

SISEMISED PROTSEDUURIREEGLID

Rahapesu ja terrorismi rahastamise tõkestamise kohustuse täitmiseks

Käesolev juhend on kinnitatud 08.12.2021.a Ringfinancial OÜ (registrikood 14716908) juhatuse poolt.

1. Üldsätted ja mõisted

- 1.1. Käesolevad protseduurireeglid (edaspidi Juhend) kehtestab sisemised protseduurireeglid Rahapesu ja terrorismi rahastamise tõkestamise seaduse (edaspidi RahaPTS) sätestatud kohustuste täitmiseks. Protseduurireeglite täitmisega maandatakse ja juhitakse muu hulgas RahaPTSi kohaselt koostatud riskihinnangu raames tuvastatud rahapesu ja terrorismi rahastamisega seotud riske.
- 1.2. Käesolevas Juhendis on alljärgnevatel mõistetel järgmine tähendus:

Ettevõtte - Ringfinancial OÜ (registrikood 14716908), aadress Harju maakond, Tallinn, Kesklinna linnaosa, Viru väljak 2, 10111, Eesti. Ettevõttel on virtuaalväringu teenuse tegevusluba RahaPTSi tähenduses, milles alusel ettevõtte osutab alljärgnevaid teenuseid:

- RahaPTS § 3 p-des 10 ja 10¹ nimetatud teenused, s.o. virtuaalväringu rahakotiteenus ehk teenus, mille raames luuakse klientidele või hoitakse klientide krüpteeritud võtmeid, mida saab kasutada virtuaalväringute hoidmise, talletamise ja ülekandmise eesmärgil ja virtuaalväringu vahetamise teenus ehk teenus, mille raames vahetab isik virtuaalväringut raha vastu või raha virtuaalväringu vastu või üht virtuaalväringut teise vastu;
- Ettevõtte tegeleb üksnes alljärgnevate virtuaalväringutega: LTC,

ВНУТРЕННИЕ ПРОЦЕДУРНЫЕ ПРАВИЛА

Выполнения обязанности противодействия отмыванию денег и финансированию терроризма

Это руководство утверждено 08.12.2021 правлением Ringfinancial OÜ (регистрационный код 14716908).

1. Общие положения и определения

- 1.1. Эти процедурные правила (далее Руководство) устанавливают внутренние правила для выполнения обязательств, исходящих из Закона о противодействии отмыванию денег и финансированию терроризма (далее Закон). С помощью выполнения процедурных правил происходит снижение и управление связанными с отмыванием денег и финансированием терроризма рисками, которые были выявлены в рамках оценки рисков, составленной на основании Закона.
- 1.2. В рамках настоящего Руководства у нижеследующих определений следующее значение:

Компания - Ringfinancial OÜ (регистрационный код 14716908), адрес Харьковский уезд, Таллинн, Кесклиннский район, Виру вяляк 2, 10111, Эстония. У компании есть лицензия на обслуживание виртуальной валюты по смыслу Закона, на основании которой Компания предоставляет следующие услуги:

- Услуги, указанные в § 3 пп. 10 и 10¹ Закона, т. е. услуга кошелька виртуальной валюты, то есть услуга, в рамках которой создаются или хранятся зашифрованные ключи для клиентов, которые могут использоваться для хранения, депонирования и передачи виртуальных валют, и услуга обмена виртуальной валюты, то есть услуга, в которой человек

BCH, BNB, ETH, JOYS, BTC
jmt avalikud virtuaalväeringud.

Rahapesu on kuritegelikust tegevusest saadud vara või selle asemel saadud vara:

- muundamine või üleandmine, kui on teada, et selline vara on saadud kuritegelikust tegevusest või selles osalemisest, eesmärgiga varjata vara ebaseaduslikku päritolu või abistada kuritegelikus tegevuses osalenud isikut, et ta saaks hoiduda oma tegude õiguslikest tagajärgedest;
- omandamine, valdamine või kasutamine, kui selle saamisel on teada, et see on saadud kuritegelikust tegevusest või selles osalemisest;
- tõelise olemuse, päritolu, asukoha, käsutamiseviisi, ümberpaigutamise või omandiõiguse varjamine või varaga seotud muude õiguste varjamine või kui on teada, et selline vara on saadud kuritegelikust tegevusest või selles osalemisest.
- Rahapesuga on tegemist ka juhul, kui kuritegelik tegevus, mille tulemusel saadi rahapesus kasutatav vara, toimus teise riigi territooriumil.

Terrorismi rahastamine on terrorikuriteo ja selle toimepanemisele suunatud tegevuse ning terroristlikul eesmärgil reisimise rahastamine ning toetamine karistusseadustiku tähenduses.

Riikliku taustaga isik (PEP) on füüsiline isik, kes täidab või on täitnud avaliku võimu olulisi ülesandeid, sealhulgas riigipea, valitsusjuht, minister ning ase- või abiminister, parlamendiliige või parlamendiga sarnase seadusandliku organi liige, erakonna juhtorgani liige, ülemkohtu ja riigikohtu liige, riigikontrolli ja keskpanga nõukogu liige, suursaadik, asjur ja kaitsejõudude kõrgem ohvitser, riigiäriühingu juhatuse ja

obменивает виртуальную валюту на деньги или деньги на виртуальную валюту или одну виртуальную валюту на другую;

- Компания работает только со следующими виртуальными валютами: LTC, BCH, BNB, ETH, JOYS, BTC и другими публичными виртуальными валютами.

Отмывание денег это предпринимаемое в отношении имущества, полученного в результате преступной деятельности, или имущества, полученного вместо него:

- Преобразование или перевод, если известно, что такое имущество получено в результате преступной деятельности или участия в ней, с целью сокрытия незаконного происхождения имущества или в целях оказания помощи лицу, участвовавшему в преступной деятельности, с тем, чтобы оно могло уклониться от правовых последствий своих действий;
- Приобретение, владение или использование, если при получении известно, что такое имущество получено в результате преступной деятельности или участия в ней;
- Сокрытие подлинного характера, происхождения, местонахождения, способа распоряжения, перемещения, прав собственности или утаивание иных прав, связанных с имуществом, или если известно, что такое имущество получено в результате преступной деятельности или участия в ней.
- Отмыванием денег считается также ситуация, когда преступная деятельность, в результате которой получили имущество,

haldus- või järelevalveorgani liige, rahvusvahelise organisatsiooni juht, juhi asetäitja ja juhtorgani liige või samaväärseid ülesandeid täitev isik, kes ei ole kesk- või alamastme ametniku staatuses.

Riikliku taustaga isiku pereliige on tema abikaasa või abikaasaga samaväärseks peetav isik, tema laps ja lapse abikaasa või abikaasaga samaväärseks peetav isik, tema vanem.

Riikliku taustaga isiku lähedane kaastöötaja on füüsiline isik, kelle kohta on teada, et ta on juriidilise isiku või õigusliku üksuse tegelik kasusaaja või ühine omanik koos riikliku taustaga isikuga või tal on lähedased ärisuhted riikliku taustaga isikuga, ning füüsiline isik, kes on sellise juriidilise isiku või õigusliku üksuse ainus kasusaav omanik, mis on teadaolevalt tegelikult asutatud riikliku taustaga isiku kasuks.

Tegelik kasusaaja on füüsiline isik, kes lõplikult omab või kontrollib juriidilist isikut piisava arvu aktsiate, osade, hääleõiguste või omandiõiguste otsese või kaudse omamise kaudu, sealhulgas osalus esitajaaktsiate või -osade kujul, või muul viisil. **Otsene omamine** on kontrolli teostamise viis, mille puhul omab füüsiline isik äriühingus 25 protsendi suurust osalust pluss üks aktsia või üle 25 protsendi suurust omandiõigust. **Kaudne omamine** on kontrolli teostamise viis, mille puhul omab äriühingus 25 protsendi suurust osalust pluss üks aktsia või üle 25 protsendi suurust omandiõigust äriühing, mis on füüsilise isiku kontrolli all, või mitu äriühingut, mis on sama füüsilise isiku kontrolli all. Kui pärast kõikvõimalike tuvastusmeetodite ammendumist ei ole tegelikku kasusaajat võimalik kindlaks teha ja puudub ka kahtlus, et selline isik siiski eksisteerib, või juhul, kui on kahtlus, kas kindlaks tehtud isik on tegelik kasusaaja, käsitatakse tegeliku kasusaajana sellist füüsilist isikut, kes on kõrgema juhtorgani liige.

используемое для отмыwania денег, происходила на территории другого государства.

Финансирование терроризма

представляет собой финансирование и поддержку террористических преступлений, а также деятельности, направленной на их осуществление, и поездок в целях терроризма в значении Пенитенциарного кодекса.

Публичное должностное лицо

(далее **ПДЛ**) является физическим лицом, выполняющим или выполнявшим важные задачи публичной власти, в том числе главы государств, главы правительств, министры и заместители министров, члены парламента или члены законодательного органа аналогичного характера, члены правления партии, члены верховного суда и государственного суда, члены советов государственных контрольных учреждений и центрального банка, послы, поверенные в делах и высшие офицеры сил обороны, члены органов управления и надзора или административных органов государственных коммерческих товариществ, руководители, заместители руководителей и члены органов управления международных организаций, или лица, выполняющие аналогичные функции и не являющиеся должностными лицами среднего или низшего уровня.

Член семьи публичного

должностного лица – его супруг(-а) или приравненный к супругу (супруге) партнер, его ребенок и супруг(-а) ребенка или приравненный к супругу/супруге партнер ребенка, его родитель.

Ближайший сотрудник публичного должностного лица

- физическое лицо, о котором известно, что оно, является

Kontaktisik on Ettevõtte juhatuse liige, kes vastutab RahaPTS-i, selle alusel kehtestatud õigusaktide ja juhendite rakendamise eest. Ta on määratud Rahapesu andmebüroo (edaspidi RAB) kontaktisikuks ning tal on RahaPTS-is sätestatud ülesannete täitmiseks vajalik pädevus, vahendid ja juurdepääs asjakohasele teabele kõigis Ettevõtte struktuuriüksustes.

Klient on Ettevõttega ärisuhtes olev isik.

Ärisuhe käesoleva Juhendi tähenduses on lepinguline püsisuhe Kliendiga.

Tehing – juriidilistele isikutele laenude andmine, juriidilistelt isikutelt laenude võtmine, tegutsemine juhatajana või juhatuse liikmena äriühingus, osanikuna täisühingus või sellisel positsioonil muus juriidilises isikus, samuti teise isiku nimetatud ametikohale asumise korraldamine.

Rahapesu andmebüroo (RAB) on Politsei- ja Piirivalveameti iseseisev struktuuriüksus, mille põhiülesandeks on rahapesu ja terrorismi rahastamise tõkestamine.

Postiaadress: Tööstuse 52, 10416, Tallinn

e-post: rahapesu@politsei.ee

telefon: (+372) 612 3840

veebipõhise teatamise vorm:

<https://rabis-web.politsei.ee/#/>

- 1.3. RahaPTS-i nõuete täitmisega tegelevad töötajad ja esindajad (edaspidi **Esindajad**) peavad tundma ja rangelt jälgima RahaPTS-is, RAB-i poolt välja antud juhendites ja käesoleva Juhendi nõudeid.
- 1.4. Esindajad, kes tegelevad RahaPTS-i nõuete täitmisega, peavad olema kursis kõikide uuendustega käesolevas Juhendis, iseseisvalt tutvuma seaduste ja teiste õigusaktide muudatustega, mis ilmuvad RAB-i kodulehel.¹
- 1.5. Esindajad, kes on tutvunud Juhendiga ning tegelevad RahaPTS-i nõuete täitmisega, vastutavad RahaPTS-i

реальным бенефициаром юридического лица или правовой единицы, или собственником с ПДЛ или у него тесные деловые отношения с ПДЛ, и физическое лицо, которое является единственным собственником-выгодоприобретателем юридического лица или правовой единицы, которое, как известно, фактически создано в интересах ПДЛ.

Бенефициарный собственник - физическое лицо, которое окончательно владеет юридическим лицом или контролирует его через достаточное количество акций, паев, прямое или косвенное владение правом голоса или правом собственности, в том числе в форме предъявительских акций или паев, или иным образом. **Прямое владение** является методом контроля, при котором физическое лицо имеет долю в юридическом лице в размере 25 процентов плюс одна акция или право собственности более чем на 25 процентов.

Косвенное владение является методом контроля, при котором доля в размере 25 процентов плюс одна акция или право собственности более чем на 25 процентов принадлежит компании, находящейся под контролем физического лица, или несколькими компаниями, находящихся под контролем одного и того же физического лица. Если после применения всех возможных методов определения невозможно выявить бенефициарного собственника и нет никаких сомнений в том, что такое лицо существует, или когда есть сомнения относительно того, является ли установленное лицо бенефициарным собственником, бенефициарным собственником считается физическое лицо, которое является членом высшего органа управления.

