



# AQDIGITAL

## AML Policy

Rules of Procedure and Internal Control Rules



AQdigital OÜ  
registrikood 14873938

## PROTSEDUURIREEGLID JA SISEKONTROLLIEESKIRI

Rahapesu ja terrorismi rahastamise seaduse  
rakendamiseks

		Tegelik uuendamise kuupäev
Koostamise kuupäev	25.05.2021	-
Järgmine planeeritav uuendamise kuupäev	25.05.2022	16.06.2022
Järgmine planeeritav uuendamise kuupäev	16.06.2023	16.08.2022
Järgmine planeeritav uuendamise kuupäev	16.08.2023	25.11.2022
Järgmine planeeritav uuendamise kuupäev	16.08.2023	

### 1 SISSEJUHATUS

AQdigital OÜ on virtuaalväringute vahetuse ja rahakoti teenuse osutaja. Aqdigital OÜ pakub oma teenust oma kodulehe kaudu <https://aqdigital.exchange> (edaspidi Koduleht) ja

Aqdigital OÜ  
Registry code 14873938

## RULES OF PROCEDURE AND INTERNAL CONTROL RULES

for the Implementation of the Money Laundering  
and Terrorist Financing Prevention Act

		Actual update date
the date of the document	25.05.2021	-
Next planned update date	25.05.2022	16.06.2022
Next planned update date	16.06.2023	16.08.2022
Next planned update date	16.08.2023	25.11.2022
Next planned update date	16.08.2023	

### 1 INTRODUCTION

AQdigital OÜ is a virtual currency exchange and wallet service provider. Aqdigital OÜ offers its service on its website at <https://aqdigital.exchange> (hereinafter the Website), and uses the technology developed by the company for that purpose. Virtual currency can be exchanged for ordinary currency or other virtual currency on the Aqdigital platform. In addition to the above, it's possible to hold and send (transfer) virtual currencies.

kasutab selleks enda poolt arendatud tehnoloogiat.

Aqdigital platvormil on võimalik nii vahetada virtuaalväering tavalise 3uesti vastu kui ka muu virtuaalväeringu vastu. Lisaks eeltoodule on võimalik hoida virtuaalväeringuid ja neid saata (üle kanda).

Aqdigital platvormil on võimalikud järgmised 3uesti paarid: eur/xbt; eur/eth; eur/etc; eur/ltc and other. Valuutapaarid võivad muutuda ja täpsem info kajastub kodulehel.

Käesolevate protseduurireeglite ja sisekontrollieeskirjade (edaspidi Juhend) eesmärk on kirjeldada äriühingu protseduurireegleid, määratleda klientide ja partnerite riskiprofiili ja anda juhiseid kuidas tagada hoolduskohustuste täitmist tulenevalt rahapesu ja terrorismi rahastamise seadusest (RahaPTS). Hoolduskohustused RahaPTS-i kohaselt on hooldusmeetmed, andmete kogumine ja säilitamine ning rahapesu ja terrorismi rahastamisega seotud riskide juhtimine.

Aqdigital OÜ (edaspidi Äriühing või Aqdigital) kohustub virtuaalväeringu raha vastu vahetamise ja rahakotiteenuse pakkujana järgima käesolevaid protseduurireegleid tulenevalt RahaPTS § 2 lg 1 p-st 10.

Äriühingu juhatus (edaspidi Juhatus) kohustub tagama, et iga äriühingu töötaja ja/või personali liige (edaspidi Personal) täidaks käesolevas Juhendis, RahaPTS-is ning selle alusel antud õigusaktides sätestatud nõudeid. Äriühingu Personal peab tundma Juhendis ja RahaPTS-i sätestatud kohustusi ja täitma neid igapäevaste tööülesannete täitmisel.

Äriühingul on olemas kontaktisik (compliance officer), kes vastutab RahaPTS-ist ja käesolevast Juhendist tulenevate nõuete täitmise eest. Nõuete rikkumine võib tuua kaasa töölepingu (või muu võlaõigusliku lepingu) lõpetamise ja muid seadusest tulenevaid sanktsioone.

Kontaktisik kohustub kontrollima protseduurireeglite ja sisekontrollieeskirja ajakohasust regulaarselt (vähemalt kord aastas), vajadusel uuendama ja muutma käesolevat Juhendit tulenevalt muudatustest äriühingus ning selle kontrollsüsteemis.

Käesolevas Juhendis on alljärgnevatel mõistetel järgmine tähendus:

**Rahapesu**- ajakohane kehtiv määratlus vastavalt RahaPTS § 4.

**Terrorismi rahastamine**- ajakohane kehtiv määratlus vastavalt RahaPTS § 5.

**Kohustatud isik**- on RahaPTS § 2 nimetatud isik.

**Tegelik kasusaaja** – füüsiline isik, kes 3uestion mõju ära kasutades tehingu või toiminguga või omab muul viisil kontrolli tehingu, toiminguga või teise isiku üle ja kelle huvides, kasuks või arvel tehing või toiming tehakse. Äriühingu puhul on tegelik

The following currency pairs are possible on the Aqdigital platform: eur/xbt; eur/eth; eur/etc; eur/ltc and other. The currency pairs may change and detailed information can be found on the Website.

The purpose of these Rules of Procedure and Internal Control Rules (hereinafter the Guidelines) is to describe the rules of procedure of the company, define the risk profile of customers and partners, and give guidelines on how to ensure the performance of the due diligence duties for the purpose of the Money Laundering and Terrorist Financing Prevention Act (hereinafter the MLTFPA). Under the MLTFPA, the due diligence duties include the taking of the due diligence measures, the collection and retention of data and the management of risks relating to money laundering and terrorist financing.

As a provider of the service of exchanging a virtual currency for a fiat currency and the wallet service, Aqdigital OÜ (hereinafter the Company or Aqdigital) is required to follow these rules of procedure under clause 2 (1) 10) of the MLTFPA.

The management board of the Company (hereinafter the Management Board) undertakes to ensure that each employee and/or staff member of the Company (hereinafter the Staff) follow the requirements provided for in these Guidelines, the MLTFPA and legislation adopted on the basis thereof. The Staff of the Company must know the duties provided for in the Guidelines and the MLTFPA and perform these upon performance of their day-to-day employment duties.

The company has a compliance officer, who is responsible for compliance with the requirements arising from the MLTFPA and these Guidelines. Failure to comply with the requirements may result in the termination of the employment contract (or another contract under the law of obligations) as well as the imposition of other statutory sanctions.

The compliance officer undertakes to regularly (at least once a year) verify whether the Rules of Procedure and Internal Control Rules are up to date and, where necessary, update and revise these Guidelines on the basis of changes in the Company and its control system.

The following terms have the following meaning in these Guidelines.

**Money laundering** means money laundering as defined in § 4 of the MLTFPA in force.

**Terrorist financing** means terrorist financing as defined in § 5 of the MLTFPA in force.

**Obliged entity** means a person specified in § 2 of the MLTFPA.

**Beneficial owner** means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose

kasusaaja füüsiline isik, kes lõplikult omab või kontrollib juriidilist isikut piisava arvu aktsiate, osade, hääleõiguste või omandiõiguse otsese või kaudse omamise kaudu, sealhulgas osalus esitajaaktsiate või -osade kujul, või muul viisil.

**AQdigital OÜ või äriühing** – virtuaalvääringute teenuste pakkuja, kes on kohustatud isikuks RahaPTS seaduse mõttes.

**Ärisuhe** – on suhe, mis tekib kehtvuslepingu sõlmimisel majandus- või kutsetegevuses kohustatud isiku poolt teenuse osutamiseks või kauba müümiseks või muul viisil turustamiseks või mis ei põhine kehtvuslepingul, kuid mille puhul kontakti loomise ajal võiks mõistlikult oodata suhte teatavat kestvust ja mille jooksul teeb kohustatud isik teenust või ametiteenust osutades, ametitoiminguid tehes või kaupa pakkuks korduvalt eraldiseisvaid tehinguid majandus-, kutse- või ametitegevuse käigus

**Personal-** äriühingu töötaja või muu võlaõigusliku lepingu alusel teenust osutav personali liige, juhatause liige.

**Juhatus-** on äriühingu juhtorgan, mis esindab ja juhib äriühingut. Juhatusel võib olla üks või mitu juhatause liiget. Kui juhatus on üle kahe liikme, valitakse juhatause liikmetest juhatause esimees, kes korraldab Juhatause tegevust.

**Kontaktisik-** juhatause poolt määratud isik, kes on rahapesu andmebüroo kontaktisikuks.

**Riskiriik-** on riik või piirkond, kus on suurenenud terrorismioht või millega seondub kõrgem terrorismi rahastamise risk. Riskiriikide või piirkondade kohta võib rahapesu andmebüroo anda RahaPTS kohustatud subjektidele töö käigus täiendavat informatsiooni. (lisa 4)

**Riskiisu-** Riskiisu on kohustatud isiku riskide taseme ja riskide tüüpide kogum, mida ta on valmis oma tegevuse käigus võtma oma majandustegevuse ja strateegiliste eesmärkide elluviimise nimel ja mille kinnitab kohustatud isiku kõrgem juhtkond kirjalikus vormis.

account a transaction or act, action, operation or step is made. In the case of companies, a beneficial owner is the natural person who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means.

**AQdigital OÜ or Company** means the virtual currency service provider, which is an obliged entity for the purposes of the MLTFPA.

**Business relationship** means a relationship that is established upon conclusion of a long-term contract by an obliged entity in economic or professional activities for the purpose of provision of a service or sale of goods or distribution thereof in another manner or that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact and during which the obliged entity repeatedly makes separate transactions in the course of economic or professional activities while providing a service or professional service, performing professional acts or offering goods.

**Staff** means an employee of the Company or a Staff member providing a service on the basis of another contract under the law of obligations or a member of the Management Board.

**Management Board** means the management body of the Company which represents and manages the Company. The Management Board may have one or several members. If the Management Board has more than two members, a chair of the Management Board is elected from among the members of the Management Board and the chair will organise the activities of the Management Board.

**Compliance Officer** means the person appointed by the Management Board to act as a contact person of the Financial Intelligence Unit (FIU).

**High-risk country** means a country or region where there is a heightened risk of terrorism or that is associated with a higher risk of terrorist financing. In the course of work, the Financial Intelligence Unit may provide obliged entities as defined in the MLTFPA with additional information regarding high-risk countries or regions (Annex 4).

**Risk appetite** means the total of the exposure level and types of the obliged entity, which the obliged entity is prepared to assume for the purpose of its economic activities and attainment of its strategic goals, and which is established by the senior management of the obliged entity in writing.

## 2 RISIKIHINNANG JA RISKIISU

Äriühingu juhatus ja vajadusel teised Personali liikmed, kes puutuvad oma igapäevatoos kokku rahapesu ja terrorismi rahastamise tõkestamise riskide maandamisega, koostavad oma tegevusega kaasnevate rahapesu ja terrorismi rahastamisega seotud riskide tuvastamiseks, hindamiseks ning analüüsimiseks riskihinnangu.

Riskihinnangu koostamisel kaardistab äriühing virtuaalvääringu vahetamise ja rahakotiteenuse osutamisega seonduvaid rahapesu ja terrorismi rahastamise riskid, võttes arvesse 3.1. ja 3.2. punktis nimetatud riskikategooriaid. Seejärel hinnatakse kaardistatud riskide mõjusid Äriühingu tegevusele ning analüüsitakse võimalikke vastumeetmeid, millega on võimalik kaardistatud riske maandada, nende mõistlikkust ning kohaldamise võimalikkust.

Seejuures peab silmas pidama, et riskide tuvastamiseks, hindamiseks ja analüüsimiseks tehtavad sammud peavad olema proportsionaalsed Aqdigital OÜ majandus- ja kutsetegevuse laadi, ulatuse ning keerukustmehhanismidega.

**Riskihinnangu tulemusel** määratakse kindlaks:

- 1) väiksema ja suurema rahapesu ja terrorismi rahastamise riskiga valdkonnad;
- 2) riskiisu, sealhulgas äritegevuse käigus pakutavate toodete ja teenuste mahu ning ulatuse;
- 3) riskijuhtimise mudeli, sealhulgas lihtsustatud ja tugevdatud hooldusmeetmed, et tuvastatud riske maandada.

Riskiisu tuvastamisel võetakse arvesse riske, mida Äriühing on valmis võtma või mida ta soovib vältida seoses oma majandustegevusega, ning kvalitatiivseid ja kvantitatiivseid kompensatsioonimehhanisme, nagu planeeritav tulu, kapitali või muude likviidsete vahendite abil rakendatavad meetmed või teised asjaolud, nagu maine riskid ning rahapesu ja terrorismi rahastamise või muu ebaeetilise tegevusega kaasnevad õiguslikud ja muud riskid.

Riskihinnang ja riskiisu kindlaksmääramine peab olema dokumenteeritud ja nõudmise/vajaduse korral neid esitatakse Rahapesu andmehüroole. Riskihinnang ja riskiisu ajakohastatakse vastavalt muutustele äriühingu tegevuses, kuid mitte harvem kui iga aasta 5.uestio.

Äriühingu riskihinnang ja riskiisu (risk table) on koostatud eraldi dokumentides. Personalil on kohustus nendega tutvuda ja juhendada oma igapäeva töös.

## 2 RISK ASSESSMENT AND RISK APPETITE

For the purpose of identification, assessment and analysis of risks of money laundering and terrorist financing related to their activities, the Management Board of the Company and, where necessary, the other Staff members engaged in mitigating the risks of money laundering and terrorist financing on a day-to-day basis prepare a risk assessment.

Upon preparation of the risk assessment, the Company maps the risks of money laundering and terrorist financing related to the provision of the service of exchanging virtual currencies and the wallet service, taking into account the risk categories specified in clauses 3.1 and 3.2. Thereafter the effects of the mapped risks on the activities of the Company are assessed and possible risk-mitigating counter-measures, their reasonableness and their applicability are analysed.

Thereby it must be kept in mind that the steps taken to identify, assess and analyse risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of Aqdigital OÜ.

**As a result of the risk assessment**, the following is established:

- 1) fields of a lower and higher risk of money laundering and terrorist financing;
- 2) the risk appetite, including the volume and scope of products and services provided in the course of business activities;
- 3) the risk management model, including simplified and enhanced due diligence measures, in order to mitigate identified risks.

Upon identifying a risk appetite, account must be taken of the risks that the Company is prepared to assume or that the Company wishes to avoid in connection with the economic activities as well as qualitative and quantitative compensation mechanisms such as the planned revenue, measures applied with the help of capital or other liquid funds, or other factors such as reputation risks as well as legal and other risks arising from money laundering and terrorist financing or other unethical activities.

The establishment of the risk assessment and risk appetite must be documented and, where requested/necessary, submitted to the Financial Intelligence Unit. The risk assessment and risk appetite are updated based on changes in the activities of the Company, but no less frequently than once every year.

The company's risk assessment and risk appetite have been prepared in separate documents. Staff have a responsibility to familiarize themselves with them and be guided in their daily work.

### 3 RISKIPROFIILI MÄÄRAMINE

#### 3.1 Riskikategooriate määramine ja nende suurendavad/vähendavad asjaolud

Klientide riskiprofiili määramisel võtab Äriühing arvesse järgmisi riskikategooriaid:

1. Kliendiga/partneriga seonduv risk;
2. Riikide või geograafiliste piirkondade või jurisdiktsioonidega seonduv risk;
3. Toodete, teenuste või tehingutega seonduv risk;
4. Aqdigital OÜ ja Klientide vaheliste suhtlus- või vahenduskanalitega või toodete, teenuste või tehingute edastamiskanalitega seonduv risk.

Juhul kui tekib kahtlus riskikategooriate määratlemisel ja esinevad vastuolulised andmed riskikategooriate suurendavate ja vähendavate asjaolude kohta, tuleb lähtuda alati nii-öelda suurema ohuallika põhimõttest – kui esineb ilminguid, mis paigutavad kliendi/jurisdiktsiooni/toote/teenuse suurema riski kategooriasse, siis peaks sellest lähtuma.

**Kliendirisk** ehk tehingus osaleva isiku või Kliendi isikust tulenevad riskifaktorid, sh:

- isiku õiguslikku vorm, juhtimisstruktuur, tegevuse valdkond;
- kas tegemist on Riikliku taustaga isikuga (PEP);
- kas füüsilisest isikust tegelik kasusaaja on keegi kolmas isik;
- kas isiku tegelike kasusaajate selgitamine on raskendatud, tulenevalt keerukatest ja läbipaistmatutest omanikusuhetest;
- isik on rahvusvahelise sanktsiooni õuestio;
- isiku suhtes on teada eelnev rahapesu ja/või terrorismi rahastamise kahtlus;
- isiku välimus ja/või käitumine viitab variisiku tunnustele;
- kas isik osaleb tehingutes, kus on suur osa sularahal;
- kas isik pakub teenust anonüümsetele klientidele;
- kas isiku vara päritolu või tehinguks kasutatavate rahaliste vahendite allikas ning päritolu on kergesti tuvastatav;

**Kliendiriski suurendavad** asjaolud on eeskätt olukorrad, kus:

- 1) ärisuhe toimib ebatavalistel asjaoludel, sealhulgas keeruliste ja ebatavaliselt suuremahuliste tehingute ning

### 3 DETERMINATION OF THE RISK PROFILE

#### 3.1 Determination of risk categories and factors increasing/reducing them

Upon determining customers' risk profiles, the Company takes into account the following risk categories:

1. risks relating to the customer/partner;
2. risks relating to countries, geographic areas or jurisdictions;
3. risks relating to products, services or transactions;
4. Risks relating to communication or mediation channels or delivery channels of products, services or transactions between Aqdigital OÜ and customers.

In the event of doubts in determining risk categories and controversial data regarding increasing and reducing factors of risk categories, the principle of a source of greater danger must be followed – if there are signs that place the customer/jurisdiction/product/service in a higher risk category, it should be relied on.

