuel wholesale trade and storage, fuel retail trade, wholesale trade of wood, currency exchange, gambling, casino);

A legal entity registered in the third countries and in Liechtenstein, whose shares are publically listed and the company deals with a fishing industry, construction and repair services, fuel wholesale trade and storage, fuel retail trade, wholesale trade of wood, currency exchange, gambling, casino);

3. Category III - High-risk category:

A legal entity registered in the third countries and in Liechtenstein (except clause 5.2.2 (iv)); A legal entity registered in a Member State of the European Union or Norway, Iceland, Switzerland, whose shares are not publicly listed, and the company deals with a fishing industry, construction and repair services, fuel wholesale trade and storage, fuel retail trade, wholesale trade of wood, currency exchange, gambling, casino);

4 If the client relates to the Category III, an administrative staff member shall apply enhanced vigilance measures. (p. 10).

5 The Risk Category is determined by an administrative staff member of Virtual Money, while entering into client relationship and during the client relationship by adding the relevant category to the data of the client.

6 While entering into business-relationship with the clients from High-risk category (Category III), an administrative staff member shall inform the contact person immediately via e-mail or via phone, specified by the Management Board. In addition, the contact person shall be informed, whether the company's business is related to the army industry, army sales or brokering.

CLEAR PERSONALIZATION OF THE CLIENT’S ACCOUNT

1. Client identification is necessary at the start of the client relationship.

2. Virtual Money is entitled to suspend or to terminate transactions, if the duration of the business relationships has already expired. In case of the suspected money laundering or in case, when the client does not submit the documents or an information, or in case, when there is a doubt, the transaction will be terminated. An assessment of the suspicion in money laundering enables Virtual Money Board or the contact person to suspend or to terminate the transactions.

PERSONALIZATION AND TRANSACTIONS OF THE CLIENTS WITH A NATIONAL BACKGROUND

1. The clients with a national background belong to the category of the persons listed in § 3 (11) of the Act, whose national backgrounds may be performed by the national and the international organizations.

2. The contact person is responsible for the identification of the persons with a national background, who are the clients of Virtual Money or the potential clients, unless Virtual Money Board appoints another responsible person;

3. There the criteria to identify a person with a national background:

1. Per client’s request;

2. Via existing public or paid databases or via Internet search results;

3. Per request or via the verification of the data through the websites of the authorities of the client’s home country.

4. Virtual Money Management of the contact person shall approve the establishment of a business-relationship with a national background. If the client has already entered into the business-relationships and it turned out that the client had acquired a national background, then it is necessary to inform the contact person in writing or in such form, which can be reproduced in writing.

LOW AND HIGH RISK TRANSACTIONS

1 While executing the transaction, the administrative staff member of Virtual Money shall assess the risk of money laundering and terrorist financing, and choose the appropriate due-diligence measures in accordance with the Guide and apply them.

2 In the process of assessment of the risk of money laundering and terrorist financing, the risk group of a client and the transaction risk shall be taken into account.

3 The risk associated with the transaction is considered to be minor under the following conditions:

1. The client cannot realize the benefits of a transaction a year later from the moment of transaction completion.
2. The transaction is not executed as a prompt payment;

3. The client’s repurchase agreement is not provided;
4. The low risk criteria of "Act on Detecting and Preventing Money Laundering and Terrorist Financing," § 34, paragraph 2 covers the group of persons, mentioned in paragraphs 1-6 or it may be applied in case, when the client’s identification and verification processes imply the following circumstances, which exist simultaneously to each other:

1. The identification of a client is possible on the ground of publically available information;
2. The client’s ownership and controlled structure are transparent and permanent;
3. The type of client’s activity, including his accounting practices is transparent;
4. The clients are accountable and controllable by the executive authority of a Contracting State of the European Economic Area, by other public authority or by the body of the European Community.
5. The client’s risk is considered to be high when the client is:
1. Listed in the United Nations of the European Union and is a person, who is involved into the international financial sanctions;
2. The person, who is suspected by the administrative staff of Virtual Money to be dealing with money laundering or terrorist financing;
6. The risk, associated with the transaction is considered to be high, if:
1. There is a deal, which is requested by a client representative, who can’t properly explain the origin of the money;
2. The transaction is intended to be executed by a client, who has previously been suspected in having the account of Virtual Money, which might be involved into money laundering and terrorist financing;
3. The transactions are requested to be executed via cash payment;
4. The transactions are executed via the cash deposits to the third parties;
5. The transaction, which meet the requirements of the Annexes 2 and 3 of this Guideline;
6. With regard to the high-risk transactions, the due-diligence measures shall be applied in an enhanced manner.
7. In case of the unusual transaction, operation or circumstance, the administrative staff member shall analyze and compare the circumstances of the transaction, paying his/her attention to the aspect of money laundering and terrorist financing. The administrative staff member shall check the legal origin of the property before the moment of the transaction execution or in the case of an unusual money laundering or terrorist financing take into account with suspicion the present relationships with the client;
8. The due-diligence measures shall be applied in an enhanced manner, even when dealing with the low-risk transactions, if the client is suspected to be involved in money laundering or terrorist financing.

THE APPLICATION OF THE DUE-DILIGENCE MEASURES IN A SIMPLIFIED MANNER

1. The due-diligence measures may be applied in a simplified manner under the following conditions:
1. In relation to the group of persons, specified in § 34 (2)1)-6) of the Act.
2. If the client has been given a written durability of the agreement;
3. If the administrative staff doesn't have doubts regarding the accuracy of the information provided by the Client or regarding the Client's ability to provide such an information;
4. If the contact person doesn't suspect any money laundering or terrorist financing in relation to the transaction;
5. If the client's risk or the transaction risk have ground to be considered low;
6. If the client has already established a business-relationship before the implementation of the Guide or the client's identity was identified after the implementation of the Guide pursuant to the rules of the Guide.

2. Upon the application of the simplified due-diligence measures:
1. The persons shall be identified in accordance with clause 3 of the Guide;
2. If the administrative staff member encounters the suspicion towards the client, when the due-diligence measures in a simplified manner are applied, the contact person shall exercise additional control. In the course of the additional check procedures, the employees of Virtual Money call a client to specify the client's data and may ask the other checking questions.
3. If it is impossible to carry out the control or the inspection reveals that the client fails to answer the checking questions, then in such case the transaction shall be terminated;
4. It is prohibited to apply the due-diligence measures in a simplified manner with any client, when:
1. There is a suspicion in money laundering or terrorist financing in the process of communication.
2. When the due-diligence measures are applied, the administrative staff member shall be liable for money laundering or terrorist financing suspicion, the administrative staff member shall inform the contact person vie phone or via e-mail.

THE APPLICATION OF THE DUE-DILIGENCE MEASURES IN AN ENHANCED MANNER

1. The administrative staff manager of Virtual Money shall apply the due-diligence measures in an enhanced manner, when the nature of the situation suspects the

high-risk of money laundering or terrorist financing. The due-diligence measures shall be applied, when:

The identity of the client, who participates in the transaction, has been identified and the information has been verified at the place, where the client is absent.

There are doubts regarding the identity of the client or the checking information, he/she provided, including the authenticity of the documents or the actual beneficiaries identification.

The client, who participates in the transaction, is a national of another contracting state of the European Economic Area or of a third country.

The obligation to apply the due-diligence measures in an enhanced manner applies in addition to the usual rules:

At least one of the following due-diligence measures shall be applied;

The identification and the verification of the information shall be provided based on the supporting documents, data or information, which is from a credible and independent source or from a credit institution, which enters in the Commercial Register in Estonia or the affiliate of a foreign credit institution or a credit institution that is registered or has a place for business in a contracting state of the European Economic Area or in a country, which meets the equivalent requirements;

Pursuant to the Act, when there is a person in that credit institution, staying in the same place as a person identified; (ii) taking further actions on the documents submitted, regarding the authenticity and veracity of the information contained therein, including the notarial acts, requesting official confirmation or confirmation of the accuracy of the data pursuant to the rules (i) of the mentioned credit institution; (iii) making the first payment of the transaction through the account, which belongs to a person, participating in an open transaction in a credit institution, which is registered or has its registered office in a contracting state of the European Economic Area or in a country subject to the equivalent requirements of the Act.