Контактное лицо является членом правления Компании, который

¹ <https://www.politsei.ee/et/rahapesu-andmebueroo>

<p>nõuete täitmise eest isiklikult seaduses sätestatud korras.</p>	<p>отвечает за исполнение Закона, правовых актов и руководств, установленных на его основе. Указанный член правления является контактным лицом для Бюро данных об отмывании денег (далее БДО) и имеет необходимую компетенцию, ресурсы и доступ к соответствующей информации во всех структурных подразделениях Компании для выполнения обязанностей, установленных Законом.</p> <p>Клиент - лицо, находящееся в Деловых отношениях с Компанией.</p> <p>Деловые отношения в значении данного Руководства это постоянные договорные отношения с Клиентом.</p> <p>Транзакция - предоставление кредитов юридическим лицам, взятие кредитов у юридических лиц, осуществление деятельности в качестве руководителя или члена правления юридического лица, собственника в обществе с полной ответственностью или в качестве подобного представителя в другом юридическом лице, также организация назначения другого лица на эту позицию.</p> <p>Бюро данных об отмывании денег (БДО) является независимым структурным подразделением Департамента полиции и погранохраны, основной задачей которого является предотвращение отмывания денег и финансирования терроризма. Почтовый адрес: Tööstuse 52, 10416, Таллинн Электронная почта: rahapesu@politsei.ee Телефон: (+372) 612 3840 Форма сообщения онлайн: https://rabis-web.politsei.ee/#/</p> <p>1.3. Персонал и представители Компании (далее Представитель/Представители), занимающиеся выполнением требований Закона, должны знать и строго следовать требованиям, исходящим из Закона, руководств БДО и настоящего Руководства.</p>
--	---

<p>2. Ettevõtte tegevusest tulenevate riskide juhtimine</p> <p>2.1. Kliendi ja tema tegevusega seotud riskide tuvastamiseks ja juhtimiseks ning Kliendi riskikategooria määramiseks hinnatakse igat Klienti vastavalt Juhendile. Kliendi hindamisel lähtub Ettevõtte tunne-oma-klienti-põhimõttest, arvestades rahvusvahelist standarde ja praktikat.</p> <p>2.2. Potentsiaalse Kliendi riskikategooria määramisel arvestatakse Kliendi</p> <ul style="list-style-type: none"> • residentsus; • majanduslikud tegevused; • õiguslik vorm; • andmed Tegelik kasusaaja kohta; • eeldatav Tehingute maht. <p>2.3. Riskide tuvastamisel võetakse arvesse ka Kliendi maine. Vajadusel küsib Esindaja Kliendilt täiendavaid andmeid ja dokumente.</p> <p>2.4. Info kogumisel on allikateks RABi ja teiste järelevalveasutuste soovitusel, RABi aastaraamatud, avaldatud uuringud, meedias kajastatud info jt.</p> <p>2.5. Suuremat riski iseloomustavad tunnused: Kliendiga seonduv risk</p> <p>2.5.1. Klient, Kliendi esindaja või Kliendi Tegelik kasusaaja on PEP, PEPi pereliige või PEPi lähedane kaastöötaja;</p> <p>2.5.2. Kliendi majandustegevuse korral on tegemist tavapärasest suurema rahapesu või terrorismi</p>	<p>1.4. Представители, занимающиеся выполнением требований Закона, должны быть осведомлены обо всех нововведениях данного Руководства, самостоятельно изучать поправки к законам и другим правовым актам, которые появляются на сайте БДО.²</p> <p>1.5. Представители, которые ознакомились с Руководством и занимаются выполнением требований Закона, несут личную ответственность за выполнение этих требований в порядке, установленном Законом.</p> <p>2. Управление рисками, возникающими в результате деятельности Компании</p> <p>2.1. Для выявления и управления рисками, связанными с Клиентом и его деятельностью, а также для определения категории риска Клиента, каждый Клиент рассматривается в соответствии с Руководством. При рассмотрении Клиента, Компания исходит из понятия «Знай своего клиента», учитывая международные стандарты и практику.</p> <p>2.2. При определении категории риска потенциального Клиента учитывается:</p> <ul style="list-style-type: none"> • Резиденство; • Экономическая деятельность; • Правовая форма; • Данные о Бенефициарном собственнике; • Ожидаемая сумма Транзакций. <p>2.3. При установлении рисков учитывается так же репутация Клиента. При необходимости Представитель запрашивает у Клиента дополнительную информацию и документы.</p> <p>2.4. При сборе информации источниками являются рекомендации БДО и других надзорных органов, ежегодники БДО, опубликованные исследования, информация средств массовой информации и др.</p>
---	--

² <https://www.politsei.ee/et/rahapesu-andmebueroo>

<p>rahastamise riskiga olukorraga (nt romukulla müük);</p> <p>2.5.3. Hooldusmeetmete rakendamisel on tekkinud kahtlus esitatud andmete tõlevastavuses või dokumentide ehtsuses või Tegeliku kasusaaja tuvastamises;</p> <p>2.5.4. Kliendiks on juriidiline isik, mis tegeleb personaalse varahaldusega;</p> <p>2.5.5. Kliendiks on suuri sularahakoguseid käitlev ettevõtja;</p> <p>2.5.6. Kliendiks oleval või temaga seotud äriühingul on variaktsionärid või esitajaaktsiad;</p> <p>2.5.7. Kliendiks oleva äriühingu omandistruktuur näib ebatavaline või liiga keeruline;</p> <p>2.5.8. Usaldusväärsete andmete kohaselt on Klient seotud finantskuriteo või teise kahtlase tegevusega;</p> <p>2.5.9. Klient on kantud ÜRO või Euroopa Liidu nimekirja, mida peetakse isikute kohta, kelle suhtes kehtivad rahvusvahelised finantssanktsioonid (Lisa 1).</p> <p>Geograafiline risk</p> <p>2.5.10. Klient on registreeritud või tema majandusliku tegevuse koht asub suure riskiga kolmandas riigis (Lisa 1);</p> <p>2.5.11. Riigid ja territooriumid, kus ei ole kehtestatud rahapesu ja terrorismi rahastamise tõkestamise tõhusaid süsteeme või mida loetakse madala maksumääraga territooriumiks (Lisa 1);</p> <p>2.5.12. Kliendiks on suurema riskiga geograafilise piirkonna resident (Lisa 1);</p> <p>2.5.13. Riigid ja territooriumid, mille suhtes on rakendatud ÜRO või Euroopa Liidu sanktsioon, embargo või muu analoogne meede (Lisa 1);</p> <p>2.5.14. Riigid, mis on usaldusväärsetel andmetel seotud terrorismi toetamisega või kus on kõrge korruptsiooni tase.</p> <p>Tehingute ja suhtluskanalitega seonduv risk</p> <p>2.5.15. Taotletakse Tehingu tegemist, millel ei ole arusaadavat mõistlikku ärilist, majanduslikku või juriidilist eesmärki;</p>	<p>2.5. Показатели повышенного риска: Риск, связанный с Клиентом</p> <p>2.5.1. Клиент, представитель Клиента или Бенефициарный собственник Клиента является ПДЛ, членом семьи ПДЛ или ближайшим сотрудником ПДЛ;</p> <p>2.5.2. Экономическая деятельность Клиента связана с повышенным риском отмывания денег или финансирования терроризма (например, продажа золотого лома);</p> <p>2.5.3. При применении мер прилежания возникают сомнения в достоверности предоставленных данных или подлинности документов либо установлении Бенефициарного собственника;</p> <p>2.5.4. Клиент является юридическим лицом, которое занимается управлением личными активами;</p> <p>2.5.5. Клиент является предприятием, занимающимся обработкой больших сумм наличных денег;</p> <p>2.5.6. Клиент или связанное с ним юридическое лицо имеет теневого акционера или представительские акции;</p> <p>2.5.7. Структура собственников Клиента-юридического лица кажется необычной или слишком сложной;</p> <p>2.5.8. По достоверным данным, Клиент связан с финансовым преступлением или другой подозрительной деятельностью;</p> <p>2.5.9. Клиент занесен в список ООН или Европейского Союза (далее ЕС) касательно лиц, попадающих под международные финансовые санкции (Приложение 1).</p> <p>Географический риск</p> <p>2.5.10. Клиент зарегистрирован или место его экономической деятельности находится в третьем государстве с высоким риском (Приложение 1);</p> <p>2.5.11. Государства и территории, где не установлены эффективные системы предотвращения отмывания денег и финансирования терроризма,</p>
---	--

- 2.5.16. Ärisuhte loomisel või Tehingu tegemisel ei viibita Kliendi/Kliendi esindajaga samas kohas ja ei kohaldata isikusamasuse tuvastamist ja andmete kontrollimist infotehnoloogiliste vahendite abil;
- 2.5.17. Hooldusmeetmete rakendamisel on tekkinud kahtlus esitatud andmete tõlevastavuses või dokumentide ehtsuses;
- 2.5.18. Tehingu eest tasub Tehingu osaliseks mitteolev isik;
- 2.5.19. Taotletakse Tehingu tegemist, mille üks eesmärkidest on tegelikke tehinguosaliste varjamine.

2.6. Väiksemat riski iseloomustavad tunnused:

- 2.6.1. Klient on reguleeritud turul noteeritud äriühing, kelle suhtes kohaldatakse avalikustamiskohustusi, millega on kehtestatud nõuded, et tagada Tegelikku kasusaaja puhul piisav läbipaistvus;
- 2.6.2. Klient on enda nimel tegutsev krediidasutus või finantseerimisasutus, Euroopa Majanduspiirkonna lepinguriigis (edaspidi EMP) (Lisa 1) või kolmandas riigis asuv krediidasutus või finantseerimisasutus, kelle kohta kehtivad tema asukohariigis Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849 nõuetega võrdväärsed nõuded;
- 2.6.3. Klient on pärit (sh elu- või asukoht, resident) järgmisest riigist:
- 2.6.3.1. Euroopa Majanduspiirkonna lepinguriigist (Lisa 1);
- 2.6.3.2. kolmandast riigist, kus on tõhusad rahapesu ja terrorismi rahastamise tõkestamise süsteemid;
- 2.6.3.3. kolmandast riigist, kus usaldusväärsete allikate kohaselt on korrupsiooni ja muu kuritegeliku tegevuse tase madal;
- 2.6.3.4. kolmandast riigist, kus on kehtestatud rahapesu ja terrorismi rahastamise tõkestamise nõuded, mis on

- или которые считаются территорией с низкой налоговой ставкой (Приложение 1);
- 2.5.12. Клиент является резидентом географического района с повышенным риском (Приложение 1);
- 2.5.13. Государства и территории, в отношении которых действуют санкции ООН или ЕС, эмбарго или другие аналогичные меры (Приложение 1);
- 2.5.14. Государства, которые, по достоверной информации, участвуют в поддержке терроризма или в которых существует высокий уровень коррупции.

Риск, связанный с Транзакциями и коммуникационными каналами

- 2.5.15. Запрашивается совершение Транзакции, не имеющей понятной разумной коммерческой, экономической или юридической цели;
- 2.5.16. При установлении Деловых отношений или совершении Транзакции Представитель не находится с Клиентом/представителем Клиента в одном месте и при установлении личности и проверки данных не используются инфотехнологические решения;
- 2.5.17. При применении мер прилежания возникают сомнения в достоверности предоставленных данных или подлинности документов;
- 2.5.18. Транзакция оплачивается лицом, которое не является участником Транзакции;
- 2.5.19. Запрашивается Транзакция, среди целей которой есть сокрытие фактических участников Транзакции.

2.6. Показатели пониженного риска:

- 2.6.1. Клиентом является котирующаяся на регулируемом рынке компания, на которую распространяются обязательства по раскрытию информации, которыми установлены требования обеспечить

<p>kooskõlas FATF muudetud soovitusetega (Lisa 1).</p> <p>2.7. Kui Kliendi, tema tegevustega ja Tehingutega seotud riskide tuvastamisel esineb vähemalt üks suurema riski tunnus, siis määratakse Kliendile kõrge riski kategooria ja Esindaja kohaldab hoolsusmeetmeid tugevdatud korras (alates punktist 3.6).</p> <p>2.8. Kui Kliendi, tema tegevustega ja Tehingutega seotud riskide tuvastamisel esinevad väiksema riski tunnused ning ei esine ühtegi suurema riski tunnust, siis määratakse Kliendile madala riski kategooria ja Esindaja võib kohaldada hoolsusmeetmeid lihtsustatud korras (alates punktist 3.11) või tavapäraseid hoolsusmeetmeid (alates punktist 3.1).</p> <p>2.9. Kui Kliendi, tema tegevustega ja Tehingutega seotud riskide tuvastamisel <u>ei esine suurema ega väiksema riski tunnuseid</u>, siis määratakse Kliendile keskmise riski kategooria ning Esindaja kohaldab tavapäraseid hoolsusmeetmeid (alates punktist 3.1).</p> <p>2.10. Kui PEP ei täida enam talle antud olulisi avalikke ülesandeid, siis vähemalt 12 kuu jooksul võtab Esindaja arvesse riske, mis on kõnealuse isikuga jätkuvalt seotud. Esindajal on õigus rakendada hoolsusmeetmeid tugevdatud korras, kuni on kindel, et PEPidele omaseid riske kõnealuse isiku puhul enam ei esine.</p> <p>2.11. Tehnoloogia- ja teenuseriskide tuvastamine ja juhtimine. Ettevõtte kasutab <i>blockchain</i> tehnoloogiat oma äritegevuse raames, mille tehnoloogiaga kaasnevate riskide tuvastamine ja juhtimine toimub läbi Ettevõtte poolt kasutatava kõrgtasemelise infosüsteemi kaudu, vastavalt käesolevas Juhendis toodud tingimustele. Kui Ettevõtte võtab kasutusele uusi tehnoloogiaid või ostab selliseid teenuseid sisse, siis vormistatakse eraldi tehnoloogiate riskide analüüs.</p> <p>2.11.1. Ettevõtte kasutab teenuste osutamiseks turvalist tehnoloogilist lahendust ning kasutab füüsilisi ja isiklikke turvameetmeid, näiteks krüptoraha riistvarakotid.</p> <p>2.11.2. Ettevõtte kasutab pakutavate teenuste turvalisuse tagamiseks ja</p>	<p>достаточную прозрачность в отношении Бенефициарного собственника;</p> <p>2.6.2. Клиентом является действующее от своего имени кредитное учреждение или небанковское финансовое учреждение, кредитное учреждение или небанковское финансовое учреждение, находящееся в государстве-участнике Европейской экономической зоны (далее ЕЭЗ) (Приложение 1) или в третьем государстве, в отношении которого в его стране действуют требования эквивалентные требованиям Директивы Европейского Парламента и Совета (ЕС) 2015/849;</p> <p>2.6.3. Место происхождения (в т. ч. место жительства, местонахождение, резиденство) из следующей страны:</p> <p>2.6.3.1. Государство-участник ЕЭЗ (Приложение 1);</p> <p>2.6.3.2. Третьи государства, где установлены эффективные системы по предотвращению отмывания денег и финансирования терроризма;</p> <p>2.6.3.3. Третьи государства, где, согласно достоверным источникам, низкий уровень коррупции и другой преступной деятельности;</p> <p>2.6.3.4. Третьи государства, где установлены требования по предотвращению отмывания денег и финансирования терроризма, соответствующие дополненным рекомендациям ФАТФ (Приложение 1).</p> <p>2.7. Если при выявлении рисков, связанных с Клиентом, его деятельностью и Транзакциями, определен хотя бы один из показателей повышенного риска, Клиенту присваивается категория</p>
---	--