**Customer risk** or risk factors arising from the person or customer participating in a transaction, incl.:

- the legal form, management structure, field of activity of the person;
- whether the customer is a politically exposed person (PEP);
- whether the beneficial owner who is a natural person is a third party;
- whether the identification of the beneficial owners is impeded by complex and non-transparent ownership relations;
- the person is subject to an international sanction;
- a prior suspicion of money laundering and/or terrorist financing is known regarding the person;
- the look and/or behaviour of the person are indicative of the person being a front;
- whether the person participates in transactions where cash plays a great role;
- whether the person renders the service to anonymous customers;
- whether the origin of the person's assets or the source and origin of the funds used for a transaction can be easily identified;

Factors **increasing the customer risk** are, above all, situations where:

- 1) the business relationship is based on unusual factors, including in the event of complex and unusually large transactions and unusual transaction patterns that do

ebatavaliste tehingumustrite korral, mille ei ole mõistlikku, selget majanduslikku või õiguspärast eesmärki või mis ei ole konkreetse ärispetsiifika jaoks iseloomulik;

- 2) Kliendiks on suuri sularahakoguseid käitlev ettevõtja;
- 3) Kliendiks oleval või temaga seotud äriühingul on variaktsionärid või esitajaaktsiad;
- 4) Kliendiks oleva äriühingu omandistruktuur näib äriühingu tegevust silmas pidades ebatavaline või liiga keeruline

**Kliendiriski vähendavad** asjaolud on eeskätt olukorrad, kus Klient on reguleeritud turul noteeritud äriühing, kelle suhtes kohaldatakse avalikustamiskohustusi, millega on kehtestatud nõuded, et tagada tegeliku kasusaaja puhul piisav läbipaistvus.

**Geograafilise piirkonnaga/jurisdiiktsiooniga** seonduv risk on risk, mis tuleb Kliendi asukoha ja/või tegevuskoha riigist, sh:

- kas riigis rakendatakse rahapesu ja terrorismi rahastamise tõkestamisel rahvusvaheliste standarditega kooskõlas olevaid õigusnorme;
- kas riigis on kõrge kuritegevuse tase, sh narkokuritegevuse tase;
- kas nimetatud riik teeb koostööd mõne kuritegeliku ühendusega; kas kuritegelikud ühendused kasutavad nimetatud riiki enda tegevuse teostamiseks;
- kas nimetatud riigis tegeletakse massihävitusrelvade leviku rahastamisega;
- kas nimetatud riigis on kõrge korruptsioonitase;
- kas selle riigi suhtes on rakendatud või rakendatakse rahvusvahelisi sanktsioone.

**Geograafilist riski suurendavad asjaolud** on eeskätt olukorrad, kus tehingus osalev isik või tehing ise on seotud riigiga või jurisdiktsiooniga:<sup>1</sup>

- 1) kus usaldusväärsete allikate kohaselt ei ole kehtestatud rahapesu ja terrorismi rahastamise tõkestamise tõhusaid süsteeme;
- 2) kus usaldusväärsete allikate kohaselt on korruptsiooni või muu kuritegeliku tegevuse tase märkimisväärne;
- 3) mille suhtes on kehtestatud sanktsioonid, embargo või nendega sarnased meetmed, näiteks Euroopa Liidu või ÜRO poolt;
- 4) mis rahastab või toetab terrorismi või mille territooriumil tegutsevad Euroopa Liidu või

not have a reasonable, clear economic or lawful purpose or that are not characteristic of the given business specifics;

- 2) the customer is a cash-intensive business;
- 3) the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;
- 4) the ownership structure of the customer company appears unusual or excessively complex, given the nature of the company's business.

Factors **reducing the customer risk** are, above all, situations where the customer is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner.

**Geographic area/jurisdiction** risk is a risk that arises from the country of the seat and/or place of business of the customer, incl.:

- whether the country applies legal provisions that are in compliance with the international standards of prevention of money laundering and terrorist financing;
- whether there is a high crime rate (incl. drug-related crime rate) in the country;
- whether the country cooperates with a criminal group; whether criminal groups use the country for pursuing their operations;
- whether the country engages in funding the spread of weapons of mass destruction;
- whether there is high level of corruption in the country;
- whether international sanctions have been or are being imposed on the country.

**Factors increasing the geographic risk** are, in particular, situations where the person involved in a transaction or the transaction itself is connected with a country or jurisdiction<sup>1</sup>:

- 1) that, according to reliable sources, has not established effective AML/CFT systems;
- 2) that, according to reliable sources, has significant levels of corruption or other criminal activity;
- 3) that is subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations;
- 4) that provides funding or support for terrorist activities or that has designated terrorist organisations operating within

<sup>1</sup> FATF-i kodulehel on võimalik kontrollida riskiriikide nimekirja siin: <https://www.fatf-gafi.org/countries/#high-risk> ja <https://www.fatf-gafi.org/countries/#other-monitored-jurisdictions>

<sup>1</sup> The list of high-risk countries published on the FATF website can be consulted here: <https://www.fatf-gafi.org/countries/#high-risk> and <https://www.fatf-gafi.org/countries/#other-monitored-jurisdictions>

ÜRO poolt kindlaks määratud terroristlikud organisatsioonid.

**Geograafilist riski vähendavad** asjaolud on eeskätt sellised olukorrad, kus tehingus osalev isik on pärit järgmisest riigist või tema elu- või asukoht on järgmises riigis:

- 1) Euroopa Majanduspiirkonna lepinguriigis;
- 2) kolmandas riigis, kus on tõhusad rahapesu ja terrorismi rahastamise tõkestamise süsteemid;
- 3) kolmandas riigis, kus usaldusväärsete allikate kohaselt on korrupsiooni ja muu kuritegeliku tegevuse tase madal;
- 4) kolmandas riigis, kus usaldusväärsete allikate kohaselt on kehtestatud rahapesu ja terrorismi rahastamise tõkestamise nõuded, mis on kooskõlas rahapesu tõkestamise nõukoja muudetud soovustega, ning kus neid nõudeid tõhusalt rakendatakse.

**Toodete, tehingute ja teenustega seonduv risk** on risk, mis tuleneb otseselt kliendi tegevusvaldkonnast ja tema poolt pakutavate teenuste iseloomust, sh:

- ravimite müük;
- erootika ja täiskasvanute kaupade müük;
- tutvumisteenused;
- e-sigarettide ja tubakatoodete müük;
- privaat- ja personaalpangandus;
- valuutavahetus ja Forex trading;
- väärismetalli ja –kivide ost-müük;
- relvade ost-müük;
- pandimajad;
- äriühingud, kes pakuvad piiriülese sularaha ja väärtpaberite vedamise teenust;
- igasugune muu illegaalne tegevusvaldkond (näiteks narkootiliste ainete müük, keelatud kaupade müük, darknet kaubad ja teenused jne.)

**Toodete/teenuste riski suurendavad** asjaolud on eeskätt järgmised olukorrad, kus on tegemist:

- 1) toote pakkumise/tehingu tegemise, mis võib soodustada anonüümsust;
- 2) tundmatutelt või mitteseotud kolmandatelt isikutelt saadud maksetega;
- 3) ärisuhte või tehinguga, mis luuakse või algatatakse viisil, mille puhul ei viibita kliendi, tema esindaja või tehingu poolega samas kohas ja ei kohaldata kaitseabinõuna RahaPTS § 31 rakendamist;
- 4) uute makseviiside ja uute äritavadega, sealhulgas uue edastatismehhanismi või uue või areneva tehnoloogia kasutamine nii uute kui ka olemasolevate toodete puhul.

their territory, as identified by the European Union or the United Nations.

Factors **reducing the geographic risk** are, above all, situations where the person participating in a transaction is from or the person's place of residence or seat is in:

- 1) a contracting state of the European Economic Area;
- 2) a third country that has effective AML/CFT systems;
- 3) a third country where, according to reliable sources, the level of corruption and other criminal activity is low;
- 4) a third country where, according to credible sources, AML/CFT requirements that are in accordance with the updated recommendations of the Financial Action Task Force (FATF) have been established, and where the requirements are effectively implemented.

**The product, transaction and service risk** is a risk that arises directly from the field of activity of the customer and from the nature of the services provided by the customer, incl.:

- sale of medicinal products;
- sale of erotic and adult goods;
- dating services;
- sale of e-cigarettes and tobacco products;
- private and personal banking;
- currency exchange and Forex trading;
- purchase and sale of precious metals and stones;
- purchase and sale of weapons;
- pawnshops;
- commercial undertakings that provide cross-border cash and security transportation services;
- any other illegal field of activity (e.g. sale of narcotic substances, sale of banned goods, darknet goods and services, etc.).

Factors **increasing the product/service risk** are, above all, situations where:

- 1) a product that may favour anonymity is provided or a transaction that may favour anonymity is made;
- 2) payments received from unknown or unassociated third parties are involved;
- 3) a business relationship or transaction is established or initiated in a manner whereby the customer, the customer's representative or party to the transaction is not met physically at the same place and whereby § 31 of the MLTFPA is not applied as a safeguard measure;
- 4) new payment methods and new business practices, including a new delivery mechanism, or new or emerging



**Toodete/teenuste riski vähendavad** asjaolud on eeskätt järgmised olukorrad, kus on tegemist:

- 1) finantstoodete või -teenustega, mis pakuvad asjakohaselt kindlaksmääratud ja piiratud teenuseid teatavatele kliendirühmadele, et suurendada juurdepääsu finantsalase kaasamise eesmärgil;
- 2) tooted, mille puhul rahapesu ja terrorismi rahastamise riski juhitakse muude teguritega nagu raha pealelaadimise piirangud või omandi läbipaistvus (nt teatavat liiki e-raha).

**Aqdigital OÜ ja Klientide vaheliste suhtlus- või vahenduskanalitega seonduv** risk on risk, mis tuleneb otseselt sellest, millisel viisil toimub suhtlus kliendiga ja kui võrd antud suhtluse viis võimaldab tuvastada klienti ja veenduda tema poolt esitatud informatsiooni tõesuses.

**Suhtluskanalitega seonduva riski suurendavad** eeskätt järgmised asjaolud:

- 1) tegemist on olukorraga, kus suhtlus kliendiga toimub pidevalt erinevate kanalite kaudu, näiteks helistatakse erinevate riikide telefoninumbritest, saadetakse kirju erinevatest e-posti aadressidest jne.;
- 2) kui klient üritab Aqdigital OÜ-ga võtta ühendust kolmandate isikute kaudu, kes ei ole tema esindaja või eeskostja;

Suhtluskanalitega seonduva riski vähendavad eeskätt järgmised asjaolud:

- 1) kui suhtlus kliendiga toimub pidevalt samade kanalite kaudu, kasutades samu kontakte, mis on välja toodud ka näiteks avalikes registrites/andmebaaside ja/või kliendi kodulehel või ankeedis.
- 2) Kui klient suhtleb OÜ-ga Aqdigital isiklikult või esindaja või eeskostja kaudu.

### 3.2 Kliendi riskiprofiili määramine

Kliendi riskiprofiili määramisel tuleb arvesse võtta riskikategooriad (-faktoreid) ning neid suurendavaid ja vähendavaid asjaolusid. Riskiprofiili määramisel tuleb arvestada kõiki riskifaktoreid kogumis ja vastastikkuses seoses. Klientidega seotud riski määramise puhul tuleb jälgida nn „tunne oma klienti“ põhimõtet (edaspidi KYC) ehk kliendi riskiprofiili määramise aluseks on hoolsusmeetmete kohaldamisel kogutud informatsioon. Aqdigital OÜ 9uestionn kliente **madal (tier 1), keskmise (tier 2), kõrge riskiga (tier 3) klientidega.**

technologies are used for both new and pre-existing products.

Factors **reducing the product/service risk** are, above all, situations where:

- 1) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes, are involved;
- 2) products whereby the risk of money laundering and terrorist financing is managed through other factors such as loading restrictions or the transparency of ownership (e.g. e-money of a certain type) are involved.

The risk **related to the communication or mediation channels between Aqdigital OÜ and customers** is a risk that directly arises from the manner of communication with the customer and from the extent to which the given manner of communication allows for identifying the customer and verifying the correctness of the information submitted by the customer.

**The risk related to communication channels is increased**, above all, by the following factors:

- 1) it is a situation where communication with the customer takes place constantly via various channels, e.g. calls are made from telephone numbers of different countries, letters are sent from different e-mail addresses, etc.;
- 2) if the customer tries to contact Aqdigital OÜ via third parties who are not their representative or guardian.

The risk related to communication channels is reduced, above all, by the following factors:

- 1) when communication with the customer takes place constantly via the same channels, using the same contact details that are also indicated, for example, in public registers/databases and/or on the customer's website or questionnaire.
- 2) If the customer communicates with Aqdigital OÜ personally or via a representative or guardian.

### 3.2 Determination of the customer's risk profile

Upon determining the customer's risk profile, the risk categories (factors) and the factors increasing and reducing them must be taken into account. Upon determining the risk profile, all the risk factors must be taken into account as a whole and in terms of their mutual relationships. In the case of determining the risk related to customers, the Know Your Customer (hereinafter KYC) principle must be followed, i.e. the basis for determining the

**Väikse (tier 1) riskiga** kliendid on need, kelle osas on täidetud järgmised tunnused:

1. Kliendi riskitase on madal, kui tehingu summa kuus on vahemikus 0-15 000 eurot;
2. Kliendi riskitase on madal, kui tehingute summa aastas on kuni 15 000 eurot. Seejuures aastaseks perioodi hakatakse lugema alates sellest, kui klient on teinud esimese tehingu. Ühe aastane tähtaeg saabub järgmise aasta vastaval kuul ja päeval.  
*Näide: klient on registreerinud platvormil 01.01.2010, esimese tehingu on teinud 15.10.2020 kui tema tehingute summa kuni 15.10.2021 on kuni 15 000 eurot, kuulub ta Tier 1 kategooriasse;*
3. Kliendi riskiaste on madal, kui temaga on sõlmitud kirjalik kehtvusleping;
4. Kliendi riskiaste on madal, kui tehing on toimunud arvelduskonto või finantsasutuse pangakaardi kasutades;
5. Kliendi riskiaste on madal, kui klient on Euroopa majanduspiirkonna resident või tema elu- või asukoht on eelnimetatud riikides;
6. Kliendi riskiaste on madal, kui klient on Euroopa majanduspiirkonna kodanik;
7. Kliendi riskiaste on madal, kui kliendiks on reguleeritud turul noteeritud äriühing, kelle suhtes kohaldatakse avalikustamiskohustusi, millega on kehtestatud nõuded, et tagada tegeliku kasusaaja puhul piisav läbipaistvus;
8. Kliendi riskiaste on madal, kui ta on kinnitanud, et tema tegevusala või amet ei ole seotud riskantse tegevusvaldkonnaga, mis on välja toodud peatükis 3.1.
9. Kui kliendiks on Eestis asutatud avalik-õiguslik juriidiline isik;
10. Kui kliendiks on Euroopa liidu asutus;
11. Kui kliendiks on Eesti või Euroopa Majanduspiirkonna lepinguriigi valitsusasutus või muu avalikke ülesandeid täitev asutus;
12. Kui kliendiks on enda nimel tegutsev krediidasutus või finantseerimisasutus, Euroopa Majanduspiirkonna lepinguriigis või kolmandas riigis asuv krediidasutus või finantseerimisasutus, kelle kohta kehtivad tema asukohariigis Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849 nõuetega võrdväärsed nõuded, mille täitmise üle tehakse riiklikku järelevalvet;
13. Kui klient ei ole riikliku taustaga isik;
14. Kui klient ei ole sanktsiooni või embargo nimekirjas;
15. Kliendi riskiaste on madal, kui info Kliendi ja tema tegeliku kasusaaja kohta on avalikult kättesaadav;

customer's risk profile is the information gathered upon application of due diligence measures. AQdigital OÜ divides its customers into **low-risk (Tier 1)**, **medium-risk (Tier 2)** and **high-risk (Tier 3) customers**.

**Low-risk (Tier 1)** customers are those who meet the following characteristics:

1. the customer's risk level is low if the amount of the transaction is in the range of 0–15,000 euros per month;
2. the customer's risk level is low if the amount of the transactions is up to 15,000 euros per year; An annual period is counted from the moment the customer concludes the first transaction. The one-year deadline arrives on the respective day of the respective month in the next year.  
*Example: the customer registered on the platform on 1 January 2010, carried out the first transaction on 15 October 2020 and if the sum of their transactions until 15 October 2021 is up to 15,000 euros, they belong to Tier 1;*
3. the customer's risk level is low where a written long-term contract has been entered into with the customer;
4. the customer's risk level is low if the transaction was carried out using a bank account or a bankcard of a financial institution;
5. the customer's risk level is low if the customer is a resident of a contracting state of the European Economic Area or their place of residence or business is in the aforementioned countries;
6. the customer's risk level is low if the customer is a citizen of the European Economic Area;
7. the customer's risk level is low if the customer is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner;
8. the customer's risk level is low if the customer has confirmed that their area of activity or profession is not related to a risky area of activity, which is specified in Article 3.1;
9. the customer is a legal entity governed by public law established in Estonia;
10. the customer is an institution of the European Union;
11. the customer is a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area;

16. Kliendi riskiaste on madal, kui isiku tegevus ja tehingud on kooskõlas tema igapäevase majandustegevusega ning ei erine teiste sarnaste Klientide 11uest ja käitumistavadest;

17. Kliendi riskiaste on madal, kui puudub ükski kõrgemale riskikategooriale viitav tunnus.

Olukorras, kus vähemalt üks riskikategooria on kvalifitseeritav kui kõrge või keskmine, ei saa rahapesu või terrorismi rahastamise riskiaste olla üldjuhul madal. Madal risk ei tähenda siiski ilmtingimata seda, et Kliendi tegevust ei võiks üldse seostada rahapesu või terrorismi rahastamisega.

Madala riskiastmega tehinguteks peetakse tehinguid, mis ei viita ühelegi peatükis 3.1. kirjeldatud riski suurendavale asjaolule ning milliste puhul on lubatud kohaldada lihtsustatud hoolsusmeetmeid.

Kui kliendi riskitase on madal, rakendatakse tema suhtes lihtsustatud hoolsusmeetmeid, mis on välja toodud peatükis 4.10.