In case of the unusual transaction, operation or circumstance, when the administrative staff shall analyze and compare the circumstances of the transaction, paying attention to the aspect of money laundering and terrorist financing.

2. The administrative staff member shall check the legal origin of the property before execute the transaction or pay attention to the present relationship with the client in case of an unusual money laundering or terrorist financing with suspicion.
3. In case of the transactions with the higher risk level of money laundering and terrorist financing, they need to be compared with the suspicious transactions of money laundering and terrorist financing.

BUSINESS CONTROL

12.1. A member of Virtual Money Board, who is appointed by the Board shall establish a regular business relationship with the clients to ensure that the transactions are executed with a respect to their business and risk profile. Pursuant to that, the administrative staff member shall:

Regularly monitor the amount of the transactions, the amounts used in the transactions;

Identify the origin of the property used in business relationships and/or in the transactions;

Check regularly the client's legal status (existence of legal capacity), financial situation, type of activity, information regarding the ownership (for the actual beneficiaries).

12.2. The administrative staff members shall monitor at least one a year the information regarding:

Client risk assessment;

Country risk assessment, where the client is located;

Combined risk assessment.

The client's risk (risk factors arising from the client's identity) shall be taken into account:

The legal form of a person, the management structure (including trusts, partnerships or the other contractual arrangements of such type, legal entities, legal entities with bearer shares); the ownership structure of a company, in particular those that has a lack of a clear commercial justification and which may be definitive to make it easier for the beneficiary to hide; the type of activity of a person (the clients involved in the business activities, who involve large amounts of cash in the transactions, acting like currency exchange services, money carriers, high value dealers, casinos, betting and the other gambling related companies that receive regular cash payments);

Whether it is a person with a national background or his/her family member or a close associate;

1. Whether it is the representative of a legal person;

The place of residence of a person, including whether he is a registered person in an offshore region (where the tax are exempted or there are low tax rates, for example, corresponding to the website of the Tax and Customs Board on the basis of data http://www.emta.ee/en/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-est-stutu- maksud/ the communication experience with the client, including his co-operation partners, owners, agents and the like circumstances (for example

suspicious transactions detected during a period of a previous business-relationship, suspicious behavior of the client, failure to provide the required documentation);

2. The duration of the activity, the nature of business-relationships.

The state risk, the risk factors, which arise due to the differences in the legal environment of the different countries, whether it is a crime or whether it is a person, who was imposed the international sanctions.

The most risky countries include:

The persons, who are the subjects of the international sanctions or embargoes;

The lack of adequate preventing money laundering laws as compared with the international standards and regulations, whereof terrorist financing or support may be identified;

The persons, who were identified to be involved into significant corruption or organized crime or otherwise the level of crime (including drug trafficking) in the tax-free and low-tax offshore financial centers.

Complex risks

The administrative staff management shall pay particular attention to the situations that indicate the higher level of risk in the number of groups, mentioned above. The administrative staff manager shall send the results of the analysis, as mentioned above, to the contact person in writing.

DATA COLLECTION, CHECK, STORAGE AND UPDATE

1. Data Collection

1 The first identification of the client shall be executed pursuant to the procedure provided in clause 3 of the Guide.

2 Every time, when the client is detected, Virtual Money registers in the computer system/exchange platform the following data:

1. Customer’s name, personal identification code, place of residence, occupation and type of activity;

2. An information about the data provided by the client and the other data, including the necessary documents pursuant to the Guide.

2. Data check

1. The validity of the client’s document in case of doubts shall be checked by Police and Border Guard Board.

The website http://www.politsei.ee/et/teenused/isikut-endancers-documents/index.dot.

3. Data storage

1. Virtual Money stores an information, submitted by the client and his/her representative, client's documentation, including the copy of the documents of his/her representative, the other documentation, that may be requested from the client pursuant to the rules of the Act digitally on a computer system (server) or on a paper copy, or in the place, specified by the administrative management board for at least five years after the termination of the contractual relationships with the client.

2. Transaction data, which relates to the suspicion in money laundering or terrorist financing are retained by the contact person in such a manner, that the other administrative staff members of Virtual Money could not have an unauthorized access without the contact person.