<p>tehingute ajaloo säilitamiseks spetsiaalset tehnilist lahendust AES 256-bitist krüpteerimist.</p> <p>2.11.3. Autoriseerimisprotsessi eelised, konto turvalisus:</p> <p>2.11.3.1. autoriseerimisprotsess toimub Google'i 2FA-ga, IP-kaitse (IP-aadresside valge nimekiri);</p> <p>2.11.3.2. vahendite väljavõtmiseks kasutab Ettevõtte iga tehingu kohta SMS-kinnitust - ühekordset parooli.</p> <p>2.11.4. Tehnoloogilise lahenduse rikkumise korral riskide vähendamise meetmed, sealhulgas varusüsteem:</p> <p>2.11.4.1. Ettevõtte kasutab mitut serverit. Ettevõttel on kuumade krüptoraha rahakotide jaoks eraldi server, mis on ühendatud teiste serveritega 256 AES-i krüptimise ja SHA512 räsialkirjaga turvalise protokolliga iga paketi jaoks;</p> <p>2.11.4.2. see server varundab rahakotte iga päev. Selle serveri blokeerib tulemüür ja sellele pääseb juurde ainult teatud IP-aadressidele;</p> <p>2.11.4.3. kõik pordid on suletud.</p> <p>2.11.5. Ettevõtte seab iga krüptoraha salvestamise piirangud ja pärast mis tahes rahakoti saldo suurendamist rohkem kui seatud limiidi summa ulatuses, saadab ettevõtte automaatselt vahendid riistvarakotile.</p> <p>2.11.6. Esindaja vastutab isiklikult turvalisuse, jälgimise, tuvastamise ja juhatusele aruandluse eest.</p> <p>2.11.7. Reeglina analüüsib Ettevõtte süstemaatiliselt täiendavate turvameetmete vajalikkust.</p>	<p>высокого риска, и Представитель применяет меры прилежания в усиленном порядке (начиная с пункта 3.6).</p> <p>2.8. Если при выявлении рисков, связанных с Клиентом, его деятельностью и Транзакциями, определены показатели пониженного риска и не присутствует ни одного показателя повышенного риска, Клиенту присваивается категория низкого риска, и Представитель может применить меры прилежания в упрощенном порядке (начиная с пункта 3.11) или в обычном порядке (начиная с пункта 3.1).</p> <p>2.9. Если при выявлении рисков, связанных с Клиентом, его деятельностью и Транзакциями, <u>не присутствует показателей повышенного или пониженного риска</u>, Клиенту присваивается категория среднего риска, и Представитель применяет обычные меры прилежания (начиная с пункта 3.1).</p> <p>2.10. Если ПДЛ больше не выполняет возложенные на него важные задачи публичной власти, то в течение по крайней мере 12 месяцев Представитель принимает во внимание риски, которые по-прежнему связаны с этим лицом. Представитель имеет право применять меры прилежания в усиленном порядке до тех пор, пока не будет установлено, что характерные для ПДЛ риски больше не присутствуют в отношении этого лица.</p> <p>2.11. Выявление и управление рисками технологий и услуг. Компания использует технологию <i>блокчейн</i> в рамках своей коммерческой деятельности, идентификация и управление рисками, связанными с технологией, осуществляется через информационную систему высокого уровня, используемую Компанией, в соответствии с условиями, изложенными в настоящих Инструкциях. Если Компания внедрит новые технологии или купит такие услуги, анализ рисков технологий будет готовиться отдельно.</p>
--	---

	<p>2.11.1. Компания использует безопасное технологическое решение для предоставления услуг и применяет физические и личные меры для обеспечения безопасности, такие как аппаратные кошельки для криптовалюты.</p> <p>2.11.2. Компания использует специальное техническое решение AES 256-битное шифрование, чтобы обеспечить безопасность предоставляемых услуг и сохранить историю транзакций.</p> <p>2.11.3. Преимущества процесса авторизации, безопасность счетов:</p> <p>2.11.3.1. процесс авторизации будет с 2FA от <i>Google</i>, защита IP (белый список IP-адресов);</p> <p>2.11.3.2. для вывода Компания будет использовать SMS-подтверждение каждой транзакции - одноразовый пароль.</p> <p>2.11.4. В случае взлома технологического решения мероприятия по снижению риска, включая систему резервного копирования:</p> <p>2.11.4.1. Компания использует несколько серверов. Компания имеет отдельный сервер для горячих кошельков криптовалюты, который связан с другими серверами защищенным протоколом с шифрованием 256 AES и хэш-подписью SHA512 для каждого пакета;</p> <p>2.11.4.2. этот сервер делает резервную копию кошельков каждый день. Этот сервер заблокирован брандмауэром и доступен только для некоторых IP-адресов;</p> <p>2.11.4.3. все порты закрыты.</p> <p>2.11.5. Компания устанавливает лимиты для хранения каждой криптовалюты, и после увеличения баланса на любом кошельке больше, чем на сумму установленного лимита,</p>
--	--

3. Hoolsusmeetmete rakendamine

Klient peab Ettevõtte koostatud kasutajatingimustes ja/või kliendilepingus kinnitama ja nõustuma, et ta kasutab Ettevõtte poolt osutatavaid teenuseid üksnes selleks ettenähtud eesmärkidel ja sihtotstarbel. Klient peab olema alati valmis selgitama tehtava tehingu eesmärki ja selleks kasutatavate rahaliste vahendite allikat ning päritolu. Ärisuhte kestel kontrollib Ettevõtte kliendi suhtes salvestatud logide alusel, kas kliendi poolt teostatud tehingutel on mõistlik majanduslik eesmärk ja võrdleb kliendi tegevust tema varasemate käitumisharjumustega ning tema kohta eelnevalt teadaoleva informatsiooniga.

Ärisuhte eesmärk on tavapärasel juhul tulenev Ettevõtte majandustegevusest, milleks on virtuaalvääringu vahetamine raha, raha vahetamine virtuaalvääringu või virtuaalvääringu vahetamine virtuaalvääringu vastu või rahakotiteenuse pakkumine.

Arvestades Ettevõtte poolt pakutava teenuse iseloomu ning et Ettevõtte kavatses oma teenuseid osutada alati internetilahenduse kaudu ja et Ettevõtte poolt kasutatavate infosüsteemide kõrgetasemelise turvalisuse ning kliendi suhtes teostavate kontrollide tõttu on rahapesu ning terrorismi rahastamise risk maandatav, siis Ettevõtte ja kliendi vaheline ärisuhe luuakse kliendiga samas kohas viibimata. Ettevõtte kohaldab hoolsusmeetmeid vastavalt

Компания автоматически отправляет средства на аппаратный кошелек.

2.11.6. Представитель несет персональную ответственность за безопасность, мониторинг, идентификацию и отчитывается перед Правлением.

2.11.7. Как правило, Компания систематически анализирует необходимость принятия дополнительных мер безопасности.

3. Применение мер прилежания

Клиент должен подтвердить и согласиться в условиях пользователя и/или клиентском договоре, подготовленными Компанией, что он использует услуги, предоставляемые Компанией, только для предусмотренных для этого целях и назначениях. Клиент всегда должен быть готов объяснить цель транзакции, а также источник и происхождение используемых для нее средств. В ходе деловых отношений Компания проверяет на основе логов, хранящихся в отношении клиента, имеют ли транзакции, выполняемые клиентом, разумную экономическую цель, и сравнивает действия клиента с его предыдущими поведенческими привычками и ранее известной информацией о нем.

Целью деловых отношений обычно является экономическая деятельность Компании, которая заключается в обмене виртуальной валюты на деньги, обмене денег на виртуальную валюту или обмене виртуальной валюты на виртуальную валюту или предоставлении услуг кошелька.

Учитывая характер услуг, предоставляемых Компанией, и то, что Компания всегда намеревается предоставлять свои услуги через Интернет-решение, и что риск отмывания денег и финансирования терроризма снижен благодаря

<p>ärisuhte, tehingu iseloomule või tehinguga seotud riskiastmele sobivas ulatuses.</p> <p>Kliendilepingu sõlmimiseks täidab klient ankeedi, kus palutakse esitada peamised hoolsusmeetmete kohaldamiseks vajalikud ning õigusaktides nõutud kohustuslikud andmed. Klient kinnitab esitatud andmete õigsust allkirjaga ning kinnitab, et valeandmete esitamisega või kaasneda nii tsiviil- kui ka kriminaalõiguslik vastutus. Ettevõtte salvestab täidetud ja allkirjastatud ankeedi kliendi kohta peetavas kaustas, kusjuures andmed säilitatakse käesoleva juhendi punktis 6 sätesatud korras.</p> <p>3.1. Ettevõtte kohaldab järgmisi tavapäraseid hoolsusmeetmeid iga kord <u>enne Ärisuhte loomist</u>:</p> <p>3.1.1. Kliendi ja Kliendi esindaja isikusamasuse tuvastamine ning esitatud teabe kontrollimine;</p> <p>3.1.2. Tegelikult kasusaaja tuvastamine ja tema isikusamasuse kontrollimine;</p> <p>3.1.3. Ärisuhtest arusaamine ja asjakohasel juhul selle kohta täiendava teabe kogumine;</p> <p>3.1.4. teabe hankimine asjaolu kohta, kas isik on PEP, tema pereliige või tema lähedaseks kaastöötajaks peetav isik.</p> <p>3.2. Ärisuhtest arusaamise eesmärgiks on selgeks teha, kas Kliendi soov läheb kokku tema tegeliku tegevuse, võime ning vajadustega. Selle jaoks uurib Esindaja Kliendi püsiva asu-, tegevus- või elukoha, tegevusala, olulisemad tehingupartnerid, maksetavad, kogemuse. Kliendiga ärisuhte loomisel ning teenuste osutamisel ärisuhte kestel salvestab ja säilitab Ettevõtte kliendi IP-aadressid. Nende alusel on võimalik jälgida kliendi asukohta ning võrrelda kliendi poolt esitatud vastava informatsiooni õigsust. Juhul, kui kliendi poolt avaldatud informatsioon ei kattu tuvastatud IP-aadressidega või klient kasutab muutuvat IP-aadressi, siis kohaldab Ettevõtte kliendi suhtes täiendavaid hoolsusmeetmeid, et selgitada välja erinevuste või tegevuse põhjuse. Asjakohasel juhtudel kogub</p>	<p>высокому уровню безопасности информационных систем, используемых Компанией, и средствам контроля со стороны клиентов, то деловые отношения между Компанией и клиентом устанавливаются без нахождения в одном месте с клиентом. Компания применяет меры должной осмотрительности в той мере, в какой это соответствует деловым отношениям, характеру операции или степени риска, связанного с операцией.</p> <p>Чтобы заключить клиентский договор, клиент заполняет анкету, в которой его просят предоставить основную обязательную информацию и требуемую законодательством, необходимую для применения мер должной осмотрительности. Клиент подтверждает достоверность предоставленных данных своей подписью и подтверждает, что предоставление ложных данных может повлечь как гражданскую, так и уголовную ответственность. Компания сохраняет заполненную и подписанную анкету в папке для клиента, при этом данные должны храниться в соответствии с процедурой, предусмотренной в пункте 6 настоящего Руководства.</p> <p>3.1. Компания применяет обычные меры прилежания каждый раз <u>перед установлением Деловых отношений</u>:</p> <p>3.1.1. Установление личности Клиента и представителя Клиента и проверка предоставленной информации;</p> <p>3.1.2. Установление Бенефициарного собственника и проверка его личности;</p> <p>3.1.3. Понимание сути Деловых отношений и при необходимости сбор дополнительной информации касательно этого;</p> <p>3.1.4. Получение информации о том, является ли лицо ПДЛ, членом его семьи или его ближайшим сотрудником.</p> <p>3.2. Целью понимания сути Деловых отношений является выяснение, совпадает ли желание Клиента с его фактической деятельностью,</p>
---	--

<p>Ettevõtte täiendavat teavet kliendi kogemuse (kust on klient saanud ärialast teavet, oskust, kontakte koostööpartnerite kohta jms), eesmärgiga tunda klienti maksimaalselt ja tema poolt tulevikus teostatavaid tehinguid, et olla võimeline teostama hiljem ärisuhte seiret.</p> <p>3.3. Ärisuhte vältel teostab Ettevõtte ärisuhte seiret, mis hõlmab Ärisuhtes tehtud Tehingute kontrolli, tagamaks, et Tehingud on kooskõlas Ettevõtte teadmistega Kliendist, tema tegevusest ja riskiprofiilist. Kliendi tehingute analüüsimiseks kasutab Ettevõtte infosüsteemi, mis võimaldab tõsta esile tehinguid etteantud parameetrite alusel. Parameetrid määratakse kindlaks juhatuse otsusega (näiteks pettuslikule tegevusele vastavad tehingud ja muud tüpoloogiate kohaselt virtuaalvääringutega seotud peamised viisid, näiteks klient ostab ja kohe müüb virtuaalvääringu maha, klient ei hooli kahjumist, mis ta tehingutega pidevalt teenib jne). Ettevõtte peab pidevalt skriinima (reaalajas järgima) ning monitoorima (tagantjärele hindama) kliendi tegevust ja hindama kliendi tegevuse muutumist. Skriinimine toimub Ettevõtte infotehnoloogiliste seadmete abil ning monitoorimine toimub kuu lõpus etteantud parameetrite alusel, kus Ettevõtte sõelub välja suurimaid käibeid teinud ja suurimaid üksikuid tehinguid teinud kliendid. Ettevõtte jälgib ka pidevalt, et virtuaalvääringu vahetamiseks kontole debiteeritud rahalised vahendid ei pärineks või kontolt krediteeritud rahalised vahendid ei oleks edastatud suure riskiga riikidesse, ning võtab vajadusel asjakohaseid meetmeid nii maksete peatamiseks kui ka RABi teavitamiseks. Kord aastas toimub Kliendi info uuendamine. Kliendi riski kategooria kuulub ümberhindamisele, kui esinevad vähemalt järgmised tunnused:</p> <p>3.3.1. Kliendi tegevuses esinevad asjaolud, mis viitavad kuritegelikule tegevusele, rahapesule või terrorismi rahastamisele, sh vastav info meedias; või</p> <p>3.3.2. Muutub Kliendi tegevus; või</p>	<p>võimalustega ja vajadustega. Для этого Представитель выясняет постоянное местонахождение, место деятельности или место жительства, сферу деятельности, наиболее важных партнеров по Транзакциям, платежные обычаи/практики, опыт Клиента. При установлении деловых отношений с клиентом и предоставлении услуг в ходе деловых отношений Компания записывает и хранит IP-адреса клиента. На их основе можно отслеживать местонахождение клиента и сравнивать достоверность соответствующей информации, предоставляемой клиентом. Если информация, раскрытая клиентом, не соответствует идентифицированным IP-адресам или клиент использует изменяющийся IP-адрес, Компания применяет к клиенту дополнительные меры должной осмотрительности, чтобы определить причину несоответствий или действий. При необходимости Компания собирает дополнительную информацию об опыте клиента (откуда клиент получил бизнес-информацию, навыки, контакты о партнерах по сотрудничеству и т. д.), чтобы знать клиента в максимальной степени и о будущих транзакциях, чтобы иметь возможность мониторить деловые отношения позже.</p> <p>3.3. В ходе Деловых отношений Компания осуществляет постоянный мониторинг Деловых отношений, который включает в себя проверку Транзакций, совершенных в рамках Деловых отношений, с целью обеспечения соответствия Транзакций знаниям Компании о Клиенте, его деятельности и профиле риска. Для анализа транзакций клиента Компания использует информационную систему, позволяющую выделять транзакции на основе заранее определенных параметров. Параметры определяются решением Правления (например, мошеннические транзакции и другие основные типы сделок, связанных с виртуальной валютой, в соответствии с</p>
--	---