**Keskmise riskiga (tier 2)** kliendid on need, kelle suhtes esinevad järgmised tunnused:

1. Kliendi riskitase on keskmine, kui tehingu summa kuus on 15 001-50 000 eurot;
2. Kliendi riskitase on keskmine, kui tehingute kogusumma aastas on kuni 100 000 eurot. Seejuures aastaseks perioodi hakatakse lugema alates sellest, kui klient on teinud esimese tehingu. Ühe aastane tähtaeg saabub järgmise aasta vastaval kuul ja päeval;
3. Kliendi riskiaste on keskmine, kui temaga on sõlmitud kirjalik kehtvusleping;
4. Kliendi riskiaste on keskmine, kui tehing on toimunud arvelduskonto või finantsasutuse pangakaardi kasutades;
5. Kliendi riskitase on keskmine, kui kliendi elu- või asukoht või residentsus on Euroopa Liidu Majanduspiirkonnas või on teistes kolmandates riikides, mis ei ole seotud kõrge riskiga riigiga või keelatud riigiga, mis on välja toodud lisas 4<sup>2</sup>.

12. the customer is a credit institution or financial institution acting on its own behalf or a credit institution or financial institution located in a contracting state of the European Economic Area or a third country, which in its country of location is subject to requirements equal to those established in Directive (EU) 2015/849 of the European Parliament and of the Council and subject to state supervision;

13. the customer is not a politically exposed person;

14. the customer is not included in a sanctions or embargo list;

15. the customer's risk level is low if information about the customer and their beneficial owner is publicly accessible;

16. the customer's risk level is low if the person's activities and transactions are in line with its day-to-day business activities and do not differ from the payment behaviour or behavioural patterns of other similar customers;

17. The customer's risk level is low if nont of the characteristics referring to a higher risk category are present.

In a situation where at least one risk category can be qualified as high or medium, the risk level of money laundering or terrorist financing cannot usually be considered low. A low risk does not necessarily mean that the customer's operations cannot at all be associated with money laundering or terrorist financing;

low-risk transactions are those that do not refer to any risk-increasing factor described in Article 3.1 and whereby it is allowed to apply simplified due diligence measures;

If the customer's risk level is low, the customer is subject to the simplified due diligence measures described in Article 4.10.

**Medium-risk customers (tier 2)** are those with the following characteristics:

1. the customer's risk level is medium if the amount of the transaction is in the range of 15,001–50,000 euros per month;
2. the customer's risk level is medium if the total amount of the transactions is up to 100,000 euros per year; An annual period is counted from the moment the customer concludes the first transaction. The one-year deadline arrives on the respective day of the respective month in the next year;
3. the customer's risk level is medium if a written long-term contract has been entered into with the customer;
4. the customer's risk level is medium if the transaction was carried out using a bank

<sup>2</sup> Pidevalt tuleb jälgida riskiriikide nimekirja FATF-i <http://www.fatf-gafi.org/countries/#high-risk> ja EL Komisjoni kodulehel <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32020R0855&from=EN>, käesolevate protseduurireeglite

6. Kliendi riskitase on keskmine, kui kliendi kodakondsus ei ole seotud riskiriigiga ega keelatud riigiga;
7. Kliendi riskitase on keskmine, kui klient ei ole riikliku taustaga isik (PEP);
8. Kliendi riskitase on keskmine, kui klient ei ole sanktsioonide või embargo nimekirjas;
9. Kliendi riskitase on keskmine, kui info tegeliku kasusaaja kohta (UBO) ei ole avalikult kättesaadav;
10. Kliendi riskitase ei ole keskmine, kui kliendil esineb kasvõi üks kriteerium, mis viitab kõrgema riskikategooria tunnustele.
11. Kui kliendi riskitase on keskmine, rakendatakse tema suhtes kõrgendatud hoolsusmeetmeid, mis on välja toodud peatükis 4.11.

**Suure riskiga kliendid (tier 3)** on need, kelle suhtes esinevad lisaks Tier 1 ja/või Tier 2 tunnustele järgmised kõrgele riskile viitavad tunnused:

1. Kliendi riskitase on kõrge, kui tehingu summa kuus on üle 50 000 eurot;
2. Kliendi riskitase on kõrge, kui tehingute summas aasta on üle 100 000 eurot. Seejuures aastaseks perioodi hakatakse lugema alates sellest, kui klient on teinud esimese tehingu. Ühe aastane tähtaeg saabub järgmise aasta vastaval kuul ja päeval;
3. Kliendi riskitase on kõrge, kui Klient on riikliku taustaga isik või tema pereliige;
4. Kliendi riskitase on kõrge, kui kliendiks oleva äriühingu omandistruktuur näib äriühingu tegevust silmas pidades ebatavaline või liiga keeruline või ei ole võimalik kindlaks teha tegelikku kasusaajat;
5. Kui kliendi tegevus või tehing ei ole tavapärane ja ebanõistlik;

account or a bankcard of a financial institution;

5. The customer's risk level is medium if the customer's place of residence or seat or residency is in the European Economic Area or in other third countries not associated with a high-risk country or a prohibited country set out in Annex 4<sup>2</sup>;
6. the customer's risk level is medium if the customer's citizenship is not associated with a high-risk country or a prohibited country;
7. the customer's risk level is medium if the customer is not a politically exposed person (PEP);
8. the customer's risk level is medium if the customer is not included in the list of sanctions or embargoes;
9. the customer's risk level is medium if information about the ultimate beneficial owner (UBO) is not publicly available;
10. the customer's risk level is not medium if even one of the criteria referring to the characteristics of a higher-risk category exists;
11. if the customer's risk level is medium, the customer is subject to enhanced due diligence measures described in Article 4.11.

**High-risk customers (tier 3)** are those in respect of whom there following referring to high risk exist in addition to Tier 1 and/or Tier 2 characteristics:

1. the customer's risk level is high if the transaction amount is larger than 50,000 euros per month;
2. the customer's risk level is high if the sum of transactions is larger than 100,000 euros per year. An annual period is counted from the moment the customer concludes the first transaction. The one-year deadline arrives on the respective day of the respective month in the next year;
3. the customer's risk level is high if the customer is a politically exposed person or their family member;
4. the customer's risk level is high if the ownership structure of the customer

koostamise seisuga on EL Komisjon kinnitanud järgmised riigid, kui riskiriigid: Afganistan, Bahama, Barbados, Botswana, Kambodža, Ghana, Iraak, Jamaica, Mauritius, Mongoolia, Myanmar/Birma, Nicaragua, Pakistan, Panama, Süüria, Trinidad ja Tobaco, Uganda, Vanuatu, Jeemen, Zimbabwe. FATF on kinnitanud järgmised riigid, kui keelatud riigid: Iraan, Korea Rahvademokraatlik Vabariik.

<sup>2</sup> The list of high-risk countries must be constantly monitored on the websites of the websites of FATF <http://www.fatf-gafi.org/countries/#high-risk> and the European Commission <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32020R0855&from=EN>.

As at the preparation of these rules of procedure, the European Commission has specified that the following countries are high-risk countries: Afghanistan, Bahamas, Barbados, Barbados, Botswana, Cambodia, Ghana, Iraq, Jamaica, Mauritius, Mongolia, Myanmar/Birma, Nicaragua, Pakistan, Syria, Trinidad and Tobago, Uganda, Vanuatu, Yemen, Zimbabwe. FATF on confirmed that the following countries are prohibited: Iran, People's Republic of Korea.

6. Isikusamasuse tuvastamisel või esitatud teabe kontrollimisel on tekkinud kahtlus esitatud andmete tõe üle vastavuses või dokumentide ehtsuses või tegeliku kasusaaja tuvastamises;
7. isiku suhtes on teada eelnev rahapesu või terrorismi rahastamise kahtlus;
8. isiku välimus või käitumine võib viidata variisikuks olemisele;
9. ärisuhe toimib ebatavalistel asjaoludel, sealhulgas keeruliste ja ebatavaliselt suuremahuliste tehingute ning ebatavaliste tehingumustrite korral, millel ei ole mõistlikku, selget majanduslikku või õiguspärast eesmärki või mis ei ole konkreetse ärispetsiifika jaoks iseloomulik;
10. kliendiks on riskantse tegevusalaga tegelev isik;
11. kliendiks oleval või temaga seotud äriühingul on variaktsionärid või esitajaaktsiad (igasugune variaktsionäride ja variisikute jms kasutamine on selline risk, mida tuleks kindlasti igal juhul vältida, sest selliste riskide maandamine ei ole üldjuhul võimalik).

Kui kliendi riskitase on kõrge, siis rakendatakse tema suhtes peatükis 4.11. kirjeldatud kõrge riskitasemele rakendatavaid tugevdatud hoolsusmeetmeid.

Seejuures on oluline silmas pidada, et riskiriigi kriteerium ja sellega seonduvad asjaolud on äärmised olulised riskiprofiili määramisel. RAB andmetel on rahapesu ja terrorismi rahastamisele viitavate kahtlaste tehingutega on tegemist siis, kui esinevad järgmised tunnused:

1. füüsiline isik on sündinud riskiriigis;
  2. füüsiline isik omab riskiriigi kodakondsust;
  3. füüsiline isik omab elukohta riskiriigis;
  4. füüsiline isik on seotud riskiriigis registreeritud juriidilise isiku või muu ühendusega;
  5. juriidiline isik või muu ühendus on registreeritud riskiriigis;
  6. juriidilise isiku või muu ühenduse filiaali emafirma on registreeritud riskiriigis.
- Riskiastme määramine peab olema dokumentaalselt fikseeritud, selgitades, millistele asjaoludele tuginedes loetakse isik teatud riskiprofiiliga kliendiks. Selleks tuleb koostada riskiastme määramise otsus (lisa 1) või 13ue moodi fikseerida kliendi riskiaste, mis võimaldab hiljem andmeid taas esitada ja edastada RAB-ile. Isiku riskiastme määramine peab olema

company appears unusual or excessively complex, given the nature of the company's business, or the beneficial owner cannot be identified;

5. if the customer's activities or transaction is unusual and unreasonable;
6. upon identification of a person or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
7. a prior suspicion of money laundering or terrorist financing is known regarding the person;
8. the appearance or behaviour of the person may refer to them being a front;
9. the business relationship is based on unusual factors, including in the event of complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or lawful purpose or that are not characteristic of the given business specifics;
10. the customer is a person engaged in a risky area of activity;
11. the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares (any use of nominee shareholders or fronts, etc. is a risk that should be avoided at all times, because such risks cannot usually be mitigated).

If the customer's risk level is high, the enhanced due diligence measures applicable to high-risk customers described in Article 4.11. are applied to them.

Here, it is important to keep in mind that the risk country criterion and the related factors are of utmost importance in determining the risk profile.

According to the FIU, suspicious transactions indicative of money laundering and terrorist financing are those with the following characteristics:

1. the natural person was born in a high-risk country;
2. the natural person is a citizen of a high-risk country;
3. the natural person has a place of residence in a high-risk country;
4. the natural person is related to a legal entity or another association registered in a high-risk country;
5. the legal entity or other association is registered in a high-risk country;

kooskõlastatud/kinnitatud kontaktisiku või juhatuse poolt.

## 4 HOOLSUSMEETMED

### 4.1 Hooldusmeetmete rakendamine ja liigid

Hooldusmeetmeid tuleb rakendada järgmistel juhtudel:

- ärisuhte loomisel;
- rahapesu või terrorismi rahastamise kahtluse korral;
- isikusamasuse tuvastamise ja esitatud teabe kontrollimise käigus kogutud teabe või dokumentide tõele mittevastavuse kahtluse korral;
- hooldusmeetmete kohaldamisel kogutud teabe kontrollimise või ajakohastamise käigus varem kogutud dokumentide või andmete piisavuse või tõele vastavuse kahtluse korral.

Virtuaalvääringu teenuse pakkujal on keelatud osutada ärisuhte väliselt teenuseid (§ 25 RahaPTS), hooldusmeetmed tuleb rakendada alati.

Rahapesu tõkestamise hooldusmeetmed on järgmised:

- 1) kliendi isikusamasuse tuvastamine ja kontrollimine usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal;
- 2) füüsilise või juriidilise isiku esindaja isikusamasuse ja esindusõiguse tuvastamine ning kontrollimine;
- 3) tegeliku kasusaaja tuvastamine usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal;
- 4) teabe hankimine ärisuhte ja tehingu eesmärgi ning olemuse kohta;
- 5) ärisuhte pidev jälgimine, sealhulgas ärisuhte vältel teostatud tehingute jälgimine, kontrollimaks, et need oleksid kooskõlas kliendi või tegeliku kasusaaja tavapärase majandustegevuse ja riski profiiliga ning vajaduse korral tehingus kasutatud vahendite allika ja päritolu tuvastamine.

Lähtuvalt hooldusmeetmete rakendamise hetkest võib need jagada kaheks: hooldusmeetmed, mida rakendatakse enne kliendi aktsepteerimist ja kliendisuhete loomist, ja hooldusmeetmed, mida kohaldatakse kliendisuhete ajal. Sel hetkel, kui hakatakse klienti aktsepteerima ja temaga kliendisuhet looma, tuleb alati kohaldada nõuetekohaseid hooldusmeetmeid. See, kui

6. the parent company of a branch of a legal entity or other association is registered in a high-risk country.

The determination of the risk level must be documented, explaining the factors based on which the person is deemed as a customer of a certain risk profile. For that purpose, a risk level determination decision must be drawn up (Annex 1) or the customer's risk level must be fixed in another manner that allows for subsequent reproduction of data and forwarding thereof to the FIU. Determination of a person's risk level must be approved/confirmed by the Compliance Officer or the Management Board.

## 4 DUE DILIGENCE MEASURES

### 4.1 Application and types of due diligence measures

Due diligence measures must be applied in the following events:

- upon establishment of a business relationship;
- upon suspicion of money laundering or terrorist financing;
- in the case of doubts as to the truthfulness of the information or documents gathered in the course of identifying a person and verifying submitted information;
- in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered earlier in the course of verifying or updating information collected during the application of due diligence measures.

Providers of virtual currency services are not allowed to provide services outside a business relationship (§ 25 MLTFPA), due diligence measures should be applied all the times.

The due diligence measures aimed at prevention of money laundering are the following:

- 1) identification and verification of identity of a customer on the basis of information obtained from a reliable and independent source;
- 2) identification and verification of identity of a natural person or a representative of a legal person and identification and verification of the right of representation;
- 3) identification of the beneficial owner on the basis of information obtained from a reliable and independent source;
- 4) acquisition of information about the purpose and nature of a business relationship and a transaction;
- 5) constant monitoring of a business relationship, including monitoring of transactions entered into during the business relationship, in order to verify whether these correspond to the ordinary business activities and risk profile of the customer or the beneficial owner and, where necessary,

intensiivne peab olema hoolsusmeetmete kohaldamine, sõltub kliendi riskiprofiilist. Personal peab alati olema veendunud, et Äriühingu klient on see, kes ta väidab end olevat, mistõttu tuleb kliendi isiku tuvastamisel ja kontrollimisel lähtuda isikut tõendavatest dokumentidest. Seevastu kliendisuhete ajal kohaldatavate hoolsusmeetmete eesmärk on kliendi tehingute jälgimise abil veenduda, et kliendi tegevus on kooskõlas mõistlike ootuste ja eeldustega tema ning tema poolt kasutatava teenustega.

Äriühingu Personal peab pöörama oma tegevuses kõrgendatud tähelepanu tehingutele, mis viitavad rahapesule või terrorismi rahastamisele, sealhulgas keerukatele, suure väärtusega ja ebatavalistele tehingutele, millel ei ole mõistlikku majanduslikku eesmärki. Eeltoodu kohaselt peab Personal hoolsusmeetmete rakendamisel tuvastama, kes on tegelikkuses äriühingu klient, kust pärineb tehingus kasutatav raha ning kellele see tegelikult kuulub. Selline kohustus eeldab oma kliendi kohta info kogumist ning seeläbi tema tundmist.

Rakendatavate hoolsusmeetmed ja nende ulatus sõltub kliendi riskiprofiilist, mis määratakse vastavalt Kliendi poolt täidetud ankeedile ja edastatud andmetele (lisa 2), mille kohta säilitatakse andmeid (riski määramise otsuse koostades (lisa 1) või muul viisil). Äriühingu poolt rakendatavad hoolsusmeetmed on kirjeldatud Aqdigital riskiprofiili tabelis (lisa 3) ja seletatakse detailsemalt peatükkides 4.10 ja 4.11.

#### **4.2 Isikusamasuse tuvastamine füüsilise isiku puhul**

Füüsilise isiku isikusamasuse tuvastamine ja kontrollimine toimub üldreeglina ühe ja sama toiminguna isikut tõendava dokumendi alusel. Isikusamasuse tuvastamisel tuleks lähtuda usaldusväärsetest ja sõltumatutest allikatest. Usaldusväärne ning sõltumatu allikas on eelkõige riigiasutuste erinevad IT-lahendused dokumentide kehtivuste ning andmete kontrollimiseks, samuti erinevate riiklike registrite informatsioon. Juhul, kui isikusamasuse tuvastamisel ei ole kogutud informatsiooni võimalik usaldusväärsest ja

identification of the source and origin of the funds used in the transaction.

Based on the moment of application of the due diligence measures, they can be divided into two categories: the due diligence measures applied before accepting a customer and establishing a customer relationship; and the due diligence measures applied during a customer relationship. The required due diligence measures must always be applied upon accepting a customer and establishing a customer relationship with the customer. The intensity of application of the due diligence measures depends on the customer's risk profile. The Staff must always be convinced that a customer of the Company is who they say they are. Therefore, a customer needs to be identified and their identity verified on the basis of their identity documents. However, the purpose of the due diligence measures applied during a customer relationship is to make certain by monitoring the customer's transactions that the customer's activities correspond to reasonable expectations and assumptions concerning the customer and the services used by the customer.

In their activities, the Staff of the Company must pay special attention to transactions indicative of money laundering or terrorist financing, including to complex, high-value and unusual transactions that do not have any reasonable economic purpose. According to the aforementioned, upon application of the due diligence measures, the Staff must identify who the Company's customer actually is, where the money used in the transaction comes from and whom it actually belongs to. Such responsibility calls for collecting information on the customer and, thus, knowing the customer.

The due diligence measures to be applied and the extent thereof depends on the customer's risk profile that is determined on the basis of the questionnaire filled in by the customer and data given by the customer (Annex 2), about which data are retained (by preparing the risk determination decision (Annex 1) or in another manner). The due diligence measures applied by the Company have been described in the AQdigital's risk profile table (Annex 3) and explained in more detail in Articles 4.10 and 4.11.

#### **4.2 Identification of a natural person**

The identification and verification of the identity of a natural person must be carried out, as a general rule, in one step on the basis of an identity document.