3. An information, which relates to the suspicion in money laundering or terrorist financing is retained in clause 14.4.1. If the investigation of the circumstances, surrounding the transaction were not completed by that moment, the client's and transaction data would be retained up to the moment of the completion of the investigation.

4. Update of data and documents, the measures of the internal control

1. The data shall be updated at least every two years. In the process of update, the administrative staff member, appointed by the Board shall draw up a report, which shall include the risks description and identify the control measures in relation to business activities to mitigate the risks and in case of shortcomings, take the preventing measures to deal with them. The report shall be submitted to the contact person and to the administrative staff of the Board.
2. The administrative staff is responsible for the relationships with the client (client's manager) and he/she shall pay much attention to:

The customer's data, identified as a high-risk category requires assessment control and business knowledge. In addition to the annual analysis, the client's manager shall be constantly on track to evaluate the potential risks of money laundering and terrorist financing related to the business of the client and shall immediately notify the contact person about the change in a risk profile of the client.

3. The contact person shall draw up a detailed monitoring plan, based on the report finding, on the grounds whereof, the contact person monitors the transactions with the higher risk and the client's profile.

4. The updated data shall be immediately entered by the contact person in the computer system of Virtual Money, where the data will be available to the other administrative staff members. The contact person shall organize the management, the process of updating and analyzing of the inclusion data and enter the results

into a data storage to evaluate all risks, to prepare the action plan and to counsel with the managers to prevent risks.

RESTRICTIONS ON TRANSACTIONS

1 The administrative staff member is prohibited:

1 To settle in cash;

2 To execute a transaction for the unidentified customers pursuant to the rules of the Guide;

3 To execute transactions for the anonymous or the fictitious persons, who use other names or denominations.

2 The administrative staff member of Virtual Money shall refuse to execute a transaction, when:

1. The documents or other information, submitted by the client, is suspected in the accuracy and the client cannot adequately explain the circumstances that caused the doubt;

2. The client's identity or credentials cannot be established or verified;

3. The client's place of residence or occupation or type of activity or profile cannot be identified;

4 The client appears to be in the list of the imposition of the international sanctions or the client's money laundering is identified by the FIU as a lender of suspicion in money laundering or terrorist financing, in case, when such information is disclosed by Financial Intelligence Unit;

5. When there are the circumstances, where there is a suspicion that a person may be involved in money laundering or financing of terrorism.

3 A refusal to execute a transaction is registered in the computer system of Virtual Money.

MONITORING AND ANALYSIS

1. The administrative staff member of Virtual money shall monitor and analyze whether the client is executing a transaction, is involved in money laundering or terrorist financing. Money laundering or terrorist financing suspicion and the list of the unusual transaction characteristics are given in Annexes 2 and 3 of the Guide (**Money Laundering Guide of FIU "Indicative Guide of Financial Intelligence Unit on suspicious transactions in money laundering"** and **Financial Intelligence Unit Guide "Indicative Guide of Financial Intelligence Unit on terrorist financing and suspicious transaction characteristics")**.

2 If the client's activity refers to money laundering or terrorist financing, the administrative staff member shall request from the customer the additional information in order to explain the origin of money. Additional information may be requested verbally and/or in writing, but the information collected, shall be recorded and linked to the client’s profile in the computer system of Virtual Money.

3 The contact person shall analyze the client’s transactions, to clarify the possible connection with the money laundering transaction or an opportunity of non-monetary origin of money, if it is necessary.

4 The contact person, who is responsible for managing of the risk assessment of money laundering and terrorist financing shall regularly analyze, whether in Virtual Money terrorist financing or money-laundering risk factors may occur, and what does the Guide not cover.

5 During the identification process, the contact person shall:

1. Prepare the explanations of how to take into account the new risk factors and how to manage risks in Virtual Money's business;

2. Complete the Guide and to draw up a new Guide.

CONTACT PERSON

1 The contact person is appointed by the management board. About the contact details, Virtual Money Board informs Financial Intelligence Unit immediately. Contact is member of Virtual Money Board unless Virtual Money appoints the other administrative staff member on the position of the contact person. If the contact person is a member of the board, where there is the only member of the management board, the contact person is accountable in front of the shareholders.

2 The contact person has the right to require all staff members to comply with the obligations set forth in the Guide, and to terminate possible violation immediately.