<p>3.3.3. Ärisuhte käigus kogutud andmed ei ole piisavad, andmed on vastuolulised või nende tõele vastavuses võib muul moel kahelda.</p> <p>3.4. Esindaja kogub teavet Kliendi rikkuse päritolu kohta</p> <p>3.4.1. <u>Ärisuhte loomisel</u>, kui see on asjakohane, et tuvastada Ärisuhte eesmärk ja olemus;</p> <p>3.4.2. Kui Esindajal on kahtlus, et Klient/Kliendi esindaja on PEP, tema pereliige või lähedane kaastöötaja.</p> <p>3.5. Esindaja nõudmisel kinnitab Klient/Kliendi esindaja hoolsusmeetmete kohaldamiseks esitatud teabe ja dokumentide õigsust oma allkirjaga.</p> <p>3.6. Ettevõtte alati kohaldab hoolsusmeetmeid tugevdatud korras, kui Kliendile on määratud kõrge riskikategooria (punkt 2.5).</p> <p>3.7. Hoolsusmeetmete tugevdatud korras rakendamine tähendab, et Esindaja kohaldab tavapärasele kohustuslikele hoolsusmeetmetele midagi lisaks:</p> <p>3.7.1. <u>Isikusamasuse tuvastamisel</u> küsib Esindaja täiendavalt lisadokumente esitatud teabe kontrollimiseks, nt teist isikut tõendavat dokumenti või teeb päringu andmebaasi (Lisa 1).</p> <p>3.7.2. <u>Välisriigi juriidilise isiku esindaja esindusõiguse kontrollimisel</u> palub Ettevõtte Esindaja esitama volitusi tõendava notariaalselt või sellega võrdsustatud korras kinnitatud dokumendi, mis on legaliseeritud või kinnitatud apostilliga, kui välislepingust ei tulene teisiti.</p> <p>3.7.3. Täiendava teabe kogumisel <u>Ärisuhte või Tehingu eesmärgi ja olemuse kohta</u> teeb Esindaja päringuid avalikest allikatest, nt internetiotsingud, Google Maps'i kasutamine tegevuskoha kohta informatsiooni hankimiseks jne. või teostab kohapealset visiiti Kliendi juurde.</p> <p>3.7.4. <u>Ärisuhte loomisel</u> tuvastab Esindaja kõigi Kliendi Tegelike kasusaajate, k.a nende, kelle osalus on alla 25%-i, isikusamasust.</p> <p>3.7.5. <u>Ärisuhte loomisel või Ärisuhte seirel</u> taotleb Esindaja Ettevõtte</p>	<p>типологиями, например, клиент покупает и немедленно продает виртуальную валюту, клиент не заботится о потерях, которые он постоянно получает от транзакций, и т. д.). Компания должна постоянно проверять (контролировать в реальном времени) и отслеживать (оценивать постфактум) деятельность клиента и оценивать изменения в деятельности клиента. Скрининг проводится с использованием инфотехнологических решений Компании, а мониторинг осуществляется в конце месяца на основе заранее определенных параметров, при этом Компания проверяет клиентов, совершивших наибольшие обороты и крупнейшие отдельные транзакции. Компания также постоянно следит за тем, чтобы средства, списанные со счета для обмена виртуальной валюты, не поступали или средства, зачисленные на счет, не переводились в страны с высоким уровнем риска, и принимает соответствующие меры для приостановки платежей и, при необходимости, информирования БДО. Информация о Клиенте обновляется один раз в год, при этом присвоенная Клиенту категория риска подлежит переоценке, если присутствуют по крайней мере следующие характеристики:</p> <p>3.3.1. В деятельности Клиента появляются обстоятельства, которые указывают на преступную деятельность, отмывание денег или финансирование терроризма, в т. ч. информация в средствах массовой информации; или</p> <p>3.3.2. Изменения в деятельности Клиента; или</p> <p>3.3.3. Данные, собранные во время Деловых отношений, недостаточны, противоречивы или в их достоверности можно иным образом усомниться.</p> <p>3.4. Представитель собирает информацию об источнике состояния Клиента:</p> <p>3.4.1. <u>При установлении Деловых отношений</u>, если это</p>
--	---

<p>kõrgema juhtkonna heakskiitu Ärisuhte loomiseks, jätkamiseks või lõpetamiseks.</p> <p>3.7.6. Kliendi <u>keeruka omandistruktuuri puhul</u> tuvastab Esindaja põhjendused ja asjaolusid, miks Klient kasutab keerukaid omandistruktuure ja/või on registreerinud äriühingu just konkreetsesse riiki.</p> <p>3.7.7. <u>Ärisuhte seirel</u> hindab Esindaja uuesti Kliendi riskiprofiili hiljemalt kuus kuud pärast Ärisuhte loomist.</p> <p>3.7.8. Esindaja hangib teabe Kliendi ja tema Tegeliku kasusaaja <u>rikkuse allika ja/või päritolu</u> kohta.</p> <p>3.7.9. Esindaja küsib täiendava teabe ja dokumente Ärisuhtes tehtavate <u>Tehingute</u> tegeliku teostamise kohta, et välistada Tehingute näilisus (nt tollidokumentid, kaupade kindlustuslepingud jne).</p> <p>3.7.10. <u>Tehinguga</u> seotud esimene makse toimub konto kaudu, mis on avatud Tehingus osaleva Kliendi nimel krediitiasutuses, mis on registreeritud või mille tegevuskoht on Euroopa Majanduspiirkonna lepinguriigis.</p> <p>3.7.11. Kui Klient, Kliendi esindaja, Kliendi pereliikme või lähedane kaastöötaja on PEP, siis Esindaja:</p> <p>3.7.11.1. saab kõrgemalt juhtkonnalt heakskiidu selle isikuga <u>ärisuhte loomiseks või jätkamiseks</u>;</p> <p>3.7.11.2. rakendab meetmeid, et teha kindlaks selle <u>isiku rikkuse päritolu ja nende rahaliste vahendite allikad</u>, mida Ärisuhtes kasutatakse;</p> <p>3.7.11.3. <u>hindab uuesti isiku riskiprofiili</u> hiljemalt 6 kuud pärast Ärisuhte loomist.</p> <p>3.8. Kui Klient tegutseb suure riskiga kolmandas riigis (Lisa 1), siis kohaldab Esindaja järgmisi hoolsusmeetmeid:</p> <p>3.8.1. lisateabe hankimine Kliendi ja tema Tegeliku kasusaaja kohta;</p> <p>3.8.2. lisateabe hankimine Ärisuhte planeeritava sisu kohta;</p> <p>3.8.3. teabe hankimine Kliendi ja tema Tegeliku kasusaaja rahaliste vahendite ning rikkuse päritolu kohta;</p>	<p>целесообразно, чтобы определить цель и суть Деловых отношений;</p> <p>3.4.2. Если Представитель подозревает, что Клиент/представитель Клиента является ПДЛ, членом его семьи или его ближайшим сотрудником.</p> <p>3.5. По требованию Представителя Клиент/представитель Клиента подтверждает верность информации и документов, предоставленных при проведении мер прилежания, своей подписью.</p> <p>3.6. Компания всегда применяет меры прилежания в усиленном порядке, когда Клиенту присваивается категория высокого риска (пункт 2. 5).</p> <p>3.7. Применение мер прилежания в усиленном порядке означает, что Представитель применяет в дополнение к обычным мерам прилежания что-то еще из списка:</p> <p>3.7.1. <u>При установлении личности</u> Представитель просит предоставить дополнительные документы для проверки предоставленной информации, например, другой документ, удостоверяющий личность, или делает запрос в базе данных (Приложение 1).</p> <p>3.7.2. <u>При проверке представительских полномочий представителя иностранного юридического лица</u>, Представитель Компании запрашивает подтверждающий полномочия документ, заверенный в нотариальном или в приравненном к нему порядке, который легализован или заверен апостилом, если иное не вытекает из международного договора.</p> <p>3.7.3. При сборе дополнительной информации касательно <u>цели и сути Деловых отношений или Транзакции</u>, Представитель делает запросы в открытых источниках, например, поиск в интернете, использование Google Maps для получения информации о местонахождении и т.д. или осуществляет визит к Клиенту.</p>
--	--

<p>3.8.4. teabe hankimine planeeritud Tehingute põhjuste kohta;</p> <p>3.8.5. Ettevõtte kõrgemalt juhtkonnalt loa saamine Ärisuhte loomiseks või selle jätkamiseks;</p> <p>3.8.6. Ärisuhte seirel Kliendi riskiprofiili uuesti hindamine hiljemalt 6 kuud pärast Ärisuhte loomist.</p> <p>3.9. <u>Ettevõtte ei loo Ärisuhet</u>, kui ta ei suuda täita Juhendi punktis 3.1.1-3.1.2 sätestatud hoolsusmeetmeid, potentsiaalse Kliendi kapitali moodustavad esitajaaktsiad/muud esitajaväärtpaberid või kui Ettevõttel on rahapesu või terrorismi rahastamise kahtlus. Kui nimetatud olukorras on <u>Ettevõttel Kliendiga Ärisuhe</u>, loetakse Kliendi poolt hoolsusmeetmete rakendamiseks vajaliku teabe või dokumentide andmisest keeldumine oluliseks lepingu rikkumiseks ning Ettevõttel on kohustus kliendileping etteteatamistähtaega järgimata erakorraliselt üles öelda ja teavitada RABi Juhendi peatükis 5 sätestatud korras. Ärisuhe loetakse lõppenuks ülesütlemisteate esitamisega Kliendile, mille järel piirab Ettevõtte teenuse osutamise Kliendile täielikult.</p> <p>3.10. Esindaja <u>keeldub Tehingu tegemisest</u>, kui</p> <p>3.10.1. Klient ei esita dokumente ja asjakohast teavet või Tehingu objektiks oleva vara päritolu tõendavaid andmeid/dokumente, või</p> <p>3.10.2. kui esitatud andmete ja dokumentide põhjal tekib kahtlus, et tegemist võib olla rahapesu või terrorismi rahastamisega või sellega seotud kuritegude toimepanemisega või sellise tegevuse katsega.</p> <p>3.11. Esindaja kohaldab hoolsusmeetmeid lihtsustatud korras, kui Kliendile ja Tehingule on määratud madala riski kategooria (punkt 2.6):</p> <p>3.11.1. Kliendi/Kliendi esindaja isikutuvastamist, esindusõiguse tuvastamist ja esitatud teabe kontrollimist usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal teostab Esindaja <u>Ärisuhte loomise ajal</u>, kui seda on vaja, et äritegevuse tavapärasest käiku mitte</p>	<p>3.7.4. <u>При установлении Деловых отношений</u>, Представитель устанавливает личность всех Бенефициарных собственников Клиента, в т. ч. тех, чье участие составляет менее 25%.</p> <p>3.7.5. <u>При установлении Деловых отношений или мониторинге Деловых отношений</u> Представитель Компании запрашивает одобрение высшего руководства Компании для установления, продолжения или прекращения Деловых отношений.</p> <p>3.7.6. <u>В случае сложной структуры собственников</u> Клиента Представитель устанавливает обоснования и обстоятельства, почему Клиент использует сложные структуры собственников и/или зарегистрировал компанию в конкретной стране.</p> <p>3.7.7. <u>При мониторинге Деловых отношений</u>, Представитель переоценивает категорию риска Клиента не позднее чем через 6 месяцев после установления Деловых отношений.</p> <p>3.7.8. Представитель узнает информацию об <u>источнике и/или происхождении состояния</u> Клиента и его Бенефициарного собственника.</p> <p>3.7.9. Представитель запрашивает дополнительную информацию и документы по фактическому совершению <u>Транзакций</u> в Деловых отношениях, чтобы исключить ничтожность Транзакции (например, таможенные документы, договоры страхования товаров и т.д.).</p> <p>3.7.10. Производство первого связанного с Транзакцией платежа через счет Клиента, который открыт в кредитном учреждении, зарегистрированным или имеющим место деятельности в государстве – участнике ЕЭЗ.</p> <p>3.7.11. Если Клиент, представитель Клиента, член семьи Клиента или его ближайший сотрудник</p>
--	--

<p>häirida. Sellisel juhul viib Esindaja isikusamasuse kontrolli lõpule võimalikult kiiresti ning enne siduvate toimingute tegemist (nt enne laenulepingu sõlmimist).</p> <p>3.11.2. Ärisuhte seire lihtsustatud korras on lubatud, kui on täidetud kõik järgmised tingimused:</p> <p>3.11.2.1. Kliendiga on sõlmitud kirjalikus või elektroonilises vormis kestavusleping;</p> <p>3.11.2.2. Ettevõttele laekuvad Ärisuhte raames maksed ainult konto kaudu, mis asub Eestis äriregistrisse kantud krediitiasutuses või välisriigi krediitiasutuse filiaalis või krediitiasutuses, mis on asutatud või mille tegevuskoht on Euroopa Majanduspiirkonna lepinguriigis või riigis, kus kohaldatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849 nõuetega võrdväärseid nõudeid;</p> <p>3.11.2.3. Ärisuhtes tehtavate Tehingute sissetulevate või väljaminevate maksete koguväärtus aastas ei ületa 15 000 eurot.</p> <p>3.12. Ettevõtte esitab Kliendile enne temaga Ärisuhte loomist isikuandmete töötlemist puudutava teabe, sh üldise teabe Ettevõtte RahaPTSist tulenevate kohustuste kohta isikuandmete töötlemisel rahapesu ja terrorismi rahastamise tõkestamise eesmärgil.</p>	<p>является ПДЛ, то Представитель:</p> <p>3.7.11.1. Получает одобрение высшего руководства Компании для <u>установления или продолжения Деловых отношений</u> с этим лицом;</p> <p>3.7.11.2. Применяет меры по выявлению <u>источника состояния</u> этого лица и <u>источников денежных средств</u>, которые используются в Деловых отношениях;</p> <p>3.7.11.3. <u>Переоценивает категорию риска</u> этого лица не позднее, чем 6 месяцев после установления Деловых отношений.</p> <p>3.8. Если Клиент действует в третьем государстве с высоким риском (Приложение 1), то Представитель применяет следующие меры прилежания:</p> <p>3.8.1. Получение дополнительной информации о Клиенте и его Бенефициарном собственнике;</p> <p>3.8.2. Получение дополнительной информации о содержании планируемых Деловых отношений;</p> <p>3.8.3. Получение информации об источнике состояния и денежных средств Клиента и его Бенефициарного собственника;</p> <p>3.8.4. Получение информации о причинах планируемых Транзакций;</p> <p>3.8.5. Получение разрешения от высшего руководства Компании на установление или продолжение Деловых отношений;</p> <p>3.8.6. При мониторинге Деловых отношений переоценка категории риска Клиента в течение 6 месяцев после установления Деловых отношений.</p> <p>3.9. Компания не устанавливает <u>Деловых отношений</u>, если она не может выполнить меры прилежания, изложенные в пунктах 3.1.1-3.1.2 Руководства, капитал потенциального Клиента состоит из</p>
--	--

представительских акций/других ценных бумаг на предъявителя, или если у Компании есть подозрение в отмывании денег или финансировании терроризма. Если в данной ситуации у Компании Деловые отношения с Клиентом, отказ Клиента в выдаче информации или документов в ходе выполнения мер прилежания, считается существенным нарушением договора, и Компания обязана отказаться от клиентского договора в исключительном порядке без предварительного уведомления и сообщить об этом в БДО в порядке, указанном в пункте 5. Деловые отношения считаются прекращенными с предоставлением сообщения Клиенту об отказе от договора, после чего Компания полностью ограничивает оказание услуг Клиенту.