A person should be identified on the basis of credible and independent sources. Credible and independent sources are, above all, various governmental IT solutions for verification of the

sõltumatust allikast kontrollida, ärisuhet luua ei tohi. Samuti ei tohi jätkata koostööd Kliendiga, kes ei ole nõus isikusamasuse tuvastamiseks vajalikke andmeid ajakohastama.

Kliendi tuvastamisel tuleb füüsilise isiku puhul koguda ja säilitada järgmised andmed

Madala (Tier 1), keskmise (Tier 2) ja kõrge riskiprofiiliga (Tier 3) klientide puhul:

- nimi;
- isikukood, selle puudumise korral sünniaeg ja -koht;
- elukoha aadress;
- e-post;
- kodakondsus;
- ärisuhte loomise eesmär;
- andmed tegevusala kohta;
- tegelik kasusaaja, kui selleks esineb vajadus vastavalt Juhendile.

Füüsilise isiku tegelikku kasusaajat peab tuvastama kahtluse korral, kui tekib tunne, et füüsilist isikut on palutud, meelitatud, ähvardatud, ära ostetud või muul viisil kallutatud ärisuhte loomisele või tehingu tegemisele. Sellisel juhul peetakse isikut, kes teostab kontrolli füüsilise isiku üle, füüsilise isiku tegelikuks kasusaajaks.

Füüsilise isiku isikusamasuse tuvastamine ja kontrollimine toimub isikut tõendava dokumendi alusel. Isikusamasuse tuvastamist ja kontrolli viib läbi Kliendiga vahetult kontaktis olev Personal. Äriühingu Personal fikseerib Kliendi elukoha ning ärisuhte loomise eesmärgi tema ütluste kohaselt. Personal teeb koopiid isiku poolt esitatud dokumendist ja salvestab andmeid. Samuti on võimalik füüsilise isiku tuvastamine elektroonsete vahendite abil, täpsem protseduur ja reeglid on kirjeldatud peatükis 4.5. Aqdigital tuvastab ja kontrollib oma füüsilisest isikust kliente eelkõige infotehnoloogiliste vahendite abil.

**Isikusamasuse tuvastamise alusena** on lubatud kasutada järgmisi kehtivaid dokumente:

- isikutunnistus;
  - digitaalne isikutunnistus
  - elamisloakaart;
- Eesti kodaniku pass;
- diplomaatiline pass;
- meremehe teenistusraamat;
- välismaalase pass;
- ajutine reisidokument;
- pagulase reisidokument;
- meresõidutunnistus;
- tagasipöördumistunnistus;
- tagasipöördumise luba;
- välisriigi kodaniku pass;
- Euroopa Liidu kodaniku ID-kaart;
- juhiluba, kui dokumenti on kantud kasutaja nimi, foto või näokujutis, allkiri või allkirjakujutis ja sünniaeg või isikukood.

validity of documents and verification of data as well as information obtained from various public registers. If the information gathered upon identifying a person cannot be verified from a credible and independent source, it is prohibited to establish a business relationship. Cooperation with a customer who is not willing to update their data required for identification may not be continued. Upon identifying a customer who is a natural person, the following data must be collected and retained.

In the case of customers with a low (Tier 1), medium (Tier 2) and high (Tier 3) risk profile:

- name;
- personal identification code or, if none, the date and place of birth;
- address of the place of residence;
- email;
- citizenship;
- the purpose of establishment of the business relationship;
- data on the field of activity;
- beneficial owner, where prescribed by the Guidelines.

The beneficial owner of a natural person must be identified if there is a reason to suspect that the natural person has been asked, cajoled, threatened, bribed or otherwise inclined to establish the business relationship or to make the transaction. In such an event the person who exercises control over the natural person must be deemed their beneficial owner.

The identification and verification of the identity of a natural person is carried out on the basis of an identity document. The identification and verification of identity is carried out by the Staff meeting the customer in person. The Company's Staff records the customer's place of residence and the purpose of establishment of the business relationship based on the customer's oral statements. The Staff makes a copy of the document submitted by the person and records data. It is also possible to identify a natural person via electronic means. A more detailed procedure and rules are given in Article 4.5. Aqdigital identifies a customer who is a natural person and verifies their identity primarily by using information technology means.

The following valid documents can be used as a **basis for identification**:

- an identity card;
  - a digital identity card;
  - a residence permit card;
- an Estonian citizen's passport;
- a diplomatic passport;
- a seafarer's discharge book;
- an alien's passport;
- a temporary travel document;



Isikut tõendava dokumendi esitamisel tuleks kontrollida:

- a) dokumendi kehtivust
- b) isiku välist samasust dokumendil oleva pildiga
- c) isikukoodi vastavust soole ja vanusele
- d) välisriigi kodanike puhul veenduda dokumendi ehtsuses ja kahtluse korral pöörduda Äriühingu juhatuse liikme poole ning võtta ühendust dokumendi ehtsuse kontrollimiseks vastava riigi välisesindusega või Välisministeeriumiga.

Kui isikutuvastamisel ei ole võimalik näha isikut tõendava dokumendi originaaldokumenti, võib kasutada isikusamasuse kontrollimiseks notariaalselt tõestatud või ametlikult kinnitatud dokumenti või muud usaldusväärsest ja sõltumatust allikast pärit teavet. Äriühing võib küsida isikutõendava dokumendi notariaalset või ametlikult kinnitatud dokumendi, kui klient kuulub Tier 3 riskikategooriasse või kui tekib kahtlus esitatud dokumendi usaldusväärsuses ja/või ehtsuses.

Oluline on silmas pidada, et kliendi isiklik tundmine või tema avalik tuntus ei ole aluseks seaduses sätestatud isikusamasuse tuvastamise siseprotseduuri mittetäitmiseks. Isikusamasust tuleb kontrollida ka kohustatud isiku poole tehingute või toimingute tegemiseks pöörduvatel avalikult tuntud ning nendega otseselt või kaudselt seotud isikutel.

Kliendi isiku tuvastamine ei ole ühekordne toiming. Personal peab regulaarselt uuendama kliendi isikuandmeid ning tegevusprofiili, tagades andmete ajakohasuse. Tulenevalt eeltoodust peavad kõik kliendid läbima isikusamasuse kontrolli tehingu tegemisel, ärisuhte loomisel ja ärisuhte kestel.

Isikusamasuse tuvastamise andmeid peab ajakohastama. Personal ajakohastab isikusamasuse tuvastamisel ja kontrollimisel saadud andmed vähemalt üks kord kahe aasta jooksul madala riskitaseme (Tier 1), vähemalt üks kord aastas keskmise riskitaseme (Tier 2) ja kõrge riskitaseme (Tier 3) puhul kaks korda aastas. Väga madala (Tier 0) klientide puhul ei toimu andmete uuendamist ja ajakohastamist.

Ajakohastamiseks teeb Personal järgmisi 17 ues:

- a) kontrollib andmeid üle avalikes andmekogudes ja registrites;
- b) dokumendi kehtivuse lõppemisel kontakteerub Kliendiga ning nõuab dokumendi uuendatud versiooni esitamist.

Juhul kui klient ei nõustu esitama uuendatud andmeid dokumendi kehtivuse lõppemisel, teavitada sellest Äriühingu kontaktisikut ja lõpetada temaga ärisuhe.

- a travel document for a refugee;
- a certificate of record of service on ships;
- a certificate of return;
- a permit of return;
- a foreign citizen's passport;
- an ID card of a citizen of the European Union;
- a driving licence, provided that the licence holder's name, photo or facial image, signature or signature image and date of birth or personal identification code have been indicated on the document.

Upon presentation of an identity document, the following should be verified:

- a) validity of the document;
- b) person's external similarity with the photo on the document;
- c) whether the personal identification code matches the gender and age;
- d) in the case of foreign nationals, the authenticity of the document must be checked. If there are any doubts, a member of the Management Board of the Company must be addressed and, to verify the authenticity of the document, a foreign mission of the country or the Ministry of Foreign Affairs must be contacted.

If it is impossible to use an original identity document with a photo to identify the person, a document authenticated by a notary or certified officially or other information obtained from a reliable and independent source can be used for verification of the identity. The Company may request a document authenticated by a notary or certified officially if the customer is included in the Tier 3 risk category or if there are doubts as to the reliability and/or authenticity of the document submitted.

It is important to keep in mind that even if the obliged entity knows the customer personally or the customer is a public figure, the internal identification procedure provided by law cannot be disregarded. The identity of the public figures and persons directly or indirectly related to them who address the obliged entity to make transactions or perform acts must also be verified.

The identification of a customer is not a one-off step. The Staff must regularly update the customer's personal data and operation profile, ensuring that they are up to date. In view of the above, all the customers must undergo identification upon making a transaction, establishing a business relationship and during the business relationship.

Identification data must be updated. The Staff updates data obtained upon identification and

### 4.3 Isikusamasuse tuvastamine juriidilise isiku puhul

Juriidiline isik tegutseb alati oma juhatuse või juhatuse poolt volitatud esindaja kaudu. Juriidilise isiku isikusamasuse tuvastamisel on oluline tuvastada nii juriidiline isik kui tema esindajat.

Juriidilise isiku tuvastamisel tuleb välja selgitada:

- ärinimi;
- registrikood;
- asukoht ja tegevuskoht;
- juhatuse liikme nimed ja nende volitused või esindaja andmed;
- sidevahendite andmed (e-mail, website);
- tegevusala;
- ärisuhte loomise eesmärk;
- riikliku taustaga isiku olemasolu;
- tegelike kasusaajate andmeid.

Samuti tuleb tuvastada ka isiku kui potentsiaalse ärisuhtes oleva kliendi tegevusprofiil, tegevuse eesmärk, ärisuhte loomise eesmärk ja iseloom ning muu sarnane oluline informatsioon ärisuhte loomiseks.

Juriidilise isiku isikusamasuse ja õigusvõime tuvastamine ning kontrollimine toimuvad üldreeglina äriregistri (Eestis) või muu samaväärse registri andmete alusel või registreerimistunnistuse ära kirja või sellega samaväärse dokumendi alusel, mis on õigusaktides ettenähtud korras esitatud.

Klient ei pea esitama registrikaardi väljatrükki, kui Personalil on ligipääs äriregistri, mittetulundusühingute ja sihtasutuste registri või välisriigi asjakohaste registrite andmetele arvutivõrgu kaudu ja andmeid on võimalik usaldusväärsest allikast kontrollida. Sellisel juhul teeb Personal ise väljatrükki Kliendi registrikaardist ja salvestab need andmed, märkides juurde väljatrükki tegemise kuupäeva.

Kui Klient on juriidiline isik, kes ei ole asutatud Eestis, tuleb küsida Kliendi registrikaardi väljatrükk. Registrikart peab olema väljastatud

verification of identity at least once every two years in the case of a low risk level (Tier 1), at least once a year in the case of a medium risk level (Tier 2) and twice a year in the case of high risk levels (Tier 3). Data are not renewed and updated in the case of customers with a very low risk profile (Tier 0).

To update data, the Staff takes the following steps:

- a) verifies data in public databases and registers;
- b) upon expiry of a document, contacts the customer and asks for a new version of the document.

If the customer is not willing to submit updated data upon expiry of the document, the Compliance Officer the Company must be informed about it and the business relationship with the customer must be terminated.

### 4.3 Identification of a legal entity

A legal entity always acts via its Management Board or via a representative authorised by its Management Board. Upon identifying a legal entity, it is important to identify the legal entity as well as its representative.

Upon identifying a legal entity, the following must be identified:

- business name;
- registry code;
- seat and place of business;
- names and authorisation of the members of the Management Board or representative;
- contact details (email, website);
- field of activity;
- purpose of establishment of a business relationship;
- politically exposed persons, if any;
- data of beneficial owners.

The operation profile and purpose of operation of the person as a potential customer having a business relationship and the purpose of establishment and nature of the business relationship and other similar important information required for the establishment of a business relationship must be identified as well.

The identification and verification of the identity and passive legal capacity of a legal entity is carried out, as a rule, on the basis of the data of the commercial register (in Estonia) or that of another equivalent register or a copy of the registration certificate or an equivalent document submitted in accordance with the procedure provided for in law.

If the Staff has access to the commercial register, non-profit associations and foundations register or the data of the relevant registers of a foreign country via the computer network and is able to verify the data from a credible source, the customer does not need to submit a printout of the

keeles, mida Personal valdab piisaval tasemele (19uestio, vene, eesti).

Registrist väljastatavad või sellega samaväärsed dokumendid ei tohi olla välja antud varem kui 6 kuud enne esitamist Aqdigital OÜ-le. Personal võib kahtluse korral nõuda ka notariaalselt tõendatud, ametlikult kinnitatud ja/või apostillitud registrikaardi väljatrukki kui klient kuulub Tier 3 kategooriasse.

Juriidilise isiku isikusamasuse tuvastamisel on oluline säilitada ka juriidilise isiku esindaja isikuttõendava dokumendi andmed ja täpsustada järgmised andmed:

1. juriidilise isiku juhataja, välismaa äriühingute puhul juhatause või muu seda asendava organi liikmete nimed ja nende volitused esindamisel;
2. juriidilise isiku põhiline tegevusvaldkond;
3. tegeliku kasusaaja andmed.

Lisaks juriidilisele isikule juriidilise isiku juhataja, juhatause liige või muud volitatud või lepinguline esindaja peab läbima samasuguse isikusamasuse tuvastamise protseduuri nagu füüsilisest isikust klient.

Välismaa juriidiliste isikute puhul tuleb rakendada isikusamasuse tuvastamiseks maksimaalselt sarnaseid meetmeid, mis Eesti juriidiliste isikute puhul, kuid välisriikide regulatsioonide erinevuse tõttu ei pruugi see olla lihtne ja üksühele võimalik. Õigusliku regulatsiooni erinevuse tõttu erinevates riikides tuleb tähelepanu pöörata eelkõige madala maksumääraga riikides või piirkondades asutatud äriühingutele, kelle õigusvõime olemasolu ei ole alati üheselt mõistetav.

Kui juriidilisest isikust klient on registreeritud riskiriigis või keelatud riigis, siis ärisuhte loomine on keelatud.

#### **4.4 Esindusõiguse tuvastamine ja kontroll**

Personal peab kindlaks tegema, kas isik tegutseb enda või teise (füüsilise või juriidilise) isiku nimel. Kui isik tegutseb teise isiku nimel, peab kohustatud isik selgitama ka selle isiku, kelle nimel tehinguid tehakse. Töötaja peab välja selgitama esindaja esindusõiguse aluse, ulatust ja kehtivuse aja. Esindajalt tuleb nõuda esindusõigust tõendava

registry card. In such an event, the Staff makes a printout of the customer's registry card and records the data, indicating the date of making the printout. A printout of the customer's registry card must be requested if the customer is a legal entity not established in Estonia. The registry card must be issued in a language that the Staff has sufficient knowledge of (English, Russian, Estonian).

Documents issued by a register or equivalent documents must have been issued not earlier than six months prior to their submission to Aqdigital OÜ. In the case of suspicions, the Staff may also demand a printout of the registry card authenticated by a notary or certified officially and/or having an apostille if the customer belongs to Tier 3.

Upon identification of a legal entity, it is also important to retain the data of the identity document of the representative of the legal entity and to clarify the following data:

1. the names of the manager of a legal entity, in the event of a foreign company the names of members of the Management Board or other body replacing the Management Board, and their authorisation in representing the legal entity;
2. the main field of activity of the legal entity;
3. data of the beneficial owner.

In addition to the legal entity, the director, member of the Management Board or other authorised or contractual representatives of the legal entity must pass a similar identification procedure as the one applied to customers who are natural persons.

In the case of foreign legal entities, the measures applied for identification must be as similar to those applied to Estonian legal entities as possible, but due to regulatory differences between foreign countries, it may not be easy or fully possible. Due to differences in the legislation of different countries, attention must be paid to, above all, companies established in countries or regions with a low tax rate, because it is not always abundantly clear whether they have passive legal capacity.

The establishment of a business relationship with a customer who is a legal entity registered in a high-risk country or prohibited country is not allowed.

#### **4.4 Identification and verification of the right of representation**

The Staff must verify whether the person is acting on their own behalf or on behalf of another (natural or legal) person. If the person is acting on behalf of another person, the obliged entity must also identify the person on whose behalf transactions are made. The employee must identify the basis, scope and term of validity of the representative's

dokumendi esitamist. Esindus võib olla seadusjärgne ja lepinguline (näiteks juhatuse liikme volitus äriühingu esindamiseks on seadusest tulenev, juriidilise isiku tegevjuhi volitus on tehingust/lepingust tulenev).

Juriidilise isiku isikusamasuse tuvastamise dokumendid esitab juriidilise isiku seadusjärgne või volitatud esindaja. Kohustatud isik peab veenduma esindusõiguse vastavuses õigusaktides sätestatud nõuetele. Kui esitatud dokumentidest ei selgu neid esitava füüsilise isiku esindusõigus ja/või volitus ei ole nõuetekohane, siis ei saa isikusamasuse tuvastamise (seega ka ärisuhte loomise ja/või tehingu tegemise) protsessi jätkata.

Kui tegemist on esindusõigusega, mis tuleneb lepingust ja on väljastatud volitus, siis tuleks nõuda koopiat volikirja või lepingust. Samuti tuleb täpsustada volitatud esindajale antud esindusõiguse ulatust (Näiteks, kas tegemist on ühekordse tehinguga või korduvate tehingute tegemisega teatud perioodi jooksul). Personal peab jälgima volitatud esindajatele antud esindusõiguse tingimusi ning osutama teenuseid ainult esindusõiguse ulatuses. Näiteks juhul kui volitatud esindajal esitatud volikirja alusel on õigus äriühingu nimel allkirjastada lepinguid ja esitada avaldusi, siis muid sätestamata õigusi volitatud esindajal pole ning seda tuleks arvestada teenuse osutamisel Kliendile.

Tulenevalt eeltoodust, kui äriühingu esindajaks on keegi muu kui juhatuse liige, siis tuleks nõuda esindusõigust tõendava dokumendi esitamist ja veenduda esindusõiguse olemasolus ja volituste ulatuses ehk selles, milliseid faktilisi toiminguid on isik õigustatud tegema esindatava äriühingu nimel. Kui tekib kahtlus volitatud esindajas või seadusjärgses esindajas, tuleks veenduda selles, kas esindaja tunneb esindatavat. Tuleks veenduda, kas esindaja teab:

- tema poolt esindatava isiku tahteavalduste sisu ja eesmärgi;
- esindatava majandus- ja kutsetegevusest;
- tehingute eesmärgi; isiku tegevuspartneritest;
- tehingus kasutatavate vahendite allika ning päritolu;
- juriidilise isiku omanikeringi.