3 The tasks of the contact person are:

1. To gather the unusual information or the suspicious transaction data, involving money laundering or terrorist financing. To organize, to analyze and to archive information;

2. To submit the information to Financial Intelligence Unit in case of a suspicion in money laundering or terrorist financing;

3. To check the names of the persons, who are Virtual Money clients and potential customers in the UN and in European Union in the financial sanctions list.

4 To check the compliance with the regulation of Virtual Money, including other regulations at least once a year, and to make the amendments into the Board and into the Guide;

5 To complete the Guide and the technical means for the timely check of the availability of the information delivery;

6 To check the performance of the Guide and the legislative requirements for money laundering and terrorist financing prevention and to analyze the results of the inspection and to inform the board about the compliance with the Guide;

7. To make proposals on risk assessment and management of money laundering and terrorist financing;

8. Staff training. To identify the training needs of the employees in combating money laundering and terrorist financing; and

9. To notify Financial Intelligence Unit about the obligation to identify the client to a third party.

10. To ensure the compliance by Financial Intelligence Unit and other authorities with the requirements of Virtual Money.

11. To identify the clients with national backgrounds among other categories of clients.

12. To fulfil the other obligations pursuant to the requirements of the Act.

4. The contact person shall familiarize himself/herself, including the documentation and other information to establish business-relationship with the client.

MEASURES OF THE INTERNAL CONTROL

1. Virtual Money shall control the execution of anti-money laundering and anti-terrorist financing measures. Contact person shall act for the purposes of this Guide and its annexes, as well as with respect to the tasks provided in legislation.

2. In addition, the contact person shall carry out an internal check at least once a year, where:

The compliance with the requirements of the Guide shall be checked;

The compliance of registrations with the Guide shall be checked;

The fulfillment of other requirements for the prevention of money laundering and terrorist financing shall be checked;

The compliance of the business relationship, monitoring procedures pursuant to the Guide shall be checked;

The compliance with the legislation and the instructions of the competent authorities shall be checked;

The training needs of a staff shall be checked;

3. The contact person shall draw up a report on the execution of the internal control. The report states:

The purpose of the inspection;

The time of inspection;

The check of the job title of the controller;

The description of the control executed;

The analysis of the inspection results or the general conclusions executed;

The description of the deficiencies and the related risks in case of deficiencies;

The time, required to eliminate defects, to take the recommended measures to correct the defects and the follow-up; While executing the the follow-up, the contact person shall add the follow-up results to the inspection report:

The list of the measures, taken to remedy the deficiencies, indicating the shortcomings;

The actual time taken to eliminate them.

4. In the course of ongoing and annual supplementary inspections, the contact person is entitled:

To monitor the work of the administrative staff management and to obtain the technical means necessary for this;

To demand the immediate termination of non-compliance with anti-money laundering and anti-terrorist financing requirements;

To make suggestions for eliminating of the shortcomings identified during the verification pursuant to the procedural rules.

IMPLEMENTATION OF THE NOTIFICATION OBLIGATION

1. The administrative staff member shall inform the contact person of any occurrence of the following situation:

1. About any transaction, where the financial liability exceeds EUR 32 000 or the equivalent in another currency and it is executed in cash regardless of whether the transaction is carried out in a single payment or in several interconnected ones;

2. About money laundering or terrorist financing suspicious transaction. Money laundering or terrorist financing list of suspicion and unusual transaction characteristics are given in Annexes 2 and 3 to the Guide

(The Guide of Financial Intelligence Unit "Recommended Guide of Financial Intelligence Unit on money laundering suspected transaction characteristics" and The Guide of Financial Intelligence Unit "Indicative Guide of Financial Intelligence Unit on terrorist financing suspicious transaction characteristics");

3. About the incidents that indicate that Virtual Money has violated the Guide;

4. If the customer does not submit an identity document despite the demand, the details of his place of residence and the type of activity and, in case of the representation, the document, the right of representation is based therein shall be informed.

2 Any person, except the contact person or Virtual Money Board cannot be notified of any suspicion in money laundering or terrorist financing (including colleagues). Informing the client about the suspicion of his/her money laundering or terrorist financing, disclosed to to FIU is forbidden.