3.10. Представитель отказывается от совершения Транзакции, если

3.10.1. Клиент не предоставляет документы и соответствующую информацию или данные/документы, подтверждающие происхождение имущества, которое является объектом Транзакции, или

3.10.2. На основе предоставленной информации и документов возникает подозрение, что может иметь место отмывание денег или финансирование терроризма, или совершение связанных с этим преступлений или попытка совершения таких действий.

3.11. Представитель применяет **меры прилежания в упрощенном порядке**, если Клиенту и Транзакции присвоена категория низкого риска (пункт 2.6):

3.11.1. Представитель осуществляет установление личности Клиента/представителя Клиента, установление представительских полномочий и проверку предоставленных данных на основе информации, полученной из достоверного и независимого источника в момент создания Деловых отношений, если это

необходимо, чтобы не нарушать привычный ход деловой деятельности. В этом случае Представитель доводит проверку подлинности личности до конца как можно скорее и перед совершением обязующих действий (например, до заключения кредитного договора).

3.11.2. Мониторинг Деловых отношений в упрощенном порядке

допускается при соблюдении всех следующих условий:

3.11.2.1. С Клиентом заключен долгосрочный договор в письменной или электронной форме;

3.11.2.2. В рамках Деловых отношений платежи поступают в Компанию только через счет, открытый во внесенном в коммерческий регистр Эстонии кредитном учреждении, или в таком филиале иностранного кредитного учреждения, или кредитном учреждении, которое учреждено или местом деятельности которого является государство-участник ЕЭЗ или страна, где действуют требования эквивалентные требованиям Директивы Европейского Парламента и Совета (ЕС) 2015/849;

3.11.2.3. Общая ценность входящих или исходящих платежей по Транзакциям в Деловых отношениях не превышает 15 000 евро в год.

3.12. Перед установлением Деловых отношений Компания предоставляет Клиенту информацию об обработке персональных данных, в т. ч. общую информацию о вытекающих из Закона обязательствах по обработке личных данных с целью предотвращения отмывания денег и финансирования терроризма.

4. Isikusamasuse tuvastamise kord

- 4.1. Esindaja peab iga kord enne Kliendiga Tehingu tegemist või Ärisuhte loomist kohaldama alljärgnevaid protseduureegleid.
- 4.2. Esindaja tuvastab füüsilise isiku ning säilitab tema kohta järgmised andmed:
 - nimi;
 - isikukood, selle puudumise korral sünniaeg ja -koht ning elu- või asukoht;
 - teave esindusõiguse ja selle ulatuse tuvastamise ja kontrollimise kohta. Kui esindusõigus ei tulene seadusest, siis esindusõiguse aluseks oleva dokumendi nimetus (nt volikiri), väljaandmise kuupäev ja väljaandja nimi või nimetus.
- 4.3. Esindaja kontrollib Juhendi punktis 4.2 esitatud teavet teisest usaldusväärsest ja sõltumatust allikast, nt kasutades teist ametlikku dokumenti (punkti 4.4 loetelust) või selle notariaalselt tõestatud või notariaalselt/ametlikult kinnitatud koopiat, tugevat autentimist võimaldava digitaalset isikutuvastusvahendit, andmete kontrolli rahvastikuregistri või muu samaväärse registri kaudu, muu teavet et kontrollida isikuga vahetult seotud andmeid (nt töö või elu kohta, s.o.: kommunaalteenuste või muu arve, mis tõendab isiku elamist või asumist viidatud kohas; dokument, mis tõendab kutse- või tegevusalal tegutsemist; makse, mis on tehtud isiku poolt avatud kontolt krediidi- või makseasutuses, mis omab tegevusluba võrdväärse riigis).
- 4.4. Esindaja tuvastab füüsilise isiku isikusamasuse järgmiste dokumentide alusel:
 - isikutunnistus;
 - digitaalne isikutunnistus;
 - elamisloakaart;
 - Eesti kodaniku pass;
 - diplomaatiline pass;
 - meremehe teenistusraamat;
 - välismaalase pass;
 - ajutine reisidokument;
 - pagulase reisidokument;
 - meresõidutunnistus;
 - tagasipöördumistunnistus;

4. Порядок установления личности

- 4.1. Представитель должен применять следующие процедурные правила каждый раз перед осуществлением Транзакцию или установлением Деловые отношения с Клиентом.
- 4.2. Представитель идентифицирует физическое лицо и сохраняет следующую информацию:
 - Имя, фамилия;
 - Личный персональный код, при его отсутствии дата и место рождения, место проживания или нахождения;
 - Информация об установлении и проверке представительских полномочий и их объема. Если право на представительство не вытекает из закона, название документа, которое лежит в основе права на представительство (например, доверенность), дата выдачи и имя или название того, кто выдал.
- 4.3. Представитель проверяет предоставленную информацию, перечисленную в пункте 4.2, в другом надежном и независимом источнике, например, используя другой официальный документ (из списка 4.4), или его нотариально заверенную или нотариально/официально заверенную копию, цифровой способ установления личности, позволяющий сильную аутентификацию, проверку данных через регистр народонаселения или другой эквивалентный регистр, другую информацию для проверки данных, непосредственно связанной с лицом (например, о работе или жизни, т. е.: счет за коммунальные услуги или другой счет, подтверждающий, что лицо проживает или находится в указанном месте; документ, подтверждающий занятие профессиональной или торговой деятельностью; платеж, произведенный со счета, открытого

<ul style="list-style-type: none"> • tagasipöördumise luba; • välisriigis välja antud kehtiv reisidokument (Lisa 1); • juhiluba, kui dokumenti on kantud kasutaja nimi, foto või näokujutis, allkiri või allkirjakujutis ja sünniaeg või isikukood. <p>4.5. Kui punktis 4.4 nimetatud originaaldokumenti ei ole võimalik näha, võib Esindaja kasutada isikusamasuse kontrollimiseks notariaalselt tõestatud või notariaalselt/ametlikult kinnitatud dokumenti või muud usaldusväärsest ja sõltumatust allikast pärit teavet, sh e-identimise vahendeid, kasutades sel juhul andmete kontrollimiseks vähemalt kahte erinevat allikat (Juhendi punktis 4.3 toodud allikad).</p> <p>4.6. Esindaja teeb isikut tõendava dokumendi isikuandmete ja fotoga leheküljest koopia.</p> <p>4.7. Töötaja tuvastab juriidilise isiku isikusamasuse ja säilitab tema kohta järgmised andmed:</p> <ul style="list-style-type: none"> • juriidilise isiku ärinimi; • registrikood või registreerimisnumber ja -aeg; • juhataja nimi või juhatuse liikmete või muu seda asendava organi liikmete nimed ja nende volitused juriidilise isiku esindamisel; • juriidilise isiku sidevahendite andmed. <p>4.8. Juriidilise isiku isikusamasuse tuvastamiseks kasutatakse järgmised dokumendid:</p> <ul style="list-style-type: none"> • asjakohase registri registrikaart, • asjakohase registri registreerimistunnistus, või • nimetatud dokumentidega võrdväärne dokument (nt Certificate of Good Standing, Certificate of Incumbency, Certificate of Incorporation jt). <p>Nimetatud dokumendid peavad olema välja antud mitte varem kui 1 kuu enne nende esitamist Ettevõttele.</p> <p>4.9. Esindaja veendub Kliendi ärinime ja registrikoodi/registreerimisnumbri ja -aja andmete õigsuses, kasutades</p>	<p>лицом в кредитном или платежном учреждении, уполномоченном в эквивалентной стране).</p> <p>4.4. Представитель устанавливает личность физического лица на основе следующих документов:</p> <ul style="list-style-type: none"> • Удостоверение личности; • Цифровое удостоверение личности; • Карта вида на жительство; • Паспорт гражданина Эстонии; • Дипломатический паспорт; • Служебная книжка моряка; • Паспорт иностранца; • Временный проездной документ; • Проездной документ беженца; • Свидетельство о мореплавании; • Свидетельство о возвращении; • Разрешение на возвращение; • Действительный проездной документ, выданный иностранным государством (Приложение 1); • Водительское удостоверение, если в документ внесены имя, фотография или изображение лица, подпись или изображение подписи и дата рождения или личный персональный код. <p>4.5. Если невозможно увидеть исходный документ, указанный в пункте 4.4, Представитель может использовать для проверки личности нотариально или официально заверенный документ или другую информацию из надежного и независимого источника, включая электронные средства идентификации, используя в этом случае, по крайней мере, два различных источника для проверки данных (источники, указанные в пункте 4.3 Руководства).</p> <p>4.6. Представитель делает копию документа, удостоверяющего личность, со страницы личных данных и фотографии.</p>
--	---

<p>selleks usaldusväärsest ja sõltumatust allikast pärit teavet, sh andmeid ametlikest registritest. Kui punktis 4.8 nimetatud originaaldokumenti ei ole võimalik näha, võib kasutada notariaalselt tõestatud või notariaalselt/ametlikult kinnitatud dokumenti või e-identimise ja e-tehingute usaldusteenuste vahendeid, kasutades sel juhul andmete kontrollimiseks vähemalt kahte erinevat allikat (nt lisapäringud riiklikes ja eraõiguslikes andmebaasides; makse, mis on tehtud isiku poolt avatud kontolt krediidi- või makseasutuses, mis omab tegevusluba võrdväärse riigis; kommunaalteenuste või muu arve, mis tõendab isiku tegutsemist viidatud kohas; muu usaldusväärsest ja sõltumatust allikast saadud teave). Kui Ettevõttel on ligipääs äriregistri, mittetulundusühingute ja sihtasutuste registri või välisriigi asjakohaste registrite andmetele arvutivõrgu kaudu, ei pea kliendilt nõudma punktis 4.7 sätestatud andmete esitamist.</p> <p>4.10. Isikusamasuse tuvastamine infotehnoloogiliste vahendite abil on kohustuslik Ettevõttele, kui hoolsusmeetmeid ei kohaldata isiku või tema esindajaga samas kohas viibides ning</p> <p>4.10.1. Ärisuhe luuakse <u>e-residendiga või isikuga, kes on pärit (sh elu- või asukoht) Euroopa Majanduspiirkonna välisest riigist;</u></p> <p>4.10.2. Ärisuhe luuakse <u>isikuga, kes on pärit (sh elu- või asukoht) Euroopa Majanduspiirkonna lepinguriigist</u> ning kelle Tehinguga või teenuse osutamise lepinguga seotud väljaminevate maksete kogusumma ühes kalendrikuus ületab füüsilisest isikust Kliendi puhul 15 000 eurot ja juriidilisest isikust Kliendi puhul 25 000 eurot.</p> <p>4.11. Infotehnoloogiliste vahendite abil isikusamasuse tuvastamiseks ja andmete kontrollimiseks kasutab Esindaja isiku ID-kaarti, elamisloakaarti, e-residendi digi-ID või muud kõrge usaldusväärse tasemega e-identimise süsteemi, mis on kantud EL usaldusnimekirjade lehitseja nimekirja (Lisa 1).</p> <p>4.12. Kui isik on <u>välisriigi kodanik</u>, küsib Esindaja lisaks punktis 4.11</p>	<p>4.7. Представитель идентифицирует юридическое лицо и сохраняет следующие данные:</p> <ul style="list-style-type: none"> • Наименование юридического лица; • Регистровый код или регистрационный номер и дату регистрации; • Имя руководителя или имени членов правления или замещающего его органа и их полномочия в представлении юридического лица; • Телекоммуникационные данные юридического лица. <p>4.8. Для идентификации юридического лица используются следующие документы:</p> <ul style="list-style-type: none"> • Регистрационная карта соответствующего регистра; • Свидетельство о регистрации из соответствующего регистра; или • Документ эквивалентный указанным документам (например, Certificate of Good Standing, Certificate of Incumbency, Certificate of Incorporation и т.д.). <p>Указанные документы должны быть выданы не ранее чем за 1 месяц до их предоставления Компании.</p> <p>4.9. Представитель убеждается в верности имени регистрационного кода/регистрационного номера и даты регистрации Клиента, используя для этого информацию из надежного и независимого источника, включая данные из официальных регистров. Если невозможно увидеть оригинал документа, указанного в пункте 4.8, можно использовать нотариально или официально заверенный документ или средства цифровой идентификации и электронных транзакций, используя в этом случае, по крайней мере, два различных источника для проверки данных (например, дополнительные запросы в государственные и частные базы данных; платеж, произведенный со счета, открытого лицом в кредитном</p>
---	---

<p>nimetatule samaaegselt ka välisriigi pädeva asutuse välja antud isikut tõendavat dokumenti.</p> <p>4.13. Infotehnoloogiliste vahendite abil isikusamasuse tuvastamisel kasutab Esindaja lisaks usaldusväärsest ja sõltumatust allikast pärit teavet (punkt 4.3) ning järgib ka RahaPTS-i ning RahaPTS § 31 lg 6 volitusnormi alusel kehtestatud rahandusministri määrust.</p> <p>4.14. Video abil isikusamasust tuvastades järgib Ettevõtte volitusnormi alusel kehtestatud rahandusministri määrust ning teeb oma veebilehel üldsusele kättesaadavaks nimetatud määruuses ettenähtud teabe infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise kohta. Isikusamasuse tuvastamine ja andmete kontrollimise protsessi edukas läbiviimine ei kohusta Ettevõtet kliendisuhet looma ega teenuste kättesaadavust tagama. Ettevõttel on õigus valida, kellega ta kliendisuhete loob ja kellega mitte.</p> <p>4.15. Ettevõtte kasutab infotehnoloogiliste vahendite abil isikusamasuse tuvastamisel ja kontrollimisel kõrge usaldusväärsuse tasemega tehnilisi vahendeid, mis tagavad tõsikindla isikusamasuse tuvastamise ning võimaldavad ära hoida edastatavate andmete muutmise või väärkasutamise. Ettevõtte tuvastab kliendi tegeliku nime ja isikusamasuse ning veendub, et eelnimetatud isik ei kasuta võõrast identiteeti.</p> <p>4.16. Ettevõtte kasutab infotehnoloogilisi vahendeid, mis võimaldavad isikusamasuse tuvastamise ja kontrollimise protseduuri salvestada ja seda taasesitada. Ettevõtte kasutab isikusamasuse tuvastamiseks sellist infotehnoloogilist vahendit, millel on biomeetriliste andmete digitaalseks tuvastamiseks vajalik riist- ja tarkvara ja mis võimaldab biomeetriliste andmete võrdlemist. Video peab olema piisava kvaliteediga, s.o piisav, selge ja kvaliteetne, et isiku isikusamasust oleks võimalik tuvastada ja seda kontrollida.</p> <p>4.17. Video vahendusel toimuva isikusamasuse tuvastamise ja andmete kontrollimise jaoks vajab tuvastatav isik</p>	<p>или платежном учреждении, уполномоченном в эквивалентной стране; счет за коммунальные услуги или другой счет, подтверждающий деятельность лица в указанном месте; другая информация, полученная из надежного и независимого источника). Если Компания имеет доступ к данным коммерческого регистра, реестра некоммерческих объединений и фондов или соответствующих иностранных регистров через компьютерную сеть, от клиента не требуется предоставлять данные, указанные в пункте 4.7.</p> <p>4.10. Идентификация лица с помощью инфотехнологических решений является обязательным для Компании, если Представитель не проводит меры прилежания, находясь в одном месте с лицом или его представителем, и</p> <p>4.10.1. Деловые отношения устанавливаются с <u>э-резидентом или лицом, которое по происхождению (включая место жительства или место нахождения) из страны, не входящей в ЕЭЗ;</u></p> <p>4.10.2. Деловые отношения устанавливаются с <u>лицом, которое по происхождению (включая место жительства или место нахождения) из страны ЕЭЗ,</u> и общая сумма исходящих платежей, связанных с Транзакцией или договором оказания услуг, в календарном месяце превышает 15 000 евро в случае Клиента-частного лица и 25 000 евро в случае Клиента-юридического лица.</p> <p>4.11. Для установления личности и проверки данных с помощью инфотехнологических решений Представитель использует ИД-карту, карточку вида на жительство, диги-ИД э-резидента или другую систему э-идентификации с высоким уровнем безопасности, включенную в Доверительный список ЕС (Приложение 1).</p> <p>4.12. Если лицо является <u>иностранным гражданином,</u> то дополнительно к документу, указанному в пункте 4.11,</p>
--	--