Kõik eelnimetatud andmed on olulised selleks, et veenduda, et esindaja on tõepoolest seotud esindatavaga ning käitub tema huvides.

right of representation. The representative must be asked to submit a document proving the right of representation. Representation may be statutory or contractual (e.g. the authorisation of a member of the Management Board to represent the company arises from law, while the authorisation of the CEO of a legal entity arises from a transaction/contract).

Documents required for identifying a legal entity must be submitted by the legal representative or authorised representative of the legal entity. The obliged entity must make certain that the right of representation complies with the requirements provided by law. If the submitted documents do not indicate the right of representation of the natural person submitting them and/or the authorisation is not in compliance with the requirements, the identification process (and, thus, also the establishment of the business relationship and/or execution of the transaction) cannot be continued. In the case of a right of representation, which arises from a contract and a power of attorney has been issued, a copy of the power of attorney or contract should be requested. Clarification must be sought on the scope of the right of representation granted to the authorised representative (for instance, whether a one-off transaction or recurring transactions over a certain period are involved). The Staff must take notice of the terms of the right of representation granted to the authorised representative and provide services only to the extent of the right of representation. For instance, if the authorised representative has the right to sign contracts and submit applications on behalf of the company on the basis of a submitted power of attorney, the authorised representative does not have any other unspecified rights and that must be taken into account upon provision of the customer with the service.

In view of the above, if a company is represented by someone other than a member of the Management Board, they should be asked for a document certifying their right of representation and the existence of their right of representation and the scope of their authorisation should be verified, i.e. which actual steps the person is entitled to take on behalf of the represented company.

If suspicions arise about an authorised representative or legal representative, it should be verified whether the representative knows the principal. It should be verified whether the representative knows:

- the substance and purpose of the declarations of intent of the person represented by the representative;
- the economic and professional activities of the principal;

#### 4.5 Isikusamasuse tuvastamine infotehnoloogiliste vahendite abil

Kliendi isikusamasuse tuvastamine on võimalik ka infotehnoloogiliste vahendite abil, kui pole võimalik isiklik kohtumine Kliendiga tema identifitseerimiseks. Üldjuhul toimub klientide identifitseerimine infotehnoloogiliste vahendite abil. Äriühing lähtub isikusamasuse tuvastamise infotehnoloogiliste vahendite abil Rahandusministri määrusest „Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise tehnilised nõuded ja kord“.<sup>3</sup> Kui tegemist on madala riskiga (tier 1) Kliendiga, siis kliendi isikusamasuse tuvastamiseks ja kontrollimiseks peab Klient esitama:

- 1) Koopia/foto isikut tõendavast dokumendist
- 2) Foto enda näokujutisest (selfie)
- 3) Foto enda näokujutisest (selfie) koos isikut tõendava dokumendiga ja paberi koos kuupäevaga
- 4) Peab läbima video verifitseerimise, mille raames isik liigub kaamera ees (liveness check), misjärel veendutakse, et video olev isik langeb dokumendil oleva isiku pildiga. Eelnimetatud teenust osutab Äriühingule rahvusvaheliselt tunnustatud verifitseerimise teenuse osutaja Sum&Substance <https://sumsub.com/>.

Infotehnoloogiliste vahendite abil isikusamasuse tuvastamisel ja kontrollimisel kehtivad isiku pildile (selfiele) järgmised nõuded:

1. isiku pea ja õlad peavad olema nähtavad;
2. nägu peab olema varjudeta;
3. nägu peab olema taustast selgelt eristatav ja äratuntav;
4. nägu peab olema ilma prillideta;
5. nägu peab olema katmata.

Kui tegemist on keskmine riski (Tier 2) Kliendiga, siis lisaks eelmainitud kohustusele (edastada koopia isikut tõendavast dokumendist, teha selfie ja teha selfie koos dokumendiga ning ka video verifitseerimine ehk liveness check), teeb Äriühing online video intervjuu Kliendiga, mille käigus on Personalil õigus esitada täiendavad küsimused ja tuvastada isikut täiendavalt video vahendusel.

- the purpose of the transactions; the business partners of the principal;
- the source and origin of the funds used in the transaction;
- the circle of the owners of the legal entity.

All the aforementioned data are important for making certain that the representative is indeed linked to the principal and acts in their interests.

#### 4.5 Identification of a person using information technology means

It is possible to identify a customer using information technology means if the customer cannot be met face-to-face for the purpose of identifying the customer. As a rule, customers are identified using information technology means. Upon identification of a person using information technology means, the Company adheres to the Regulation “Technical Requirements of and Procedure for Identification of Persons and Verification of Data Using Information Technology Means” of the Minister of Finance<sup>4</sup>.

A low-risk (tier 1) customer must, for the purpose of being identified and having their identity verified, submit:

- 1) a copy/photo of the identity document;
- 2) a photo of their facial image (selfie);
- 3) a photo of their facial image (selfie) along with an identity document and a paper with the date;
- 4) a video verification must be passed, which involves the customer moving in front of the camera (liveness check), followed by the verification that the person in the video is the same as the person whose photo is on the document. The aforementioned services is provided to the Company by the internationally recognised verification service provider Sum&Substance <https://sumsub.com/>.

Upon identification of persons and verification of identity using information technology means, the photo (selfie) of a person must comply with the following requirements:

1. the person's head and shoulders must be visible;
2. the face must be clear of shadows;
3. the face must be clearly distinguishable from the background and recognisable;
4. the person may not wear glasses;
5. the face must be uncovered.

If the risk level of the customer is medium (Tier 2), the Company carries out an online video interview with the customer, during which the Staff has the

<sup>3</sup> <https://www.riigiteataja.ee/akt/125052018017>

Kui tegemist on kõrge riski Kliendiga (tier 3) ja Äriühingul on tekkinud kahtlus isikusamasuse tuvastamisel, siis lisaks eelmainitud kohustusele küsib Äriühingu notariaalselt tõestatud või ametlikult kinnitatud koopiat isikut tõendavast dokumendist, et veenduda isiku dokumendi ehtsuses ja usaldusväärsuses.

Isikusamasuse tuvastamine on võimalik nii äriühingu enda Personali poolt kui ka usaldusväärsete äriühingute kaudu, mis pakuvad verifitseerimisteenuseid, seejuures jälgib äriühingu RahaPTS § 24 sätestatud reegleid seoses teiste isikute poolt kogutud andmete tuginemisega ja sõlmib temaga kirjalikku lepingu.

Äriühing kasutab järgmise partneri verifitseerimise teostamiseks:

Sum & Substance- Sum and Substance LTD, address 30 St. Mary Axe, London, England, EC3A 8BF, registrikood 09688671, koduleht <https://sumsub.com>

Kui esitatakse Koopia või foto isikuttõendavast dokumendist, siis tuleb samamoodi nagu ka tavalise isikuttõendava dokumendi puhul pöörata tähelepanu järgmistele olulistele asjaoludele:

- Veenduda, et dokumendi liik võimaldab isiku tuvastamist;
- Veenduda, et edastatud fotol või koopial on andmed selgelt nähtavad;
- Veenduda dokumendi kehtivuses<sup>4</sup>;
- välisriigi kodanike puhul veenduda dokumendi ehtsuses ning kahtluse korral võtta ühendust dokumendi ehtsuse kontrollimiseks vastava riigi välisesindusega või Välisministeeriumiga, või küsida notariaalselt tõestatud või ametlikult kinnitatud koopiat või kontrollida dokumendi muust usaldusväärsest ja sõltumatust allikast.<sup>5</sup>

EL liikmesriikide dokumentide kehtivust on võimalik kontrollida PRADO 22uestion poolt loodud juhendi abil. Juhendis on olemas info iga riigi kohta, milliste kanalite ja veebilehtede kaudu on võimalik kontrollida dokumentide kehtivust.<sup>6</sup>

Kui tegemist on keskmise ja kõrge riskitaseme kliendiga, siis kliendiga korraldatakse lisaks ka video intervjuu. Video intervjuu eesmärgiks on veenduda, et verifitseerimist läbiv isik on elus ning seesama isik, kes on ankeetküsitluse täitnud ning esitanud oma isikut tõendavat dokumenti. Intervjuu

right to ask additional questions and identify the person additionally via video, in addition to the obligation specified above (to send a copy of the identity document, take a selfie and take a selfie with a document, video verification, i.e. liveness check).

If the risk level of the customer is high (Tier 3) and the Company becomes suspicious during identification, the Company requests a copy of an identity document, which is authenticated by a notary or certified officially, in order to make certain that the document is authentic and reliable, in addition to the obligation specified above.

The identification can be carried out by the Staff of the Company as well as by using reliable companies providing verification services. Thereby the Company adheres to the rules provided for in § 24 of the MLTFPA concerning reliance on data gathered by other persons and enters into a written contract with such a person.

The Company uses the following partner for verification:

Sum & Substance – Sum and Substance LTD, address 30 St. Mary Axe, London, England, EC3A 8BF, registry code 09688671, website <https://sumsub.com>.

If a copy of an identity document or a photo is submitted, attention must be paid to the following essential aspects, similarly to ordinary identity documents:

- it must be made certain that the document type allows for establishing the person's identity;
- make sure that the data on the sent photo or copy are clearly visible;
- It must be made certain that the document is valid<sup>5</sup>;
- in the case of foreign nationals, the authenticity of the document must be checked. If there are any doubts, a foreign mission of the country or the Ministry of Foreign Affairs must be contacted to verify the authenticity of the document, or a copy authenticated by a notary or certified officially must be requested or the document must be verified on the basis of any other reliable and independent source<sup>6</sup>.

<sup>4</sup> Dokumendi kehtivust on võimalik kontrollida siin: <https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/>

<sup>4</sup> The validity of a document can be verified here: <https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/>

<sup>5</sup> EL riikide dokumentide ehtsust on võimalik kontrollida siin: <https://www.consilium.europa.eu/prado/en/search-by-document-country.html>

<sup>5</sup> The authenticity of the documents of EU Member States can be verified here: <https://www.consilium.europa.eu/prado/en/search-by-document-country.html>

<sup>6</sup> <https://www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf>

viiakse läbi reaalajas. Video intervjuu viib läbi Aqdigital või Äriühingu tehingupartner, kellega on sõlmitud selleks vastav leping. Kõik videointervjuu käigus saadud andmeid säilitatakse selliselt, et neid oleks võimalik taas esitada.

Video intervjuu raames Personal küsib järgmist:

1. Ees- ja perekonnanimi;
2. Kodakondsus;
3. Elukoha aadress;
4. Residentsuse riik;
5. Sünniaeg;
6. Kliendi unikaalne personaalne ID-kood (tegemist on unikaalse koodiga, mis genereeritakse iga kliendi jaoks verifitseerimise protseduuri läbimisel. Tänu sellele Äriühing saab veenduda, et video intervjuu läbib seesama isik, kes on läbinud ka algselt verifitseerimist);
7. Registreerimise eesmärk Äriühingu platvormil;
8. Muud küsimused vastavalt vajadusele (kahtluste elimineerimiseks).

Kui video intervjuu katkeb või on poolik, siis Klient peab uuesti läbima video intervjuu edukaks verifitseerimise läbimiseks. Video intervjuu viiakse läbi pärast seda, kui isik on juba edukalt läbinud:

- esmase isikusamasuse kontrolli (isikuttõendava dokumendi, selfie ja liveness kontrolli abil)
- riikliku taustaga isiku ja sanktsioonide nimekirja kontroll (PEP and sanctions check)
- dokumendi ehtsuse kontrolli

Kui Kliendi isikusamasuse tuvastamine ei õnnestu infotehnoloogiliste vahendite abil või tekkis kahtlus Kliendi poolt esitatud andmete õigsuses, siis tuleb tuvastada Kliendi isikusamasus vahetult kohtumisel ning kui see ei ole võimalik, keelduda tehingu tegemisest/ärisuhte loomisest.

Kui kliendile edastakse ankeet (lisa 2), siis füüsiline isik või juriidilise isiku seaduslik esindaja kinnitab ärisuhte loomisest ja/või tehingu juhuti tegemisel, et:

1) ta on nõus läbiviidavate protseduuride käigus isikuandmete töötlemisega ja nende salvestamisega;

2) ta sooritab identifikatsiooniseerimise protseduurid isiklikult;

3) täidetud ankeetküsitluse andmed on õiged ja täielikud ning ta on teadlik tagajärgedest, mis kaasnevad ärisuhte loomisest väära, eksitava või puuduliku teabe esitamisega;

Kui tegemist on välismaa kodanikuga või E-residendi digitaalset isikutunnistust kasutava füüsilise isiku või juriidilise isiku seadusliku esindajaga, on isik kohustatud nõustuma Eesti õiguskorralduse kohaldamisega;

The validity of the documents of EU Member States can be checked with the help of the manual created by the PRADO register. The manual contains information on every country and the channels and websites through which the validity of the documents can be checked.<sup>7</sup>

A video interview is also carried out with a medium-risk and a high-risk customer. The objective of a video interview is to make sure that the person being verified is alive and the same person who filled in the questionnaire and presented their identity document. The interview will be carried out in real time. The video interview will be carried out by Aqdigital or the transaction partner of the Company with whom the respective contract has been entered into. All of the data received in the course of the video interview are recorded in a manner that they can be reproduced.

The Staff asks the following during a video interview:

1. first name and surname;
2. citizenship;
3. address of the place of residence;
4. country of residence;
5. date of birth;
6. the customer's unique personal ID code (this is a unique code generated for each customer in the verification process. This allows the Company to make sure that the video interview is passed by the same person who passed the initial verification);
7. purpose of registration on the Company's platform;
8. other questions as necessary (for elimination of suspicions).

If the video interview is interrupted or is incomplete, the customer must pass the video interview again in order to pass the verification successfully. The video interview will be carried out after the person has already successfully passed the following:

- primary identification with an identity document, selfie and liveness check);
- check of the PEP and sanctions list;
- verification of the authenticity of the document;

If the customer cannot be identified using information technology means or there are doubts about the correctness of the data given by the customer, the customer will need to be identified by way of a face-to-face meeting and, if that is not possible, the transaction or business relationship must be refused.

If a questionnaire (Annex 2) is sent to a customer, a natural person or a legal representative of a legal entity warrants upon establishment of a business relationship and/or making of an occasional transaction that:

1) they consent to the processing and recording of personal data in the course of the procedures



Kõik Kliendi poolt isikusamasuse tuvastamiseks edastatud dokumendid ja andmed salvestatakse selliselt, et neid oleks võimalik taas esitada.

Kujutist ja heli sisaldav infovoog tuleb salvestada koos ajatempliga, kliendi IP-aadressi või personaalse ID-koodiga/numbriga ning kliendi nimega. Kui kliendil puudub personaalse kood, mis on märgitud dokumendil, siis märkida sünniaeg ja –koht ning elukohariik, kusjuures ajatempel peab olema seotud seda puudutavate andmetega sellisel viisil, et iga hilisem andmemuudatus, selle muudatuse tegija, aeg, viis ja põhjus on tuvastatavad.

#### 4.6 Tegelik kasusaaja tuvastamine

**Tegelik kasusaaja** on füüsiline isik, kes teeb oma mõju ära kasutades tehingu või toimingu või omab muul viisil kontrolli tehingu, toimingu või teise isiku üle ja kelle huvides, kasuks või arvel tehing või toiming tehakse.

Äriühingu puhul on tegelik kasusaaja füüsiline isik, kes lõplikult omab või kontrollib juriidilist isikut piisava arvu aktsiate, osade, hääleõiguste või omandiõiguse 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 ühegi füüsilise isiku osalus või tuvastatav kontrolli määr ei ületa 25%, nõutakse informatsiooni nende osanike, aktsionäride, partnerite vm isikute kohta, kellel on juriidilise isiku tegevuse üle kontroll või muu oluline mõju.

carried out;  
2) they perform the identification procedures personally;  
3) the data in the questionnaire are correct and complete and they are aware of the consequences of giving false, misleading or incomplete information upon establishing a business relationship.

A foreign national or a natural person or a legal representative of a legal entity using the digital identity card of an e-resident is required to consent to the application of Estonian legislation.

All documents and data sent by the customer for identification purposes are recorded in a manner that they can be reproduced.

The information flow including the image and the sound must be saved with the timestamp, the customer's IP address or personal ID code/number and the customer's name. If the customer has no personal code indicated on the identity document, their date and place of birth and the country of residence must be noted, and the timestamp must be linked to the data related thereto in a manner that any subsequent change in the data, the person making the change, and the time, manner of and reason for the change can be identified.

#### 4.6 Identification of the beneficial owner

**Beneficial owner** means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.

In the case of companies, a beneficial owner is the natural person who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means.

**Direct ownership** is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

**Indirect ownership** is a manner of exercising control whereby a company that is under the control of a natural person holds or multiple companies that are under the control of the same



Kui isikusamasuse tuvastamisel esitatud dokumentides vm esitatud dokumentidest ei nähtu otseselt, kes on juriidilise isiku tegelik kasusaaja, siis registreeritakse vastavad andmed juriidilise isiku esindaja ütluste või tema kirjalikult esitatud dokumendi alusel.

Personalil on kohustus küsida tegeliku kasusaaja andmed Kliendilt, kui tegemist on juriidilise isikuga. Ütluste või Kliendi poolt kirjaliku dokumendi alusel esitatud andmete õigsust kontrollitakse rakendades mõistlikke meetmeid, sh tehakse päringuid vastavatesse registritesse, nõutakse juriidilise isiku majandusaasta aruanne vm asjakohase dokumendi esitamist. Ütluste või dokumendi aktsepteerimisel teavitab töötaja Klienti vastutusest, mis kaasneb eksitavate või valeandmete esitamisega.