3 When being contacted about a suspicious transaction of money laundering or terrorist financing, the contact person shall analyze:

The content of the information received with respect to the client’s present transactions and the other known information and then he/she shall consult with the administrative staff member of Virtual Money if it is necessary, whether it could be money laundering or terrorist financing transaction, referring to the recognition.

4 The contact person shall stay informed of any suspicion in money laundering or terrorist financing in such a way that other employees of Virtual Money had no written permission to access the contact person.

5. The detection procedure of a transaction, which traits indicate money laundering or financing the terrorists shall be the following:

1. The contact person shall immediately inform Financial Intelligence Unit about the notice of the suspicious transaction verbally, in writing or in a form, which can be reproduced in writing. If there is an oral message, it shall have such details:

The contact person no later than the next working day shall submit it in writing;

2. The contact person shall allow the employee of Virtual Money to execute the transaction, when Financial Intelligence Unit draws up the permission to execute the transaction; or consult the member of Virtual Money Board if the postponement of the transaction may lead to the significant damages. In this case, a written notice to

Financial Intelligence Unit will be forwarded immediately after the execution of a transaction.

6. The contact person shall inform Financial Intelligence Unit of any notification from Virtual Money Board within three working days from the date of the notification.

7. At the request of Financial Intelligence Unit, the contact person shall submit an additional information to FIU regarding money laundering or terrorist financing suspicious transaction circumstances and about the customer, if such information is available.

8. In case of money laundering and terrorist financing, the additional requirements for the fulfillment of the reporting obligations, which the contact person must do at least once a year, may result from the instructions of Financial Intelligence Unit, which the contact person shall be acquainted.

9. Virtual Money shall retain all reports, received from the employees about suspicious and unusual transactions at least 5 years from the date of receipt of the notice, as well as the information collected for the analysis of these messages and other related documents and notifications shall be submitted to the Financial Intelligence Unit, together with a time of submission and the data provided by the employee.

10. Pursuant to § 52 (2) of the Act, money laundering and terrorist financing are not considered obligated in case of doubt. The persons, who have fulfilled obligation to provide information in good faith and the provision of relevant information about money laundering, are not liable for a breach of the confidentiality claim imposed by the law or contract by the data bureau and for the act of disclosure of the relevant data.

TRAINING AND EDUCATION OF WORKERS

1 The contact person shall periodically conduct training and education on the administrative staff of Virtual Money to raise the staff’s level of awareness:

1. Related to the typical incidents with suspicious and unusual transactions and the application of the preventive measures.

2. Related to the compliance with legal requirements;

3. Related to the penalties for non-compliance with the legal requirements.

2 Upon entering a new employee, the contact person or an authorized Virtual Money employee introduces the employee to the rest of the staff, and informs the employee about the application of the due-diligence measures with respect to the suspicion in money laundering.

Requirements for contacting the contact person.

3. The employee may request the contact person on the explanations or supplementary training on how to prevent money laundering and terrorist financing.

4. The contact person shall regularly evaluate the worker’s need for training on money laundering and terrorist financing and shall submit a report to the management board.

MONITORING

1. The compliance with the rules is monitored by the contact person. The contact person is monitored by the governing board, unless otherwise is provided by this guide.

2 The contact person shall, in particular, monitor risk assessment and management, data collection and storage, including the enforcement of the notifications. The management board supervises the implementation of the bureau’s information obligation.

3 The contact person has the right to access the computer system of Virtual Money for the fulfillment of the documents and other information.

4 The contact person has the right to verify that the administrative staff members of Virtual Money satisfy the prevention requirements in relation to money laundering and terrorist financing, and to demand the immediate termination of violations.

5. Virtual Money Board and the contact person cooperate with Financial Intelligence Unit by submitting the aforementioned information on the implementation of the Guide and the other relevant rules upon request to the Authorities.

Annex 1. "Indicative Guide of Financial Intelligence Unit on suspicious transactions in money laundering”

Annex 2. “Indicative Guide of Financial Intelligence Unit on terrorist financing and suspicious transaction characteristics"

Annex 3. Introduction to the Guide

I have read Virtual Money, Ltd. Guides for Preventing Money Laundering and Terrorist Financing and I undertake to fulfill them.

First and last name Date Signature