<p>lisaks punktides 4.11. ja 4.12. nimetatud dokumentidele järgnevaid vahendeid:</p> <p>4.17.1. biomeetriliste andmete digitaalseks tuvastamiseks vajalik riist- ja tarkvara;</p> <p>4.17.2. internetiühendust, veebikaamerat ja mikrofoni. Isikutuvastamise sessioon peab olema püsiv. Isik ei tohi lahkuda sessiooni ajal kaadrist või kaamera vaateväljast. Kui isik ei ole tegutsenud aktiivselt 15 minutit Ettevõtte infosüsteemis, loeb Ettevõtte isikusamasuse tuvastamise ebaõnnestunuks.</p> <p>4.17.3. Veebilehitsejat.</p> <p>4.18. Isikusamasuse tuvastamine ja andmete kontroll toimub järgmiste etappidena:</p> <p>4.18.1. Ettevõtte identifitseerib isiku digitaalset tuvastamist võimaldava isikut tõendava dokumendi abil, millega isik logib sisse Ettevõtte e-keskkonda.</p> <p>4.18.2. Õnnestunud identifitseerimise järel annab isik seadusest tulenevad kinnitused, mis on vajalikud sessiooni jätkamiseks ning täidab ankeetküsitluse ja allkirjastab selle digitaalselt;</p> <p>4.18.3. välisriigi kodanik näitab kaamerasse oma kehtivat välisriigi reisidokumendi. Eesti ID-kaardi või mobiil-ID abil identifitseerinud isiku foto kuvab Ettevõtte ekraanile süsteem. Ettevõtte kontrollib isiku reaajas video teel kaamerast nähtava isikukujutise ja dokumendifoto kokkulangevust.</p> <p>4.18.4. Ettevõtte viib isikuga läbi intervjuu reaajas, mille käigus Ettevõtte täidab tunne-oma-klienti põhimõtet ja selgitab välja kliendisuhete loomise asjaolud. Intervjuu käigus esitab Ettevõtte ankeedi vastuste põhjal isikule kontrollküsimusi isikuandmete kontrollimiseks või täpsustamiseks ning küsib vajadusel lisaandmeid isiku riskiprofiili selgitamiseks. Esindaja on kohustatud hindama intervjuu käigus isiku reageeringut, saadud info ja andmete usaldusväärsust ja kooskõla muude protseduuridega saadud info või andmetega ja</p>	<p>Представитель запрашивает удостоверяющий личность документ, выданный компетентным органом иностранного ведомства.</p> <p>4.13. При идентификации лица с помощью инфотехнологических решений Представитель дополнительно использует информацию из надежного и независимого источника (пункт 4.3), а также соблюдает постановление Министра финансов, установленное на основании разрешительной нормы § 31 ч. 6 Закона.</p> <p>4.14. При идентификации лица с помощью видео Компания соблюдает постановление Министра финансов, установленное на основании разрешительной нормы, и делает доступной для общественности на своем веб-сайте информацию, предусмотренную постановлением об идентификации и проверке данных с помощью информационных технологий. Идентификация и успешное завершение процесса проверки данных не обязывают Компанию устанавливать отношения с клиентами или обеспечивать доступность услуг. Компания имеет право выбирать, с кем она устанавливает клиентские отношения, а с кем нет.</p> <p>4.15. Компания использует высоконадежные технические средства для идентификации и проверки информации с помощью инфотехнологических решений, которые обеспечивают надежную идентификацию и предотвращают изменение или неправомерное использование передаваемых данных. Компания идентифицирует настоящее имя и личность клиента и следит за тем, чтобы вышеупомянутое лицо не использовало чужую личность.</p> <p>4.16. Компания использует инфотехнологические решения, которые позволяют записывать и воспроизводить процедуры идентификации и проверки. Компания использует инфотехнологические решения для идентификации, которые имеют необходимое оборудование и</p>
---	--

<p>kajastama nii hinnangu kui ka selle aluseks olevad asjaolud kliendiprofilis. Kui isikuga ei ole võimalik arusaadavalt suhelda või esineb muu asjaolu, mis takistab intervjuu läbiviimist, tuleb Ettevõtte see protseduur katkestada.</p> <p>4.19. Ettevõtte loeb isikusamasuse tuvastamise ja andmete kontrollimise ebaõnnestunuks, kui:</p> <p>4.19.1. isik on tahtlikult esitanud andmeid, mis ei vasta isikut tõendavate dokumentide andmekogusse kantud andmetele või andmed ei lange kokku sessiooni käigus saadud muu info või andmetega;</p> <p>4.19.2. sessioon isikusamasuse tuvastamise, ankeetküsitluse või intervjuu käigus katkeb või kui 15 minuti jooksul ei ole isik viinud lõpuni Ettevõtte e-keskkonnas ühtegi toimingut;</p> <p>4.19.3. heli ja kujutist edastav infovoog ei vasta käesolevates protseduurireeglites kehtestatud nõuetele;</p> <p>4.19.4. Ettevõtte infosüsteemis tekivad digitaalsel tuvastamisel, digitaalsel allkirjastamisel või sessiooni salvestamisel tõrked;</p> <p>4.19.5. isik ei anna sessiooni käigus nõutud kinnitusi;</p> <p>4.19.6. isik ei täida Ettevõtte juhiseid, näiteks ei eemalda pea- või näokatet, prille, ei muuda keha- või peaaasendit, ei näita dokumendile kantud andmeid kaamerasse;</p> <p>4.19.7. isik kasutab Ettevõtte loata teise isiku abi;</p> <p>4.19.8. ilmnevad asjaolud, mis viitavad rahapesu või terrorismi rahastamise kahtlusele.</p> <p>4.20. Nõuded kujutist ja heli salvestavale infovoole (video) ning videoga kogutud andmetele:</p> <p>4.20.1. kujutist ja heli sisaldav infovoog salvestatakse viisil, mis võimaldab selle taasesitamist samaväärse kvaliteediga kui algselt toimunud sünkroniseeritud heli ja kujutise edastamine;</p> <p>4.20.2. kujutist ja heli sisaldav infovoog salvestatakse koos ajatempliga, kliendi IP-aadressi, tuvastatava</p>	<p>programmne обеспечение для цифровой идентификации биометрических данных и позволяют сравнивать биометрические данные. Видео должно быть достаточно качественным, то есть достаточным, четким и высококачественным, чтобы можно было идентифицировать и проверить личность.</p> <p>4.17. Чтобы идентифицировать и проверить данные по видео, идентифицируемое лицо также должно иметь в добавок к установленным в пунктах 4.11. и 4.12. документам следующие инструменты:</p> <p>4.1.7.1. аппаратное и программное обеспечение для цифровой идентификации биометрических данных;</p> <p>4.1.7.2. подключение к интернету, веб-камера и микрофон. Сеанс аутентификации должен быть постоянным. Во время сеанса человек не должен покидать кадр или поле зрения камеры. Если человек не был активен в информационной системе Компании в течение 15 минут, Компания считает идентификацию неудачной.</p> <p>4.1.7.3. веб-браузер.</p> <p>4.18. Идентификация и проверка данных происходит в следующие этапы:</p> <p>4.18.1. Компания идентифицирует человека с помощью документа, удостоверяющего личность, позволяющего цифровую идентификацию, с помощью которого лицо входит в электронную среду Компании;</p> <p>4.18.2. После успешной идентификации человек предоставляет юридические подтверждения, необходимые для продолжения сеанса, заполняет анкету и подписывает ее цифровой подписью;</p> <p>4.18.3. иностранный гражданин показывает на камеру действующий заграничный проездной документ. Система отображает фотографию человека, который был идентифицирован с помощью эстонской ID-карты или</p>
--	--

<p>isiku, tuvastatava isiku isikukoodiga, isikukoodi puudumisel sünniaja ja –kohaga ning elukohariigiga, kusjuures ajatempel on seotud seda puudutavate andmetega sellisel viisil, et iga hilisem andmemuudatus, selle muudatuse tegija, aeg, viis ja põhjus on tuvastatavad.</p> <p>4.20.3. intervjuu sessiooni pildi- ja helikvaliteet peab võimaldama ärisuhet loova isikuga suhelda, mistõttu Ettevõtte hindab eraldi kliendi infotehnoloogiliste vahendite pildi- ja helikvaliteeti. Koht, kus isik viibib, peab olema piisava valgusega ja kõne ei tohi olla häiritud akustiliselt (kaja, taustamüra). Oluline on see, et kõnest arusaamine poleks häiritud. Heli ja kujutist edastav infovoog peab olema piisavalt kvaliteetne tagamaks, et isiku nägu oleks võimalik näha ja üheselt tuvastada, isiku pea ja õlad peavad olema nähtaval ja kadreeritud. Tehnoloogiline lahendus peab edastama värvilist pilti koos selge heliga ning tagama taasesitatava salvestuse. Heli ja pilt peavad olema sünkroonsed ja taasesitatavad ilma märgatava viivitusega. Lisaks peavad asjaomase isiku välimus, näoilmed ja žestid olema selgelt märgatavad. Kõne peab alati olema kergesti arusaadav. Helikvaliteet peab olema ühtlane ja ilma väliste häireteta. Valgustus peaks olema võimalikult selline, et näoilme oleks alati kergesti eristatav, et silmade ümber ei oleks varje ning ekraan ei helgiks vastu. Ettevõtte võib anda juhiseid isiku kehaasendi muutmiseks ning isiku ja dokumendi kaadrisse paigutamiseks, et isikusamasust oleks võimalik tuvastada ja kontrollida, sealhulgas vaadelda dokumendile kantud andmeid või kujutisi. Ettevõttel on õigus nõuda pea- või näokatte ja prillide eemaldamist või tema esitatud isikusamasuse tuvastamise ja kontrollimise tagamisega seotud juhiste täitmist.</p>	<p>мобильного ID, на экране Компании. Компания проверяет совпадение личного изображения и фотографии документа, видимой с камеры, через видео в режиме реального времени;</p> <p>4.18.4. Компания проводит интервью с человеком в режиме реального времени, в ходе которого Компания соблюдает принцип «знай своего клиента» и выясняет обстоятельства установления отношений с клиентом. Во время собеседования Компания на основе ответов на анкету задает человеку проверочные вопросы для проверки или уточнения личных данных и, при необходимости, запрашивает дополнительную информацию для уточнения профиля риска человека. Представитель обязан оценить реакцию человека во время собеседования, надежность полученной информации и данных и согласованность с информацией или данными, полученными с помощью других процедур, и отразить как оценку, так и основные обстоятельства в профиле клиента. Если невозможно вразумительно пообщаться с человеком или если есть другие обстоятельства, препятствующие проведению интервью, Компания должна прервать эту процедуру.</p> <p>4.19. Компания считает, что идентификация и проверка не удалась, если:</p> <p>4.19.1. лицо намеренно предоставило данные, которые не соответствуют данным, внесенным в базу документов, удостоверяющих личность, или данные не совпадают с другой информацией или данными, полученными во время сеанса;</p> <p>4.19.2. сессия прерывается во время идентификации, анкетирования или интервью, или если человек не выполнил никаких действий в</p>
---	---

<p>4.20.4. intervjuu alusel määrab Ettevõtte kindlaks kliendiprofiili, kogub informatsiooni ja andmeid ning kontrollib neid. Intervjuu käigus esitab Ettevõtte isikule struktureeritud küsimusi, lähtudes ankeetküsitluse tulemustest. Ettevõtte loal võib füüsiline isik või juriidilise isiku seaduslik esindaja intervjuu ajal tekkinud tehniliste probleemide kõrvaldamiseks kasutada teise isiku kaasabi. Ettevõtte on kohustatud hindama intervjuu käigus isiku reageeringut, saadud info ja andmete usaldusväärsust ja kooskõla muude protseduuridega saadud informatsiooni või andmetega ning kajastama nii hinnangu kui ka selle aluseks olevad asjaolusid kliendi- ja riskiprofiilis.</p> <p>4.20.5. Ettevõtte salvestab video ja ankeetküsitlusega kogutud andmed ja järgmised protseduurid:</p> <p>4.20.5.1. isikusamasuse tuvastamine;</p> <p>4.20.5.2. ebaõnnestunud isikusamasuse tuvastamine ja andmete kontrollimine;</p> <p>4.20.5.3. reaajas läbiviidud intervjuu.</p> <p>4.20.6. Videosalvestamine algab isikusamasuse tuvastamisega ja lõpeb, kui lp-s 5.18.5 nimetatud andmed on kogutud ja protseduurid läbi viidud.</p> <p>4.20.7. Ettevõtte salvestab iga videokohtumise ja säilitab need salvestisi ning sellega kaasnevaid andmeid (sh infotehnoloogilise vahendi abil isikusamasuse tuvastamise informatsiooni) nende taasesitamist võimaldavas vormis vähemalt viis aastat, kui õigusaktidega ei ole ette nähtud pikemat tähtaega.</p> <p>4.21. Isikusamasuse tuvastamise ja kontrollimise eeltingimuste täitmise ning ankeetküsitluse viib läbi Esindaja, vastav automaatsüsteem või tegevuse edasiandmise puhul isik, kellele tegevus edasi anti. Ettevõtte võtab kasutusele</p>	<p>elektronic keskkonnas Ettevõtte voolu 15 minutid;</p> <p>4.19.3. informatsiooniline vool, edastav heli ja pildid, mis ei vasta nõuetele, kehtestatud juhendiga;</p> <p>4.19.4. informatsioonilises süsteemis Ettevõtte tekivad takistused digitaalse identifitseerimise, digitaalse kirjutamise või kirjutamise salvestamise;</p> <p>4.19.5. isik ei pakub vajalikke kinnitusi voolu ajal;</p> <p>4.19.6. isik ei järgi Ettevõtte juhiseid, näiteks, ei eemalda juukseid või maski, ei muuda keha asendit või pead, ei näitab kaamerale andmeid, sisestatud dokument;</p> <p>4.19.7. isik kasutab teise isiku loata Ettevõtte;</p> <p>4.19.8. on märke kahtluse kohta raha pesemise või terrorismi rahastamise.</p> <p>4.20. Nõuded k infohvfwbjyujve voolu säilitatavale pildile ja helisalvestusele (video) ja andmetele, kogutavale videole:</p> <p>4.20.1. informatsiooniline vool, mis sisaldab pildid ja heli, salvestatakse sellisel viisil, et seda oleks võimalik taastada samal viisil, mis esialgselt edastatud sünkroniseeritud heli ja pildid;</p> <p>4.20.2. informatsiooniline vool, mis sisaldab pildid ja heli, peaks olema märgitud ajaga, IP-ajaloo, kliendi, identifitseeritava isiku, isiku identifitseerimise numbriga identifitseeritava isiku, kui puudub isiku identifitseerimise kood, ajaga ja sündimise kohaga ja riigiga, millel on märk ajaga seotud andmetele, mis on seotud nendega sellisel viisil, et igal järgneval muutusel</p>
---	--