Tegeliku kasusaaja määratlemisel võib abiks kasutada Rahandusministeeriumi juhendi, mis on kättesaadav lingil:

<https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/tegeliku-kasusaaja>

Tegeliku kasusaaja tuvastamiseks tuleb:

- Küsida registrikaardi väljatrukki, kus nähtuks osanike andmed (juriidilise isiku puhul)
- Kontrollida andmete õigsust ja tõe vastavust
- Vajadusel küsida kliendilt ütlusi ja/või täiendavaid dokumente

Nimetatud kohustuse täitmise tulemusel peab Personal teadma, kes on Kliendi tegelik kasusaaja, ja saada aru kliendi või juhuti tehtavas tehingus osaleva isiku omandi- ja kontrollstruktuurist.

Kui Kliendil on omandi- või kontrollstruktuur on keeruline ja või arusaamatu, on see risk suurendavaks asjaoluks. Juhul kui tegeliku kasusaaja tuvastamine ei ole võimalik, ei tohi Personal ärisuhet luua või jätkata.

Andmed tegeliku kasusaaja väljaselgitamiseks tehtud toimingute kohta tuleb salvestada.

natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

Where no natural person holds or identifiably controls more than 25%, information must be requested about the shareholders, partners or other persons who exercise control or other significant influence over the activities of the legal entity.

If the documents submitted upon identification or other documents do not explicitly indicate who the beneficial owner of the legal entity is, the relevant information is registered on the basis of the oral statements made or a written document submitted by the representative of the legal entity.

The staff are obliged to request the data of the beneficial owner from the customer in the case of a legal entity.

The correctness of the submitted data based on the oral statements or the written document of the customer is verified by taking reasonable measures, incl. queries are made to respective registers, the submission of the annual report of the legal entity or the submission of another relevant document is requested. Upon acceptance of the oral statements or the document, the employee informs the customer of the liability arising from giving misleading or false information.

Upon determining the beneficial owner, the instructions given by the Ministry of Finance may be of help. The instructions are available at:

<https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/tegeliku-kasusaaja>

To identify the beneficial owner:

- Ask for a printout of the registry card showing the details of the shareholders (in the case of a legal entity)
- Check the accuracy and veracity of the data
- If necessary, ask the client for testimony and / or additional documents

As a result of fulfilling this obligation, the Staff must know who the actual beneficiary of the Client is and understand the ownership and control structure of the Client or the person participating in the occasional transaction.

If the ownership or control structure of the Client is complex and / or incomprehensible, it is a factor that increases the risk. If it is not possible to identify the beneficial owner, the Staff may not establish or continue a business relationship.

The data of the actions taken to identify the beneficial owner must be recorded.

#### **4.7 Ärisuhte ja tehingu eesmärgi tuvastamine**

Personal teeb kindlaks ärisuhte ja tehingu eesmärgi ja olemuse tuginedes alljärgnevatele andmetele:

- Kliendi poolt ärisuhte loomisel või tehingu teostamisel antud kinnitused;
- Kliendi tegevuseprofili ja tegevusvaldkonna kohta saadud andmed.

Tegevusvaldkonna informatsiooni saamiseks peab klient ankeetküsitluse raames kinnitama, et tema ei tegele riskantse tegevusvaldkonnaga. Juhul kui tehingu eesmärk või ärisuhte loomine on ebamõistlik ja/või ebatavapärane ning Klient ei esita selle kohta veenvat põhjendust, on antud asjaolu tugevdatud hoolsusnõuete täitmise ja kõrgendatud tähelepanu saamise aluseks.

Juhul kui klient on riskantse tegevusvaldkonna esindaja, kuulub ka kõrge riskitaseme klientide hulka ja tema suhtes rakendatakse tugevdatud hoolsusmeetmeid.

Andmed tehingu eesmärgi kohta füüsiliste isikute puhul küsitakse video intervjuu raames Tier 2 ja Tier 3 klientidelt.

Juriidilise isiku puhul küsitakse andmed ärisuhte eesmärgi kohta nii ankeetküsitluse kui ka video intervjuu raames.

#### **4.8 Tunne oma kliendi põhimõtte (KYC) rakendamine**

„Tunne oma klienti” põhimõtte tähendab asjakohase informatsiooni ja andmete kogumine Kliendi kohta, sh lisaks isikusamasuse tuvastamisele ka Kliendi tegevusprofili, tema tegevuse eesmärgi, tegeliku kasusaaja ja vajadusel ka tehingus kasutatavate allikate ja päritolu tuvastamine, mis võimaldavad Äriühingul hinnata, kas Kliendi poolt sooritatud tehingud vastavad tema põhitegevusele ja/või maksetavatele ning otsustada, kas tegemist on tavapärase või kahtlase või ebahariliku tehinguga. Oluline on see, et Aqdigital OÜ kogub täiendavad andmeid selleks, et:

- teada, kes on klient ja milline on tema tavapärane tegevus;
- teada kliendi kehtivad kontaktandmeid, kodakondsuse, residentsuse ja tegevusvaldkonna andmeid;
- Jälgida, et Kliendi tehingud oleksid kooskõlas tema majandustegevuse laadi ja ulatusega.

#### **4.7 Identifying the purpose of a business relationship and transaction**

The Staff identifies the purpose and nature of a business relationship and transaction based on the following data:

- warranties given by the customer upon establishment of the business relationship or making of the transaction;
- data received on the customer's operation profile and field of activity.

In order to obtain information on the area of activity, the customer must confirm within the scope of the questionnaire that they are not engaged in a risk area of activity.

If the purpose of a transaction or the establishment of a business relationship is unreasonable and/or unusual and the customer does not submit a convincing reason for it, this fact serves as the basis for complying with enhanced due diligence measures and paying special attention.

If the customer represents a risky area of activity, they also belong among high-risk customers and enhanced due diligence measures are applied to them.

In the case of natural persons, the data of the objective of a transaction are requested from the Tier 2 and Tier 3 customers within the scope of video interviews.

In the case of legal entities, the data of the purpose of the business relationship are requested in the questionnaire as well as within the scope of video interviews.

#### **4.8 Application of the Know Your Customer (KYC) principle**

The Know Your Customer principle means the gathering of relevant information and data on the customer, including, in addition to identification of the person, the establishment of the customer's operation profile, the purpose of the customer's activities, the beneficial owner of the customer and, where necessary, the sources and origin of the funds used in the transaction, which allow the Company to assess whether the transactions made by the customer correspond to the customer's principal activity and/or payment habits and decide if the transaction is ordinary, suspicious or unusual.

It is important that Aqdigital OÜ collects additional data in order to:

- know who the customer is and what their ordinary activity is;
- know the customer's actual contact details, citizenship, residency and field of activity;
- make certain that the customer's transactions correspond to the nature and

Seejuures on oluline silmas pidada, et „tunne oma klienti“ põhimõtte rakendamise kohaselt ei toimu lisaandmete küsimine ühe 27ues, vaid tegemist on pideva kliendi tundmise ja jälgimisega. Tulenevalt sellest ajakohastab Äriühing oma klientide andmeid järgnevalt:

1. Kõrge riskiga (Tier 3) Klientide puhul vähemalt kaks korda aastas.
2. Keskmise riskiga (Tier 2) Klientide puhul vähemalt ühe 27ues aastas.
3. Madala riskiga (Tier 1) klientide puhul vähemalt üks kord kahe aasta jooksul.

Selleks edastab Äriühing oma kliendile täitmiseks ankeedi/küsitluse, et veenduda andmete õiguses ja kehtivuses.

„Tunne oma klienti“ põhimõtte kohaldamiseks tuleb Personalil:

- rakendada meetmeid Kliendi tegevusvaldkonna ja tegevusprofiili väljaselgitamiseks, sh
- ärisuhte loomisel või tehingu tegemisel Kliendi käest andmete küsimine;
- avalike andmebaaside ja registrite kontroll (nt MTR, MTA, Äriregister jne.);
- juhul, kui vastutaval töötajal on madala riskiastmega tehinguga seoses tekkinud rahapesu või terrorismi rahastamise kahtlus, tuleb kohaldada tugevdatud hoolsusmeetmed.

Tunne oma klienti põhimõtte rakendamine toimub läbi selle, et kliendile edastatakse ankeet täiendavate andmete kogumiseks ja seejärel analüüsitakse esitatud andmeid. Sealhulgas hindab Äriühing kliendi tegevuse muutumist ja seda, kas sellise muutumisega võib tõusta riskiaste, mistõttu on vajalik kohaldada täiendavaid hoolsusmeetmeid.

KYC põhimõtte rakendamine ja selle tehniline teostus on kirjeldatud eraldi dokumendis „Description of technology measures and systems for KYC and KYT AQDigital OÜ“.

#### **4.9 Tunne oma tehingu (KYT) ja travel rule põhimõtte rakendamine**

Tunne oma tehingu (KYT) põhimõtte rakendamiseks kasutab äriühing usaldusväärse partneri AML Corporation Limited (edaspidi ka AMLBot või KYT partner). KYT partneri teenuseid kasutatakse selleks, et monitoorida ja analüüsida ploki ahela tehinguid ning välja selgitada ja ennetada tehingute toimumist e-rahakottidega, mis

scope of the customer's economic activities.

Thereby it is important to keep in mind that, according to the Know Your Customer principle, additional information is requested not once, but it is a constant process of knowing and monitoring the customer. Therefore, the Company updates the data of its customers as follows:

1. in the case of high-risk (Tier 3) customers, at least twice a year;
2. in the case of medium-risk (Tier 2) customers, at least once a year;
3. in the case of low-risk (Tier 1) customers, at least once every two years.

To that end, the Company sends a questionnaire to its customers in order to make certain that the data are correct and valid.

To apply the Know Your Customer principle, the Staff must:

- apply measures to identify the customer's field of activity and operation profile, incl.
- ask data from the customer upon establishment of a business relationship or making a transaction;
- check public databases and registers (e.g. the register of economic activities, the Tax and Customs Board, the commercial register, etc.);
- if the employee in charge suspects the customer of money laundering or terrorist financing in connection with a low-risk transaction, enhanced due diligence measures must be applied.

The Know Your Customer principle is applied by sending the customer a questionnaire for collecting additional data and thereafter the submitted data are analysed. Among others, the Company assesses the changes in the customer's activities and whether the changes may raise the risk level so that additional due diligence measures need to be taken.

The implementation of the KYC principle and its technical implementation are described in a separate document „Description of technology measures and systems for KYC and KYT AQDigital OÜ“.

#### **4.9 Know your transaction (KYT) and travel rule principles**

To implement the Know Your Transaction (KYT) principle, the Company uses a trusted partner, AML Corporation Limited (hereinafter also AMLBot or KYT Partner). The services of a KYT partner are used to monitor and analyze block chain transactions and to detect and prevent transactions with e-wallets related to money

on seotud rahapesu, terrorismi rahastamise või finantspettustega. Kõik kontrolli käigus saadud andmed salvestatakse selliselt, et neid oleks võimalik taas esitada.

AMLBot kasutab Crystal andmebaasi (veebisait on <https://crystalblockchain.com/>) ja oma sisemisi andmebaase, mida AML-ametnikud värskendavad klientide tehingute põhjal.

KYT raames AMLBot analüüsib, kas esineb järgmine riskifaktor:

- Hasartmängud
- Ebaseaduslik teenus
- Miner
- Mixer teenus
- Interneti 28uestionnai
- Interneti-rahakott (wallet)
- Muu
- P2P-vahetusplatvorm kõrge ML-riskiga
- P2P-vahetusplatvorm Madala ML-riskiga
- Makse töötleja (payment processor)
- Lunaraha
- Pettus
- Varastatud mündid
- Pangaautomaat
- Darkneti turg
- Darkneti teenus
- Vahetada kõrge müügiriskiga
- Vahetada madala müügiriskiga
- Vahetada mõõduka müügiriskiga
- Vahetada väga kõrge müügiriskiga
- Petturlik vahetus

Iga tehing nii sissetulev kui väljaminev, kontrollitakse AMLBot kaudu.

Tulenevalt eelnimetatud riskifaktoritest ja analüüsi tulemusena kujuneb tehingu riskiskooring. Kui analüüsi tulemusena selgub, et esineb kahtlus rahapesus või terrorismirahastamises, siis tuleb Personalil kaaluda teate esitamist ja lähtuda peatükis 7 kirjeldatust.

Lisaks eeltoodule AMLbot pakub teenust ka seoses travel rule reeglite täitmisega. *Travel rule* tähendab, et Äriühing kui teenuse pakkuja peaks koguma nii tehingu algataja kui ka saaja andmed.

**Tehingu algataja** osas tuleb koguda järgmised andmed:

1. Füüsilise isiku puhul

nimi, tehingu kordumatu tunnus, maksekonto või virtuaalvääringu rahakoti identifikaator, isikut tõendava dokumendi nimetus ja number ning isikukood või sünniaeg, sünnikoht ja elukoht

laundering, terrorist financing or financial fraud. All data obtained during the inspection shall be recorded in such a way that they can be re-submitted.

AMLBot uses the Crystal database (the website is <https://crystalblockchain.com/>), as well as its internal databases, which AML officers update based on clients' transactions.

Under KYT, AMLBot analyzes whether the following risk factor exists:

- Gambling
- Illegal service
- Miner
- Mixer service
- Internet marketplace
- Wallet
- Sell
- P2P exchange platform with high ML risk
- P2P exchange platform with low ML risk
- Payment processor
- Redemption
- Fraud
- Stolen coins
- ATM
- Darknet Market
- Darknet service
- Exchange with high sales risk
- Exchange with low sales risk
- Exchange with moderate sales risk
- Exchange with a very high sales risk
- Fraudulent exchange

All transactions, incoming and outgoing, are verified by AMLBot.

Due to the before mentioned risk factors and according to the analyze, the risk score of the transaction is formed. If the transaction from the analysis is found to be suspected of money laundering or terrorist financing, the Staff should consider making a report and follow the instructions in Chapter 7.

In addition to the above, AMLbot also offers a service related to compliance with travel rules. The travel rule means that the company, as a service provider, should collect the data of both the originator and the recipient of the transaction.

The following data must be collected for **the originator of the transaction**:

1. In the case of a natural person

Name, unique identifier of the transaction, identifier of the payment account or virtual currency wallet, name and number of the identity document and personal identification code or date

address;

2. Juriidilise isiku puhul nimi, tehingu kordumatu tunnus, maksekonto või virtuaalvääringu rahakoti identifikaator, registrikood, selle puudumise korral asukohariigi asjakohane identifitseerimistunnus (registreerimisnumbriga võrdsustatav numbri- või tähekombinatsioon) ja asukoha aadress.

**Tehingu saaja** kohta tuleb koguda järgmised andmed:

tehingu kordumatu tunnuse andmed ning maksekonto või virtuaalvääringu rahakoti identifikaatori andmed juhul, kui maksekonto või virtuaalvääringu rahakoti identifikaatori andmeid kasutatakse tehingu tegemiseks.

Kui andmed on kogutud ja Äriühingu klient on tehingu algata, siis kogutud andmed tuleb edastada tehingu saaja teenuse osutajale viivitamatult ja turvaliselt. Kui see ei ole võimalik, siis tuleb kasutada tehingute reaajas jälgimise, mida teostab AMLBot ehk KYT või plokiahela analüütikat.

KYT põhimõtte rakendamine ja tehniline teostus on kirjeldatud eraldi dokumendis „Description of technology measures and systems for KYC and KYT AQDigital OÜ“.

#### 4.10 Ärisuhte jälgimine

Aqdigital OÜ juhatuse poolt määratud Personali liige kohustub regulaarselt kliendiga ärisuhte jälgima, kindlustamaks, et teostatavad tehingud vastavad tema riskiprofiilile.

Selleks kohustub Personali liige:

- jälgima tehingus kasutatavate rahasummade suurust ning tehingute sagedust ning vajadusel välja selgitama ärisuhtes ja/või tehingutes kasutava vara päritolu;
- kontrollima kliendi juriidilist staatust (õigusvõime olemasolu), vajadusel finantsolukorda ja tegevusala;
- kontrollima omandikuuluvust puuduvat informatsiooni (tegelikke kasusaajaid).

Tuleneval eeltoodust tuleb Personalil vähemalt kord kahe aasta jooksul madala riskiprofiiliga

of birth, place of residence and address of residence;

2. In the case of a legal person the name, the unique identifier of the transaction, the identifier of the payment account or virtual currency wallet, the registry code, the relevant identification of the country of its proper location (a combination of numbers or letters equivalent to the registration number) and the address of the location.

The following information must be collected about the **recipient of the transaction**:

the data of the unique identifier of the transaction and the data of the identifier of the payment account or virtual currency wallet if the data of the identification account of the payment account or virtual currency wallet is used for the execution of the transaction.

Once the data has been collected and the Company's customer has initiated the transaction, the collected data must be transmitted to the service provider of the recipient of the transaction immediately and securely. If this is not possible, real-time transaction monitoring by AMLBot or KYT or blockchain analytics must be used.

The implementation and technical implementation of the KYT principle is described in a separate document "Description of technology measures and systems for KYC and KYT AQDigital OÜ".

#### 4.10 Monitoring a business relationship

A Staff member appointed by the Management Board of AQdigital OÜ undertakes to regularly monitor the business relationship with the customer in order to ensure that the transactions to be made correspond to the customer's risk profile.

To that end, the Staff member undertakes to:

- monitor the size of the sums used in transactions and the frequency of transactions and, where necessary, identify the origin of the assets used in the business relationship and/or the transactions;
- check the customer's legal status (existence of the passive legal capacity), financial situation and the field of activity, where necessary;
- verify ownership information (beneficial owners).

In view of the above, the Staff must, at least once in two years in respect of customers with a low risk profile (Tier 1), at least once a year in respect of customers with a medium risk profile (Tier 2)

kliendi (Tier 1), vähemalt kord aastas keskmise riskiprofiiliga (Tier 2) ning vähemalt kaks korda aastas kõrge (Tier 3) riskiprofiiliga kliendi puhul edastada kliendile täitmiseks ankeedi ja seejärel:

- a) kontrollida, kas kliendi andmed on muutunud seoses kliendiriskiga;
- b) kontrollida, kas kliendi andmed on muutunud seoses geograafilise riskiga;
- c) kontrollida, kas kliendi andmed on muutunud seoses tegevusala riskiga;
- d) määrata/uuendada riskiprofiil.

Ärisuhte pideva seire käigus Äriühing rakendab järgmiseid meetmeid:

- skriinimine ehk klientide ja tehingute reaajas jälgimine;
- monitoorimine ehk klientide ja tehingute hilisem analüüs;

**Skriinimise** eesmärgiks on tuvastada:

- kahtlaseid ja ebaharilikke tehinguid ning tehingumustreid;
- etteantud piirmäärasid ületavaid tehinguid;
- riikliku taustaga isikuid ja rahvusvahelisi sanktsiooniga seotud asjaolusid.

Äriühing kasutab skriinimiseks ehk reaajas tehingute jälgimiseks automaatse süsteemi, mille parameetrid/stsenaariumid, kontrollivad (AML watchlisti):

1. Kas kliendi staatus seose PEP isikuga ei ole muutunud;
2. Kas isikust ei ole saanud rahvusvahelise sanktsiooni subjekt;
3. Kas isiku kohta ei ole avaldatud negatiivset informatsiooni meedias.

Eelnimetatud kontrolli (edaspidi *ongoing AML 30questionnai*) tehakse igapäevaselt.

Lisaks eeltoodule rakendatakse ka tehingute järgimiseks plokiahela analüütikat. Eelnimetatud teenust (KYT) osutab äriühingule AML Corporation Limited<sup>7</sup> (edaspidi AMLBot).

**Monitoorimise** eesmärgiks on tuvastada tehinguid ja asjaolusid, mida ei olnud võimalik tuvastada reaajas (neisse ei olnud võimalik sekkuda) või mis tehingu iseloomust tulenevalt ei kajastanud reaajas tehingute jälgimise parameetrites IT- lahendi puhul või toimingutes manuaalse jälgimise puhul (näiteks suuremad tehingud summade, valuutade või klienditüüpide kaupa) ja kontrollida, kas midagi on muutunud seoses esialgsete andmetega kliendi või tehingute kohta.

Äriühing pöörab kõrgendatud tähelepanu ehk kohaldab tugevdatud hoolsusmeetmeid keerukatele, suure väärtusega ja ebatavalistele tehingutele ja tehingumustritele, millel ei ole

and at least twice a year in respect of customers with a high risk profile (Tier 3), send a questionnaire to the customer for filling in and, thereafter:

- a) verify whether the customer's risk data have changed;
- b) verify whether the customer's geographic risk data have changed;
- c) verify whether the customer's field of activity risk data have changed;
- d) set/update the customer's risk profile.

The Company monitoring of the business relationship on an ongoing basis shall take the following measures:

- screening, ie real-time monitoring of customers and transactions;
- monitoring, ie subsequent analysis of customers and transactions;

The purpose of **screening** is to identify:

- suspicious and unusual transactions and transaction patterns;
- transactions exceeding the specified limits;
- Persons with a national background and international circumstances related to the sanction.

The company uses an automated system for screening or real-time transaction monitoring, the parameters / scenarios of which check (AML watchlist):

1. Has the client's status in relation to the PEP person have changed;
2. Has the person not become the subject of an international sanction;
3. Has no negative information about the person been published in the media.

The aforementioned inspection (hereinafter ongoing AML monitoring) is performed on a daily basis.

In addition to the above, block chain analytics is also used to track transactions. The aforesaid service (KYT) is provided by AML Corporation Limited ("AMLBot").

The purpose of **monitoring** is to identify transactions and circumstances that could not be identified in real time (could not be interfered with) or that, due to the nature of the transaction, did not reflect real-time transaction tracking parameters in the IT solution or manual tracking by item) and check if anything has changed due to initial customer or transaction data.

The Company pays close attention to enhanced due diligence measures for complex, high-value and unusual transactions and transaction patterns that do not have a reasonable or apparent

<sup>7</sup> Rohkem informatsiooni AMLBot kohta kodulehele: <https://amlbot.com>

mõistlikku või nähtavat majanduslikku või õiguspärast eesmärki või mis ei ole konkreetse ärispetsiifika jaoks iseloomulik.

Lisaks tugevdatud hoolsusmeetmete kohaldamisele tuleb iga kahtlust tekitava tehingu tausta uurida nii palju, kui see on mõistlikult vajalik, sh tuleb fikseerida tehingu üksikasjad ning ilmnenud asjaolusid analüüsida, eesmärgiga selgitada välja sagedamini esinevate tehingute tüüpilisemaid tunnuseid. Need andmed tuleb säilitada. Seejuures peamised asjaolud, millele tuleb selliste tehingute analüüsimisel tähelepanu pöörata, on järgmised:

- milline on kahtlustäratav asjaolu toimingute, tehingute või muude asjaolude juures;
- kas Äriühing on veendunud, et tunneb klienti vajalikul määral ja kas klienti tegevus vastab tema kohta eelnevalt teadaolevale informatsioonile või on tema kohta vaja koguda lisaandmeid ning võtta mõistlike ja piisavaid meetmeid, et mõista tehingu tausta ja eesmärki, näiteks selgitades välja rahaliste vahendite allika ja sihtkoha või otsides rohkem teavet klienti tegevuse kohta, et teha kindlaks sellise tehingu tõesus;
- kas on esinenud korduvaid kahtlaste toimingute ja tehingute ilminguid (sh sarnaste olukordade või asjaolude osas);
- kas klienti tegevusele ja ärisuhtele üldiselt on vajalik pöörata edaspidi suuremat tähelepanu, sh üksikasjadele;
- kas on vajalik täita rahapesu andmebüroole teatamiskohustust.

Ärisuhte käigus tuvastab Personal vajadusel tehingus kasutatud vahendite allika ja päritolu.

Tehingus kasutatud vahendite allika ja päritolu kohta küsimine on sisuliselt võrdväärne ärisuhte pideva seirega, selle erisusega, et kui ärisuhte pidev seire katab kogu klienti ärisuhet ning selle elutsükli, siis tehingus kasutatud vahendite allikas ja päritolu eesmärk seondub pelgalt sissetulevate tehingutega. Eesmärk on siiski sama, saada klientist piisav ülevaade ning teada, kas see vastab klienti kohta eelnevalt teadaolevale informatsioonile.

**Tehingus kasutatud vahendite allikaks** on põhjus, selgitus ja alus (õigussuhe ja selle sisu), millisel põhjusel rahalisi vahendeid kanti.

**Tehingus kasutatud vahendite päritolu** mõiste sisuks on tegevus, mille abil rahalised vahendid teeniti või saadi ning on lähedasem rikkuse allika ja/või päritolu tuvastamisele.

Tehingus kasutatud vahendite allikas ja päritolu tuleb tuvastada vajadusel. Vajadus vahendite allikat ja päritolu tuvastada sõltub nii klienti eelnevast tegevusest kui ka muust teadaolevast

economic or legitimate purpose or are not specific to a particular business.

In addition to the application of enhanced due diligence measures, the background to each suspicious transaction should be investigated to the extent reasonably necessary, including the details of the transaction and the analysis of the circumstances in order to identify the most common features of more frequent transactions. These records must be kept. The main factors to consider in analyzing such transactions are:

- What is the suspicious circumstance of the acts, transactions or other circumstances;
- Whether the Company is satisfied that it knows the customer to the required extent and that the customer's activities correspond to previously known information about the customer or need to collect additional information and take reasonable and sufficient steps to understand the background and purpose of the transaction, such as the source and destination of funds. or seeking more information about a customer's actions to determine the veracity of such a transaction;
- Whether there have been repeated instances of suspicious activity and transactions (including similar situations or circumstances);
- whether it is necessary to pay more attention to the client's activities and business relationship in general in the future, including details;
- whether it is necessary to comply with the obligation to notify the FIU.

In the course of the business relationship, the Staff shall, if necessary, identify the source and origin of the funds used in the transaction. Asking about the source and origin of the funds used in a transaction is essentially equivalent to continuous monitoring of the business relationship, with the difference that while continuous monitoring of the business relationship covers the customer's business relationship and life cycle, the source and origin of the funds used in the transaction are merely incoming transactions. However, the aim is the same, to get a sufficient overview of the customer and to know whether it corresponds to previously known information about the customer.

**The source of the funds** used in the transaction is the reason, explanation and basis (legal relationship and its content) for which the funds were transferred.

**The concept of the origin of the funds** used in a transaction refers to the activity by which the funds were earned or received and is closer to identifying the source and / or origin of the wealth. The source and origin of the funds used in the transaction must be identified, if applicable. The need to identify the source and origin of funds depends on the client's previous activities as well



informatsioonist. Seejuures suureneb vajadus vahendite allika ja päritolu tuvastamiseks:

- proportsionaalselt rahaliste vahendite suurusega;
- kui tehingud ei vasta kliendi kohta eelnevalt teadaolevale informatsioonile;
- kui kohustatud isik soovib või peaks mõistlikult pidama vajalikuks hinnata, kas tehingud vastavad kliendi kohta eelnevalt teadaolevale informatsioonile;
- kui kohustatud isikul tekib kahtlus, et tehingud viitavad kuritegelikule tegevusele, rahapesule või terrorismi rahastamisele või mille seotus rahapesu või terrorismi rahastamisega on tõenäoline, sh keerukatele, suure väärtusega ja ebatavalistele tehingutele ja tehingumustritele, millel ei ole mõistlikku või nähtavat majanduslikku või õiguspärast eesmärki või mis ei ole konkreetse ärispetsiifika jaoks iseloomulik.
- Päritolu on laiem ning sisaldab tegevust, mille abil rahalised vahendid teeniti või saadi ning on lähedasem rikkuse allika ja/või päritolu tuvastamisele.

Tehingus kasutatud vara päritolu tuleb alati välja selgitada kui:

1. Tegemist on 2 või 3 riskitaseme Kliendiga (Tier 2 või Tier 3);
2. Kliendi varalist seisut arvestades ei ole tõenäoline, et klient on tehinguks olevad vahendid teeninud legaalselt.

#### 4.11 Lihtsustatud hoolsusmeetmed

Personal võib kohaldada Kliendi suhtes hoolsusmeetmeid rahapesu või terrorismi rahastamise väikse riski korral lihtsustatud korras, kui Kliendi riskiprofiil on madal ning riskiprofiili määramise otsuses on tuvastatud, et selliste asjaolude korral on tegemist tavapärasest madalama rahapesu või terrorismi rahastamise olukorraga. Äriühing kohaldab lihtsustatud hoolsusmeetmeid Tier 1 riskikategooria klientide suhtes.

Lihtsustatud hoolsusmeetmete rakendamise alusel on Personali hinnang Kliendi riskifaktorite esinemise kohta ja vastav otsus riskiprofiili kohta või muud moodi selle fikseerimine (lisa 1).

Aqdigital OÜ kohaldab hoolsusmeetmeid lihtsustatud korras üksnes ulatuses, milles on tagatud tehingute ja ärisuhete piisav jälgimine, et oleks võimalik tuvastada ebatavalised tehingud ning võimaldada kahtlastest tehingutest teatamine.

as other known information. At the same time, the need to identify the source and origin of funds is increasing:

- in proportion to the amount of funds;
- if the transactions do not correspond to the previously known information about the client;
- if the obligated person wishes or should reasonably consider it necessary to assess whether the transactions correspond to previously known information about the client;
- where the obligated person suspects that the transactions involve or are likely to involve money laundering or terrorist financing, including complex, high-value and unusual transactions and transaction patterns that do not have a reasonable or apparent economic or legitimate purpose; or is not specific to a particular business.
- The origin is broader and includes the activities by which the funds were earned or received and is closer to identifying the source and / or origin of wealth.

The origin of the assets used in the transaction must always be ascertained if:

1. It is a Client with 2 or 3 risk levels (Tier 2 or Tier 3);
2. Given the client's financial situation, it is unlikely that the client has legally earned the funds available for the transaction.

#### 4.11 Simplified due diligence measures

The Staff may apply simplified due diligence measures to a customer in the event of a low risk of money laundering or terrorist financing if the customer's risk profile is low and the risk profile determination decision specifies that such factors amount to a lower-than-usual risk of money laundering or terrorist financing. The Company applies simplified due diligence measures to customers of Tier 1 risk category.

The basis for the application of simplified due diligence measures is the Staff's estimate of the existence of the customer's risk factors and a respective decision on the risk profile, or the recording of this in any other manner (Annex 1).

AQdigital OÜ applies simplified due diligence measures only to the extent that the sufficient monitoring of transactions, acts and business relationships is ensured, so that it would be possible to identify unusual transactions and allow for reporting of suspicious transactions.

Upon application of the due diligence measures specified in clauses 4.2, 4.3 and 4.4 of the Guidelines by way of the simplified procedure, the identity of a customer or of the customer's representative may be verified on the basis of information obtained from a credible and independent source at the time of establishment of



Juhendi punktides 4.2, 4.3. ja 4.4. hoolsusmeetmete rakendamisel lihtsustatud korras võib Kliendi ja tema esindaja isikusamasust kontrollida usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal ärisuhte loomise ajal, kui seda on vaja, et äritegevuse tavapärasest käiku mitte häirida.

Ärisuhte pidavat jälgimist saab lihtsustatud korras teha, kui on tuvastatud väiksemat riski iseloomustav asjaolu ning kui on täidetud vähemalt järgmised tingimused:

- Kliendiga on sõlmitud kirjalikus, elektroonilises või kirjalikku taasesitamist võimaldavas vormis kestvusleping;
- Kliendi poolt ärisuhte raames tasutud maksed laekuvad ainult arvelduskonto kaudu või pangakaardi kaudu;
- ärisuhtes tehtavate tehingute sissetulevate või väljaminevate maksete koguväärtus kuus ei ületa 15 000 eurot;
- ärisuhtes tehtavate tehingute sissetulevate või väljaminevate maksete koguväärtus aastas ei ületa 15 000 eurot;
- Kliendi tegeliku kasusaaja andmed on avalikult kättesaadavad ja kontrollitavad;
- Klient on resident või on pärit Euroopa Majanduspiirkonna riigist;
- Klient on Euroopa Majanduspiirkonna riigi kodanik;
- Klient ei ole PEP ega sanktsioonide/embargo nimekirjas;
- Kliendi tegevusvaldkond ei ole riskantne.

Juhul kui Personalil tekib kas ärisuhte loomisel, tehingu tegemisel või ärisuhte seire korral kahtlus rahapesu või terrorismi rahastamises, ei tohi rakendada Kliendi suhtes lihtsustatud hoolsusmeetmeid vaatamata sellele, et ta kuulub madala riskiprofiiliga kliendigruppi mingite kriteeriumite alusel.

Kui kliendi riskiprofiil on madal ja klient kuulub **Tier 1 riskiprofiili gruppi**, siis kliendi suhtes rakendatakse lihtsustatud hoolsusmeetmeid ja palutakse esitada järgmised andmed:

1. Täidetud kliendi andkeet (lisa 2)<sup>8</sup>;
2. Isikuttõendava dokumendi koopia edastamine;
3. Näopildi (selfie) edastamine;
4. Näopildi (selfie) edastamine koos dokumendi ja paberiga, milles on märgitud näopildi tegemise kuupäev;

the business relationship, provided that it is necessary for not disturbing the ordinary course of business.

The constant monitoring of a business relationship can be done by way of the simplified procedure, provided that a factor characterising a lower risk has been established and at least the following criteria are met:

- a long-term contract has been entered into with the customer in writing, electronically or in a form reproducible in writing;
- the payments made by the customer within the scope of the business relationship are received only through a current account or a bankcard;
- the total value of incoming and outgoing payments in transactions made in the business relationship does not exceed 15,000 euros per month;
- the total value of incoming and outgoing payments in transactions made in the business relationship does not exceed 15,000 euros per year;
- the data of the beneficial owner of the customer are publicly available and can be verified;
- the customer is a resident or originally from a member state of the European Economic Area;
- the customer is a citizen of a member state of the European Economic Area;
- the customer is not a PEP or entered in the list of sanctions/embargo;
- the customer's area of activity of the customer is not high-risk.

If the Staff has any suspicion of money laundering or terrorist financing upon establishing a business relationship, making a transaction or monitoring a business relationship, simplified due diligence measures cannot be applied to the customer even though the customer belongs to a customer group with a low risk profile based on certain criteria.

If the customer's risk profile is low and the customer is included in the **Tier 1 risk profile group**, simplified due diligence measures are applied to the customer and the following data are requested from the customer:

1. Completed customer questionnaire (Annex 2)<sup>8</sup>;
2. sending a copy of the identity document;
3. sending a facial image (selfie);

<sup>8</sup> FOR the individuals: name, surname, citizenship, residential address, place of birth, date of birth 18+, e-mail, consent of non participation of suspicion professions; FOR the company: Name, registry code, address, place of establishment (country), e-mail, business field, data about member of the board or other company representative person (the same as for individuals), purpose of use of the account

5. Video verifitseerimise täiendava kontrolli läbimine (liveness check);
6. Juriidilise isiku puhul äriregistri väljavõte (kui andmed on avalikud, siis Personal ise kogub neid, kui andmed ei ole avalikud, küsitakse kliendi käest);
7. Juriidilise isiku puhul andmed tegeliku kasusaaja kohta;
8. Kui tekib kahtlus, siis tõend vara päritolu kohta  
Juhul kui tekkib kahtlus kliendi vara päritolu kohta, on Personalil õigus küsida vara päritolu tõendavat dokumendi. Selliseks tõendiks võib olla näiteks: laenuleping, vara müügileping, kindlustusleping, pärandvara saamise tõend, maksudeklaratsioon vms. Kui tegemist on välismaise dokumendiga, mis ei ole koostatud eesti, 34uestio või vene keeles, see peab olema tõlgitud, et Personal saaks veenduda lepingu sisus. Lepingu puhul kindlasti jälgida, et see oleks allkirjastatud ja kehtiv. Rahaliste vahendite tõendiks võib alternatiivina lugeda viimase kolme kuu väljavõtte krediitiasutusest
9. Kontroll, kas Klient on riikliku taustaga isik (PEP) või tema abikaasa;
10. Kontroll, kas klient on finantssanktsioonide (Euroopa Liit, FATF, United Nations) või embargo nimekirjas.

#### 4.12 Tugevdatud hoolsusmeetmed

Aqdigital OÜ kohaldab hoolsusmeetmeid tugevdatud korras, et asjakohaselt juhtida ja maandada tavapärasest kõrgemat rahapesu ja terrorismi rahastamise riski. Tugevdatud hoolsusmeetmed kohaldatakse Tier 2 ja Tier 3 klientide suhtes.