<p>meetmed, et vältida automatiseeritud süsteemiga manipuleerimise riske.</p> <p>4.22. Ankeetküsitluse ja intervjuu koostamisel ning teostamisel (kliendile esitatavate küsimuste esitamisel) võtab Ettevõtte arvesse andmete kogumisele käesolevas juhendis kehtestatud põhimõtteid ja nõudeid.</p> <p>4.23. Ettevõtte koostab käesolevate protseduurireeglite ja infotehnoloogiliste vahendite kasutamise abil kogutud andmete, ankeetküsitluse, intervjuu ja muu kättesaadava informatsiooni ning andmete süstematiseeritud kogumise, analüüsimise ja asjaolude selgitamise põhjal kliendiprofiili ja selle ühe osana riskiprofiili. Kliendi- ja riskiprofiili koostab Ettevõtte kirjalikku taasesitamist võimaldavas vormis. Ettevõtte annab hinnangu andmetele, mida koguti infotehnoloogilise vahendi abil tehtud protseduuridega ning otsustab kas luua isikuga ärisuhet või milline on kliendi suhtes rakendatava ärisuhte jälgimise edasine režiim.</p>	<p>данных, лицо, вносящее изменение, время, способ и причину этого, можно идентифицировать.</p> <p>4.20.3. качество изображения и звука во время собеседования должно позволять общаться с лицом, устанавливающим деловые отношения, поэтому Компания отдельно оценивает качество изображения и звука инфотехнологического решения клиента. Место, где находится человек, должно быть хорошо освещено, а речь не должна искажаться акустически (эхо, фоновый шум). Важно, чтобы не нарушалось понимание речи. Информационный поток, передающий звук и изображение, должен быть достаточного качества, чтобы гарантировать, что лицо человека можно увидеть и однозначно идентифицировать, а голова и плечи человека должны быть видны и обрамлены. Технологическое решение должно передавать цветное изображение с чистым звуком и обеспечивать воспроизводимую запись. Звук и изображение должны быть синхронными и воспроизводиться без заметной задержки. Кроме того, должны быть четко видны внешний вид, мимика и жесты заинтересованного лица. Речь всегда должна быть простой для понимания. Качество звука должно быть равномерным и без внешних помех. Освещение должно быть максимально близким, чтобы выражение лица всегда было легко различимо, чтобы не было тени вокруг глаз и не светился экран. Компания может дать инструкции по изменению положения тела лица и расположению в кадре лица и его документа, чтобы личность могла быть идентифицирована и проверена, в том числе путем просмотра данных или изображений в документе. Компания имеет</p>
--	--

	<p>право потребовать снятия головного убора или маски и очков либо следовать предоставленным ею инструкциям по обеспечению идентификации и проверки.</p> <p>4.20.4. на основе интервью Компания определяет профиль клиента, собирает информацию и данные и контролирует их. Во время интервью Компания задает человеку структурированные вопросы по результатам анкетного опроса. С разрешения Компании физическое лицо или законный представитель юридического лица может воспользоваться помощью другого лица для устранения технических проблем, возникших во время собеседования. Компания должна оценить реакцию человека во время собеседования, надежность полученной информации и данных и согласованность с информацией или данными, полученными с помощью других процедур, а также отразить как оценку, так и основные обстоятельства в профиле клиента и профиле риска.</p> <p>4.20.5. Компания должна записывать данные, собранные с помощью видео и анкетирования, а также следующих процедур:</p> <p>4.20.5.1. идентификация личности;</p> <p>4.20.5.2. неудачная идентификация личности и проверка данных;</p> <p>4.20.5.3. интервью в реальном времени.</p> <p>4.20.6. видеозапись начинается с идентификации личности и заканчивается, когда данные, указанные на странице 4.20.5, собраны и процедуры выполнены.</p> <p>4.20.7. Компания должна записывать каждую видеовстречу и хранить эти записи и сопутствующие данные (включая идентификационную</p>
--	---

<p>5. Teatamiskohustus</p> <p>5.1. Kui Esindaja tuvastab tegevuse või asjaolud, mille tunnused osutavad kuritegelikust tegevusest saadud tulu kasutamisele, terrorismi rahastamisele või sellega seotud kuritegude toimepanemisele või sellise tegevuse katsele või mille puhul tal on kahtlus või ta teab, et tegemist on rahapesu või</p>	<p>информацию с помощью инфотехнологических решений) форме, допускающей письменное воспроизведение записи в течение как минимум пяти лет, если более длительный период не установлен законом.</p> <p>4.21. Выполнение предварительных условий для идентификации и проверки личности, а также анкетного интервью должно выполняться Представителем, соответствующей автоматизированной системой или, в случае передачи деятельности, лицом, которому передана деятельность. Компания должна принять меры, чтобы избежать рисков манипулирования автоматизированной системой.</p> <p>4.22. При подготовке и проведении анкетирования и интервью (задавая вопросы клиенту) Компания учитывает принципы и требования, установленные в данном руководстве по сбору данных.</p> <p>4.23. Компания составляет профиль клиента и, как его часть, профиль риска, основанный на систематическом сборе, анализе и уточнении данных, собранных с использованием этого Руководства и инфотехнологических решений, анкет, интервью и другой доступной информации. Компания составляет профиль клиента и профиль риска в форме, допускающей письменное воспроизведение. Компания оценивает данные, собранные в ходе процедур, выполняемых с помощью инфотехнологических решений, и решает, устанавливать ли деловые отношения с этим лицом или какой дальнейший способ мониторинга деловых отношений применяется к клиенту.</p> <p>5. Обязанность сообщения при наличии подозрений в отмывании денег и финансировании терроризма:</p> <p>5.1. В тех случаях, когда Представитель обнаруживает деятельность или обстоятельства, характеристики которых указывают на</p>
--	--

<p>terrorismi rahastamisega või sellega seotud kuritegude toimepanemisega, on ta kohustatud sellest viivitamata, kuid hiljemalt ühe tööpäeva jooksul pärast tegevuse või asjaolude tuvastamist või kahtluse tekkimist, teatama Kontaktisikule, kes edastab informatsiooni RABile hiljemalt 2 tööpäeva pärast tegevuse või asjaolude tuvastamist või kahtluse tekkimist (sh kui Ärisuhte loomine, Tehing või teenuse osutamine jääb teostamata). Kontaktisiku kinnitusel edastab Esindaja teate RABile ise.</p> <p>5.2. Kontaktisik teatab RABile viivitamata, kuid hiljemalt 2 tööpäeva pärast Tehingu tegemist, igast teatavaks saanud Tehingust, kus <u>rahaline kohustus suurusega üle 32 000 euro</u> või sellega võrdväärne summa muus vääringus <u>täidetakse sularahas</u>, sõltumata sellest, kas Tehing tehakse ühe maksena või mitme omavahel seotud maksena kuni üheaastase perioodi jooksul.</p> <p>5.3. Kui Esindajal on kahtlus või ta teab, et tegemist on rahapesu või terrorismi rahastamisega või sellega seotud kuritegude toimepanemisega, tuleb Tehingu tegemine edasi lükata kuni RABile teate esitamiseni. Kui Tehingu edasilükkamine võib tekitada olulist kahju, selle tegemata jätmise ei ole võimalik või võib takistada võimaliku rahapesu või terrorismi rahastamise toimepanija tabamist, tehakse Tehing ning pärast seda esitatakse teade RABile.</p> <p>5.4. Kontaktisik teatab viivitamata RABile, kui Ettevõtte tuvastab, et temaga Ärisuhtes olev või seda kavandav isik on finantssanktsiooni subjekt või tema poolt kavandatav või tehtav Tehing rikub finantssanktsiooni.</p> <p>5.5. Teade esitatakse RABi veebivormi või X-tee teenuse kaudu. Teatele lisatakse isiku isikusamasuse tuvastamiseks ja esitatud teabe kontrollimiseks kasutatud andmed ning olemasolu korral dokumentide koopiad.</p> <p>5.6. Esindajal on keelatud isikut, selle isiku tegelikku kasusaajat, esindajat või kolmandat isikut teavitada nende kohta RABile esitatud teatest, sellise teate esitamise plaanist või esitamise toimumisest ning RABi poolt tehtud</p>	<p>использование доходов от преступной деятельности, финансирование терроризма или на попытку такой деятельности, или когда Представитель знает, что это отмывание денег или финансирование терроризма или совершение связанных с этим преступлений, он обязан незамедлительно, но не <u>позднее одного рабочего дня</u> после обнаружения деятельности или обстоятельств, уведомить об этом Контактное лицо, которое передает эту информацию в БДО не позднее, чем через 2 рабочих дня после обнаружения деятельности или обстоятельств или возникновения сомнения (в т. ч. если установление Деловых отношений, Транзакция или оказание услуг остается несовершенным). При разрешении Контактного лица Представитель отправляет информацию в БДО самостоятельно.</p> <p>5.2. Контактное лицо незамедлительно, но не позднее чем через 2 рабочих дня после осуществления Транзакции, сообщает в БДО о совершении любой Транзакции, когда <u>финансовое обязательство более 32 000 евро</u> или эквивалентная сумма в других валютах исполняется <u>наличными</u>, независимо от того, производится ли Транзакция одним платежом или несколькими связанными между собой платежами в течение периода до одного года.</p> <p>5.3. Если у Представителя подозрение или он знает, что это отмывание денег или финансирование терроризма, или совершение связанных с этим преступлений, необходимо отложить совершение Транзакции до передачи информации в БДО. Если отсрочка Транзакции может нанести существенный ущерб, откладывание Транзакции невозможно или может препятствовать поимке лица, потенциально совершившего отмывание денег или финансирование терроризма, Транзакция проводится и после этого отправляется сообщение в БДО.</p>
---	---

<p>ettekirjutusest või kriminaalmenetluse alustamisest.</p>	<p>5.4. Контактное лицо незамедлительно уведомляет БДО, если Компания обнаруживает, что находящееся или намеревающееся быть с ним в Деловых отношениях лицо является субъектом финансовых санкций, или если планируемая или совершаемая Сделка нарушает финансовые санкции.</p> <p>5.5. Сообщение предоставляется через веб-форму БДО или услуги X-tee. К сообщению добавляются данные, использованные для установления личности/идентификации и проверки предоставленной информации и, если имеются, копии документов.</p> <p>5.6. Представителю запрещается информировать лицо, Бенефициарного собственника, представителя или третье лицо о сообщении, отправленном касательно него/их в БДО, о плане представления такого сообщения или о том, что происходит отправка такого сообщения, а также о сделанных БДО предписаниях, или возбуждении уголовного производства.</p>
<p>6. Andmete registreerimine ja säilitamine</p> <p>6.1. Esindaja registreerib andmed iga Kliendi ja Tehingu kohta selleks etteantud vormidel, sh</p> <p>6.1.1. Juriidilise isiku juhatuse liikme või muu seda asendava organi liikmete nimed ja nende volitused juriidilise isiku esindamisel;</p> <p>6.1.2. Kliendi tegevusvaldkonna ja sidevahendite numbrid;</p> <p>6.1.3. Asjaolu, kas Kliendi puhul on tegemist PEPiga;</p> <p>6.1.4. Tehingu tüübi ja viisi (sularaha, ülekanne), tegemise kuupäeva või ajavahemiku, Tehingu summa ja valuuta ning sisu kirjelduse, sh pangakonto numbrid;</p> <p>6.1.5. Teabe Ettevõtte poolt Ärisuhte loomisest keeldumise asjaolude kohta;</p> <p>6.1.6. Kliendi algatusel Ärisuhte loomisest või Tehingu tegemisest loobumise asjaolud, kui loobumine on seotud Ettevõtte poolt hoolsusmeetmete kohaldamisega;</p>	<p>6. Регистрация и хранение данных</p> <p>6.1. Представитель регистрирует данные по каждому Клиенту и Транзакции в предназначенных для этого формах, в т. ч.</p> <p>6.1.7. Имена членов правления или иного заменяющего органа и их полномочия при представлении юридического лица;</p> <p>6.1.8. Сфера деятельности и телекоммуникационные данные;</p> <p>6.1.9. Обстоятельство, является ли Клиент ПДЛ;</p> <p>6.1.10. Тип и способ Транзакции (наличные деньги, перевод), дата совершения или период времени, сумма и валюта Транзакции, и описание содержания, в т. ч. номера банковских счетов;</p> <p>6.1.11. Обстоятельства отказа Компании от установления Деловых отношений;</p> <p>6.1.12. Обстоятельства отказа от установления Деловых отношений или проведения Транзакции по инициативе Клиента, если отказ</p>

<p>6.1.7. Teabe, kui infotehnoloogiliste vahendite abil ei ole võimalik Juhendi punktides 3.1-3.2 nimetatud hoolsusmeetmeid kohaldada;</p> <p>6.1.8. Teabe Ärisuhte lõpetamise asjaolude kohta seoses hoolsusmeetmete kohaldamise võimatusega;</p> <p>6.1.9. Rahapesu ja terrorismi rahastamise kahtluse korral teatamiskohustuse aluseks oleva teabe;</p> <p>6.1.10. Seltsingu, ühisuse või muu juriidilise isiku staatust mitteomava isikute ühenduse esindajaga või usaldusfondi või usaldusisikuga Tehinguid tehes asjaolu, et isik omab sellist staatust, ning registrikaardi väljavõtte registrist või tõendi sellise registri pidajalt, kus juriidilise isiku staatust mitteomav isikute ühendus on registreeritud,</p> <p>6.1.11. Teabe finantssanktsiooni rakendamise kohta.</p> <p>6.2. Ettevõtte säilitab</p> <p>6.2.1. Isikusamasuse tuvastamise ja esitatud teabe kontrollimise aluseks olevate dokumentide originaale või koopiaid (sh teave elektroonilise päringu tegemise kohta riigi infosüsteemi kuulusse andmekogusse) ja Ärisuhte loomise aluseks olevaid dokumente 5 aastat pärast Ärisuhte lõppemist või Tehingu tegemist;</p> <p>6.2.2. Infotehnoloogiliste vahendite abil isikusamasuse tuvastamisel digitaalseks isiku tõendamiseks ette nähtud dokumendi andmeid, teavet elektroonilise päringu tegemise kohta isikut tõendavate dokumentide andmekogusse ning isikusamasuse tuvastamise ja kontrollimise protseduuri heli- ja videosalvestist 5 aastat pärast Ärisuhte lõppemist;</p> <p>6.2.3. RahaPTSist tulenevate kohustuste täitmisega seotud kogu kirjavahetuse ning kõik Ärisuhte seire käigus kogutud andmed ja dokumendid, samuti andmed kahtlaste või ebatavaliste Tehingute/asjaolude kohta, millest</p>	<p>связан с применением мер прилежания;</p> <p>6.1.13. Информация, когда при помощи инфотехнологических решений невозможно применить меры прилежания, указанные в пунктах 3.1-3.2 Руководства;</p> <p>6.1.14. Обстоятельства о прекращения Деловых отношений по причине невозможности проведения мер прилежания;</p> <p>6.1.15. В случае подозрений в отмытии денег и финансировании терроризма информация, на которой основано обязательство об уведомлении;</p> <p>6.1.16. При проведении Транзакции с представителем сообщества или общности, или другого объединения лиц, не имеющих статуса юридического лица, или с трастом или доверенным лицом, тот факт, что лицо имеет такой статус и выписку регистровой карты из регистра или справку от держателя такого регистра, в котором зарегистрировано такое лицо.</p> <p>6.2. Компания сохраняет</p> <p>6.2.7. Оригиналы или копии документов, которые служат основанием для установления личности/идентификации и проверки предоставленной информации (в т. ч. информацию об электронном запросе в базу данных государственной информационной системы), а также документы, которые служат основанием для установления Деловых отношений, - 5 лет после прекращения Деловых отношений или проведения Транзакции;</p> <p>6.2.8. Данные документа, предусмотренного для цифрового установления личности, использованного при установлении личности при помощи инфотехнологических решений, информацию о проведении электронного запроса в базе данных удостоверяющих личность документов, а также аудио- и видеозаписи процедуры установления и проверки личности - 5 лет после прекращения Деловых отношений;</p>
---	---

<p>RABi ei teavitatud, 5 aastat pärast Ärisuhte lõppemist;</p> <p>6.2.4. Tehingu kohta koostatud dokumente ning rahapesu ja terrorismi rahastamise kahtluse korral teatamiskohustuse aluseks olevaid dokumente ja andmeid vähemalt 5 aastat pärast Tehingu tegemist või teatamiskohustuse täitmist;</p> <p>6.2.5. Finantssanktsioonide jõustumise, muutmise ja lõppemise kohta kontrolli läbiviimise teavet, ning finantssanktsioonid rakendamise käigus kogutud andmed ja dokumendid, 5 aastat.</p> <p>7. Andmete ja dokumentide ajakohastamine</p> <p>7.1. Isikusamasuse tuvastamise ja kontrollimise käigus saadud andmete ajakohastamise eest vastutab andmed sisestanud Esindaja.</p> <p>7.2. Isikusamasuse tuvastamise ja kontrollimise käigus varem kogutud andmete piisavust, muutumist või tõlevastavusest kontrollib vastutav Esindaja vähemalt korra aastas (tugevdatud korras hoolsusmeetmete rakendamisel tihedamini vastavalt Juhendile).</p> <p>7.3. Andmete ajakohastamiseks kasutatakse Kliendiga samas kohas viibimist, avalikke andmekogusid, e-identimist ja Kliendiga e-posti teel suhtlemist.</p> <p>7.4. Ajakohastatud andmed peavad olema registreeritud koheselt pärast uuendatud info teatavaks saamist.</p>	<p>6.2.9. Общая корреспонденция, касающаяся выполнения обязательств, исходящих из Закона, все данные и документы, собранные в ходе мониторинга Деловых отношений, а также данные о подозрительных или необычных Транзакциях/обстоятельствах, о которых не было сообщено в БДО, - 5 лет после прекращения Деловых отношений;</p> <p>6.2.10. Документы, составленные о Транзакции, документы и данные, которые служат основанием для обязанности сообщения в случае подозрения отмыывания денег и финансирования терроризма, - по крайней мере 5 лет после совершения Транзакции или выполнения обязательства сообщения.</p> <p>6.2.11. Информацию о проведении контроля касательно вступления в силу, изменения и окончания финансовых санкций, и данные и документы собранные в ходе применения финансовых санкций – 5 лет.</p> <p>7. Обновление данных и документов</p> <p>7.1. За обновление данных, полученных в ходе установления и контроля личности/идентификации, отвечает Представитель, который ввел данные.</p> <p>7.2. Представитель, который ввел данные, проверяет достаточность, изменения или верность ранее собранных в ходе установления и контроля личности/идентификации данных по крайней мере раз в год (при применении мер прилежания в усиленном порядке чаще согласно Руководству).</p> <p>7.3. Для обновления данных используется нахождение с Клиентом в одном месте, общедоступные базы данных, э-идентификация и общение с Клиентом по электронной почте.</p> <p>7.4. Обновленные данные должны быть зарегистрированы сразу же после получения обновленной информации.</p>
---	---

8. Kontaktisik

- 8.1. Kontaktisikuks määrab Ettevõtte juhatus üksnes isiku, kellel on kontaktisiku ülesannete täitmiseks vajalik haridus, kutsealane sobivus, vajalikud võimed, isikuomadused ja kogemused ning laitmatu maine. Kontaktisiku määramine kooskõlastatakse RABiga.
- 8.2. Kontaktisiku ülesandeks on:
 - 8.2.1. Ettevõtte tegevuses ilmnevatele ebatavalistele või rahapesu kahtlusega Tehingutele või asjaoludele või terrorismi rahastamisele viitava teabe kogumise korraldamine ja analüüsimine ning otsustamine selle edastamise kohta RABile;
 - 8.2.2. Teabe edastamine RABile rahapesu või terrorismi rahastamise kahtluse korral ning RABi poolt esitatud päringutele ja ettekirjutustele vastamine;
 - 8.2.3. Ettevõtte juhatusel perioodiliselt kirjalike ülevaadete esitamine RahaPTSist tulenevate nõuete täitmise kohta;
 - 8.2.4. Rahapesu ja terrorismi rahastamise tõkestamise alaste koolituste läbiviimine Ettevõtte Esindajatele vähemalt kord aastas (Esindaja kinnitab koolitusel osalemist oma allkirjaga);
 - 8.2.5. Esindajatelt laekunud kahtlaste ja/või ebaharilike toimingute kohta laekunud andmete kogumine ning nende andmete töötlemine ja säilitamine selleks ettenähtud korras;
 - 8.2.6. Juhendi õigeaegne ajakohastamine ja sellest Esindajate informeerimine;
 - 8.2.7. Ettevõtte uute Esindajate instrueerimine vastavalt kehtestatud korrale vähemalt ühe nädala jooksul arvates nende tööleasumisest ning käesoleva Juhendi tutvustamine allkirja vastu.
- 8.3. Kontaktisikul on õigus:
 - 8.3.1. Teha Ettevõtte juhatusel ettepanekuid Juhendi muutmiseks ja täiendamiseks ning Esindajatele rahapesualase koolituse korraldamiseks;

8. Контактное лицо

- 8.1. В качестве Контактного лица правление Компании назначает только такое лицо, которое имеет достаточное образование для выполнения заданий Контактного лица, профпригодность, необходимые способности, личные характеристики и опыт и безупречная репутация. Назначение Контактного лица согласовывается с БДО.
- 8.2. В задания Контактного лица входит:
 - 8.2.7. Организация сбора и анализ информации, указывающей на необычные или вызывающие подозрения в отмывании денег Транзакции или обстоятельства, или на финансирование терроризма, и принятие решения о ее передаче в БДО;
 - 8.2.8. Передача информации в БДО в случае подозрения в отмывании денег или финансировании терроризма, и ответы на запросы и предписания БДО;
 - 8.2.9. Периодическое представление письменных обзоров относительно выполнения требований Закона правлению Компании;
 - 8.2.10. Проведение тренингов по предупреждению отмывания денег и финансированию терроризма для Представителей Компании не реже одного раза в год (Представитель подтверждает прохождение тренинга своей подписью);
 - 8.2.11. Сбор данных, поступивших от Представителей касательно подозрительных и/или необычных Транзакциях/операциях, а также обработка и сохранение таких данных в соответствии с предписанной для этого процедурой;
 - 8.2.12. Своевременное обновление Руководства и информирование об этом Представителей Компании;
 - 8.2.13. Инструктаж новых Представителей Компании, в соответствии с установленными процедурами, по крайней мере в течение одной недели с момента их преступления к работе и взятие их подписи об ознакомлении с Руководством.
- 8.3. Контактное Лицо имеет право:

<p>8.3.2. Nõuda Esindajatelt rahapesu ja terrorismi rahastamise tõkestamise nõuete täitmisel tuvastatud puuduste kõrvaldamist mõistliku aja jooksul;</p> <p>8.3.3. Saada Kontaktisiku ülesannete täitmiseks vajalikke andmeid ja teavet;</p> <p>8.3.4. Teha ettepanekuid kahtlaste ja ebatavaliste teatiste esitamise protsessi korraldamiseks;</p> <p>8.3.5. Saada valdkonnaalaseid koolitusi.</p>	<p>8.3.7. Делать предложения правлению Компании для внесения изменений или дополнений в Руководство и организовать обучение Представителям Компании по предупреждению отмывания денег;</p> <p>8.3.8. Требовать от Представителей устранения недостатков, выявленных при выполнении требований по предотвращению отмывания денег и финансирования терроризма в разумные сроки;</p> <p>8.3.9. Получать данные и информацию, необходимые для выполнения заданий Контактного лица;</p> <p>8.3.10. Делать предложения для организации процесса предоставления подозрительных и необычных уведомлений;</p> <p>8.3.11. Участвовать в тренингах по своей сфере.</p>
---	---

LISA 1

1. Euroopa Majanduspiirkonna lepinguriigid

Austria, Belgia, Bulgaaria, Eesti, Hispaania, Holland, Horvaatia, Itaalia, Iirimaa, Island, Kreeka, Küpros, Leedu, Liechtenstein, Luksemburg, Läti, Malta, Norra, Poola, Portugal, Prantsusmaa, Rootsi, Rumeenia, Saksamaa, Slovakkia, Sloveenia, Soome, Taani, Tšehhi, Ungari.

Allikas: <https://elik.nlib.ee/et/pohifakte>

2. Suure riskiga kolmandad riigid

KOMISJONI DELEGEERITUD MÄÄRUSE (EL) 2016/1675 alusel: Afganistan, Bosnia ja Hertsegoviina, Guyana, Iraak, Laose RDV, Süüria, Uganda, Vanuatu, Jeemen, Iraan, Korea Rahvademokraatlik Vabariik.

Rahapesu andmehüüroo andmetel:

Afganistan, Alžeeria, Araabia Ühendmehüraadid, Bahrein, Bangladesh, Egiptus, Indoneesia, Iraak, Iraan, Jeemen, Jordaania, Katar, Kuveit, Liibanon, Liibüa, Malaisia, Mali, Maroko, Mauritaania, Nigeeria, Omaan, Pakistan, Palestiina, Saudi Araabia, Somaalia, Sri Lanka, Sudaan, Süüria, Tuneesia, Türgi, Vene Föderatsiooni kuuluvad Kaukaasia rahvusgrupid (tšetšeenid, lesgid, osseedid, ingušid jne).

FATF andmetel: <http://www.fatf-gafi.org/countries/#high-risk> (uuendatakse kolm korda aastas).

3. Nimekiri territooriumidest, mida EI LOETA madala maksumääraga territooriumiks, ja info madala maksumääraga territooriumide kohta

Maksu- ja Tolliameti andmetel: <https://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest>

4. Finantssanktsioonide info ja otsing

<https://www.politsei.ee/et/rahapesu/>

<https://www.sanctionsmap.eu/#/main>

ПРИЛОЖЕНИЕ 1

1. Страны Европейской экономической зоны

Австрия, Бельгия, Болгария, Эстония, Испания, Голландия, Хорватия, Италия, Ирландия, Исландия, Греция, Кипр, Литва, Лихтенштейн, Люксембург, Латвия, Мальта, Норвегия, Польша, Португалия, Франция, Швеция, Румыния, Германия, Словакия, Словения, Финляндия, Дания, Чехия, Венгрия.

Источник: <https://elik.nlib.ee/et/pohifakte>

2. Третьи страны с высоким риском

На основе Положения Комиссии (ЕС) 2016/1675: Афганистан, Босния и Герцеговина, Гайана, Ирак, Лаос, Сирия, Уганда, Вануату, Йемен, Иран, Корейская Народно-Демократическая Республика.

Данные БДО: Афганистан, Алжир, Объединенные Арабские Эмираты, Бахрейн, Бангладеш, Египет, Индонезия, Ирак, Иран, Йемен, Иордания, Катар, Кувейт, Ливан, Ливия, Малайзия, Мали, Марокко, Мавритания, Нигерия, Оман, Пакистан, Палестина, Саудовская Аравия, Сомали, Шри-Ланка, Судан, Сирия, Тунис, Турция, принадлежащие Российской Федерации этнические группы Кавказа (чеченцы, лезгины, осетины, ингуши).

По данным FATF: http://www.fatf-gafi.org/countries/#high_risk (обновляется три раза в год).

3. Перечень территорий, которые не являются территориями с низкой налоговой ставкой, и информация о территориях с низкой налоговой ставкой

По данным Налогово-Таможенного департамента: <https://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest>

4. Информация и поиск финансовых санкций

<p>5. FATFi soovitused</p> <p>http://www.fatf-gafi.org/</p> <p>http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html</p> <p>6. Eestis väljastatud isikut tõendava dokumendi kehtivuse kontroll</p> <p>https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/</p> <p>7. PRADO Ehtsate isikut tõendavate ja reisidokumentide avalik veebiregister</p> <p>https://www.consilium.europa.eu/prado/ET/prado-start-page.html</p> <p>8. EL usaldusnimekirjade lehitseja</p> <p>https://webgate.ec.europa.eu/tl-browser/#/</p>	<p>https://www.politsei.ee/et/rahapesu/</p> <p>https://www.sanctionsmap.eu/#/main</p> <p>5. Рекомендации ФАТФ</p> <p>http://www.fatf-gafi.org/</p> <p>http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html</p> <p>6. Проверка действия удостоверяющего личность документа, выданного в Эстонии</p> <p>https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/</p> <p>7. Общественный веб-регистр подлинных удостоверений личности и проездных документов (PRADO)</p> <p>https://www.consilium.europa.eu/prado/ET/prado-start-page.html</p> <p>8. Доверительный список ЕС</p> <p>https://webgate.ec.europa.eu/tl-browser/#/</p>
--	---