4. sending a facial image (selfie) with a document and paper on which the date when the selfie was taken is indicated;
5. passing the additional check of video verification (liveness check);
6. in the event of a legal entity, extract from the commercial register (if the data are public, the Staff collects the data on their own, if the data are not public, the data are requested from the customer);
7. data of the beneficial owner in the case of a legal entity;
8. proof of the origin of assets in the case suspicions;  
the Staff has the right to request a document that proves the origin of assets if suspicions arise about the origin of the customer's assets. Such proof may include, for instance, a loan contract, contract of sale of property, insurance contract, certificate of receipt of estate, income declaration, etc. In the event of a foreign document not prepared in Estonian, English or Russian, the document must be translated to enable the Staff to examine the substance of the contract. In the event of a contract, it must be made sure that the contract is signed and valid. As an alternative, a statement from a credit institution for the last three months may be considered proof of funds.
9. a check of whether the Customer is a politically exposed person (PEP) or their spouse;
10. a check of whether the customer is in a list of financial sanctions (European Union, FATF, United Nations) or embargo.

#### 4.12 Enhanced due diligence measures

AQdigital OÜ applies enhanced due diligence measures in order to adequately manage and mitigate a higher-than-usual risk of money laundering and terrorist financing. Enhanced due diligence measures are applied to Tier 2 and Tier 3 customers.

**In the event of a medium-risk (Tier 2) customer,** the company applies enhanced due diligence measures and requests the following data:

1. completed customer questionnaire (Annex 2);
2. sending a copy of the identity document;
3. sending a facial image (selfie);
4. sending a facial image (selfie) with a document and paper on which the date when the selfie was taken is indicated;
5. passing the liveness check (video verification);
6. passing the online video interview;

**Kui klient on keskmise riskiga Tier 2**, rakendab äriühing tugevdatud hoolsusmeetmed ja küsib järgmised andmed:

1. Täidetud kliendi andkeet (lisa 2);
2. Isikuttõendava dokumendi koopia edastamine;
3. Näopildi (*selfie*) edastamine;
4. Näopildi (*selfie*) edastamine koos dokumendi ja paberiga, milles on märgitud näopildi tegemise kuupäev;
5. Liveness kontrolli läbimine (video verifitseerimine);
6. Online videointervjuu läbiviimine;  
Online videointervjuu raames on Personal eesmärgiks tuvastada isik, veenduda isikut tõendava dokumendi usaldusväärsuses ja koguda täiendavat teavet tehingu eesmärgi, tegevusala kohta, selleks et maandada rahapesu ja terrorismi rahastamise ohtu.
7. Juriidilise isiku puhul äriregistri väljavõte (kui andmed on avalikud, siis Personal ise kogub neid, kui andmed ei ole avalikud, küsitakse kliendi käest);
8. Elukoha tõendi esitamine (*proof of residential address*)  
Kui Klient elu või asukoht on riigis, kus on olemas keskne sissekirjutuse süsteem, siis tõend sissekirjutuse kohta. Kui selline sissekirjutuse keskne register puudub, siis kolme kuu kommunaalarved, mis ei tohi olla vanem kui 3 kuud VÕI alternatiivina viimase kolme kuu pangakonto väljavõte, millel on märgitud Kliendi aadress;
9. Rahaliste vahendite tõend (*proof of funds*)  
Klient peab esitama tõendi, mis kinnitab ja tõestab tehingu jaoks saadud rahaliste vahendite päritolu. Selliseks tõendiks võib olla näiteks: laenuleping, vara müügileping, kindlustusleping, pärandvara saamise tõend, maksudeklaratsioon vms. Kui tegemist on välismaise dokumendiga, mis ei ole koostatud eesti, 35uestio või vene keeles, see peab olema tõlgitud, et Personal saaks veenduda lepingu sisus. Lepingu puhul kindlasti jälgida, et see oleks allkirjastatud ja kehtiv. Rahaliste vahendite tõendiks võib alternatiivina lugeda viimase kolme kuu väljavõtte krediidasutusest;
10. Kontroll, kas Klient on riikliku taustaga isik (PEP) või tema abikaasa;
11. Kontroll, kas klient on finantssanktsioonide (Euroopa Liit, FATF, United Nations) või embargo nimekirjas;
12. Tõend või andmed tegeliku kasusaaja kohta;

during the online video interview, the purpose of the Staff is to identify the person, make sure that the identity document is credible and gather additional information about the purpose of the transaction and field of activity in order to mitigate the risk of money laundering and terrorist financing;

7. in the event of a legal entity, extract from the commercial register (if the data are public, the Staff collects the data on their own, if the data are not public, the data are requested from the customer);
8. submission of proof of residential address. A certificate of enrolment if the customer's place of residence or location is in a country that has a central enrolment system. Utility bills for three months that may not be older than three months OR, as an alternative, bank account statement for the last three months that bears the customer's address if there is no such central enrolment system;
9. proof of funds.  
The customer must submit a certificate that confirms and proves the origin of funds obtained for the transaction. Such proof may include, for instance, a loan contract, contract of sale of property, insurance contract, certificate of receipt of estate, income declaration, etc. In the event of a foreign document not prepared in Estonian, English or Russian, the document must be translated to enable the Staff to examine the substance of the contract. In the event of a contract, it must be made sure that the contract is signed and valid. As an alternative, a statement from a credit institution for the last three months may be considered proof of funds;
10. a check of whether the Customer is a politically exposed person (PEP) or their spouse;
11. a check of whether the customer is in a list of financial sanctions (European Union, FATF, United Nations) or embargo.
12. a certificate or data concerning the beneficial owner.

**In the event of a high-risk (Tier 3) customer**, the Company applies enhanced due diligence measures and requests the following data:

1. completed customer questionnaire (Annex 2);
2. sending a copy of the identity document; if necessary, a signature card authenticated by a notary or certified officially, and where necessary, certified by an apostille;

**Kui tegemist on kõrge riskiga kliendiga (tier 3),** siis rakendab äriühing tugevdatud hoolsusmeetmed ja küsib järgmised andmed:

1. Täidetud kliendi andkeet (lisa 2);
2. Isikuttõendava dokumendi koopia edastamine;  
Vajadusel notariaalselt tõestatud või ametlikult kinnitatud, lisaks vajaduse korral apostilliga;
3. Näopildi (*selfie*) edastamine;
4. Näopildi koos dokumendi ja paberiga, milles on märgitud näopildi tegemise kuupäev;
5. Liveness kontrolli läbimine (video verifitseerimine);
6. Online videointervjuu;  
Online videointervjuu raames on Personal eesmärgiks tuvastada isik, veenduda isikut tõendava dokumendi usaldusväärsuses ja koguda täiendavat teavet tehingu eesmärgi, tegevusala kohta, selleks et maandada rahapesu ja terrorismi rahastamise ohtu.
7. Juriidilise isiku puhul äriregistri väljavõte  
Kui andmed on avalikud, siis Personal ise kogub neid, kui andmed ei ole avalikud, küsitakse kliendi käest.  
Kui esineb kahtlus esitatud andmetes, siis tuleb küsida notariaalselt tõestatud koopia ja vajadusel korral tõlge.
8. Elukoha tõendi esitamine (*proof of residential address*)  
Kui Klient elu või asukoht on riigis, kus on olemas keskne sissekirjutuse süsteem, siis tõend sissekirjutuse kohta. Kui selline sissekirjutuse keskne register puudub, siis kolme kuu kommunaalarve, mis ei tohi olla vanem kui 3 kuud. Lisaks eeltoodule tuleb küsida viimase kolme kuu pangakonto väljavõtte;
9. Rahaliste vahendite tõend (*proof of funds*)  
Klient peab esitama tõendi, mis kinnitab ja tõestab tehingu jaoks saadud rahaliste vahendite päritolu. Selliseks tõendiks võib olla näiteks: laenuleping, vara müügileping, kindlustusleping, pärandvara saamise tõend vms. Kui tegemist on välismaise dokumendiga, mis ei ole koostatud eesti, 36uestio või vene keeles, see peab olema tõlgitud, et Personal saaks veenduda lepingu sisus. Lepingu puhul kindlasti jälgida, et see oleks allkirjastatud ja kehtiv. Alternatiivina eeltoodule võib esitada kolme kuu väljavõtte krediidasutusest. Kui äriühingul on tekkinud kahtlus rahaliste vahendite päritolus, tuleb vajadusel küsida

3. sending a facial image (selfie);
4. sending a facial image with a document and paper on which the date when the selfie was taken is indicated;
5. passing the liveness check (video verification);
6. online video interview.  
during the online video interview, the purpose of the Staff is to identify the person, make sure that the identity document is credible and gather additional information about the purpose of the transaction and field of activity in order to mitigate the risk of money laundering and terrorist financing;
7. extract from the Commercial Register in the case of a legal entity.  
If the data are public, the Staff collects the data on their own, if the data are not public, the data are requested from the customer. If the data submitted raise doubts, a copy authenticated by a notary and, where necessary, a translation thereof must be requested;
8. submission of proof of residential address.  
A certificate of enrolment if the customer's place of residence or location is in a country that has a central enrolment system. If the country does not have a central enrolment system, utility bills for three months, which are not older than three months. A bank statement for the last three months must be requested in addition to the above;
9. proof of funds.  
The customer must submit a certificate that confirms and proves the origin of funds obtained for the transaction. Such proof may include, for instance, a loan contract, contract of sale of property, insurance contract, certificate of receipt of estate, etc. In the event of a foreign document not prepared in Estonian, English or Russian, the document must be translated to enable the Staff to examine the substance of the contract. In the event of a contract, it must be made sure that the contract is signed and valid. A statement for three months issued by a credit institution may be submitted as an alternative. If the company has suspicions about the origin of funds, a document that proves the origin of the assets and a bank account statement for the last three months must be requested if necessary;
10. a check of whether the Customer is a politically exposed person (PEP) or their spouse;

- nii vara päritolu tõendavat dokumenti kui ka viimase kolme kuu pangakonto väljavõtte;
10. Kontroll, kas Klient on riikliku taustaga isik (PEP) või tema abikaasa;
  11. Kontroll, kas klient on finantssanktsioonide (Euroopa Liit, FATF, United Nations) või embargo nimekirjas;
  12. Tõend või andmed tegeliku kasusaaja kohta, vajadusel notariaalse kinnitusega.

Hoolsusmeetmeid kohaldatakse tugevdatud 37uest, alati kui:

- isikusamasuse tuvastamisel või Kliendi poolt esitatud teabe kontrollimisel tekib kahtlus esitatud andmete tõele vastavuses või dokumentide ehtsuses või tegeliku kasusaaja või tegelike kasusaajate tuvastamises;
- tehingus osaleja on Riikliku taustaga isik (välja arvatud Eesti Riikliku taustaga isik) või tema pereliige;
- tehingus osaleja on kõrge riskiga riigi kodanik või tema elu- või asukoht on kõrge riskiga kolmandas riigis;
- klient tegevusala või -valdkond on riskantne.

Kui esineb ükskõik milline kliendist, geograafilisest piirkonnast või tehingu/teenuse/toote 37uestion tulenev riski suurendav asjaolu, siis tuleb rakendada tugevdatud hoolsusmeetmeid, s.t. iga peatükis 3.1. ja 3.2. toodud riski suurendav asjaolu nõuab Kliendi suhtes tugevdatud hoolsusmeetme kohaldamist.

Tugevdatud hoolsusmeetmete kohaldamisel järgitakse vähemalt ühte järgmistest täiendavatest hoolsusmeetmetest:

- isikusamasuse tuvastamine ja esitatud teabe kontrollimine lisadokumentide, andmete või teabe põhjal, mis pärinevad usaldusväärsest ja sõltumatust allikast;
- lisameetmete võtmine esitatud dokumentide ehtsuses ja nendes sisalduvate andmete õigsuses veendumiseks, muu hulgas nende notariaalse või ametliku kinnitamise nõudmine;
- täiendava teabe kogumine ärisuhte või tehingu eesmärgi ja olemuse kohta ning esitatud teabe kontrollimine lisadokumentide, andmete või teabe põhjal, mis pärinevad usaldusväärsest ja sõltumatust allikast;
- täiendava teabe ja dokumentide kogumine tehingute tegeliku teostamise kohta ja tehingus kasutatavate vahendite allika ja päritolu tuvastamiseks, et välistada tehingute näilisus;

Tugevdatud hoolsusmeetmete kohaldamise korral kohaldab Äriühing tavapärasest sagedamini

11. a check of whether the customer is in a list of financial sanctions (European Union, FATF, United Nations) or embargo.
12. a certificate or data concerning the beneficial owner, authenticated by a notary if necessary.

Enhanced due diligence measures are applied always when:

- upon identification of a person or verification of information submitted by the customer, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner(s);
- a party to the transaction is a politically exposed person (except for an Estonian politically exposed person) or their family member;
- a party to the transaction is a citizen of a high-risk third country or their place of residence or location in a high-risk third country;
- the customer's area or field of activity is risky.

Where any risk-increasing factor arising from the customer, geographic area or transaction/service/product risk exists, enhanced due diligence measures need to be applied, i.e. each risk-increasing factor specified in Articles 3.1 and 3.2 calls for the application of enhanced due diligence measures to the customer.

Upon application of enhanced due diligence measures, at least one of the following additional due diligence measures is applied:

- identification of a person and verification of submitted information based on additional documents, data or information originating from a credible and independent source;
- application of additional measures for the purpose of verifying the authenticity of documents and the data contained therein, among other things, demanding that they be certified by a notary or officially certified;
- gathering additional information on the purpose and nature of the business relationship or transaction and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
- gathering additional information and documents regarding the actual execution of transactions and for the purpose of identifying the source and origin of the funds used in a transaction in order to rule out the ostensibility of the transactions;

Upon application of enhanced due diligence measures, the Company applies the monitoring of

ärisuhte seiret ja hindab uuesti Kliendi riskiprofiili hiljemalt ühe aasta Tier 2 puhul ja hiljemalt kuus kuud Tier 3 pärast ärisuhte loomist.

Ebahariliku tehingu, toimingu või asjaolu ilmnmisel on Personalil kohustus analüüsida ja võrrelda tehingu asjaolusid rahapesu ja terrorismi rahastamise kahtlusega tehingute tunnustega (vt. Peatükki 4).

Tulenevalt eeltoodust, kui esineb mingi asjaolu, mis viitab sellele, et tegemist võib olla keskmise või kõrge riskiprofiiliga Kliendiga ja tema suhtes tuleb rakendada tugevdatud hoolsusmeetmed, siis Personal kohustub koguma täiendavat teavet veendumaks selles, et tehingute tegemine ja ärisuhte loomine kliendiga on lubatud ning puudub kahtlus tema seoses rahapesu ja terrorismi rahastamisega.

#### **4.13 Tehingud riikliku taustaga, kohaliku taustaga isikuga isikuga, kelle suhtes rakendatakse rahvusvahelisi sanktsioone**

**Riikliku taustaga isik** 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 haldus- või järelevalveorgani liige, rahvusvahelise organisatsiooni juht, juhi asetäitja ja juhtorgani liige või samaväärseid ülesandeid täitev isik, kes ei ole kesk- või alamastme ametniku 38uestion.

Personal kohustub täitma täiendavad hoolsusmeetmed olukorras, kus majandus- või kutsetegevuses tehtavas tehingus või ametitoimingus osalev isik, ametiteenust kasutav isik, klient või nende tegelik kasusaaja on riikliku taustaga isik, riikliku taustaga isiku pereliige või riikliku taustaga isiku lähedaseks kaastöötajaks peetav isik, mis on järgmised:

a business relationship more frequently than usual and reassesses the customer's risk profile no later than a year in the case of Tier 2 and no later than six months in the case of Tier 3 after the establishment of the business relationship.

Upon emergence of an unusual transaction, act or factor, the Staff is required to analyse and compare the circumstances of the transaction with the characteristics of transactions suspected of money laundering and terrorist financing (see Article 4).

In view of the above, if there is a factor that refers to a possible medium-risk or high-risk customer and enhanced due diligence measures need to be applied to the customer, the Staff undertakes to gather additional information in order to make certain that the making of transactions and the establishment of a business relationship with the customer is allowed and the customer is not suspected of being involved in money laundering or terrorist financing.

#### **4.13 Transactions with a politically exposed person, a local politically exposed person and a person subject to international sanctions**

**Politically exposed person** means a natural person who is or who has been entrusted with prominent public functions, including a head of State, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a *chargé d'affaires* and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a State-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials.

In a situation where a person participating in a transaction made in economic or professional activities, a person participating in a professional act, a person using a professional service, a customer or their beneficial owner is a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person, the Staff is required to apply the following due diligence measures:

1. request the required additional information from the customer, in order to identify the sources of wealth and funds used in the framework of the business relationship or transaction;
2. verify data or make queries to the databases of the public authorities of the

1. Kliendilt vajaliku täiendava informatsiooni küsimine, tegemaks kindlaks varanduse ja rahaliste vahendite allikad, mida ärisuhete või tehingu raames kasutatakse;
2. andmete kontrollimine või päringute tegemine vastava riigi riigiasutuste andmebaasidesse ja internetis saadavate andmete otsimine ja kontroll;

Riikliku taustaga isikuga ärisuhete loomise otsustab Aqdigital juhatus või kontaktisik. Andmeid kontrolliv Personal informeerib juhatust siis, kui Klient või tegelik kasusaaja osutub hiljem või saab Riikliku taustaga isikuks.

Riikliku taustaga isikuga loodud ärisuhetes rakendatakse regulaarset tugevdatud kontrolli. Regulaarset tugevdatud kontrolli rakendatakse ka pärast isiku Riikliku taustaga isikuna tegevuse lõpetamist, kui tulenevalt riskipõhise lähenemise põhimõttest nimetatud isikuga kaasneb endiselt kõrgendatud risk.

Riikliku taustaga isiku osas rakendatakse täiendavaid hoolsusmeetmeid vähemalt 12 kuud pärast seda, kui Riikliku taustaga isik ei täida talle antud olulisi avalikke ülesandeid.

**Kohaliku riikliku tausta** isik on kui isik, kes täidab või on täitnud avaliku võimu olulisi ülesandeid Eestis, teises Euroopa Majanduspiirkonna lepinguriigis või Euroopa Liidu institutsiooni juures. Kohaliku riiklikuga taustaga isiku puhul rakenduvad üldjuhul samad täiendavad hoolsusmeetmed, mis ka riikliku taustaga isiku puhul. Kuid Aqdigital OÜ-l on õigus jätta eelnevalt nimetatud täiendavad hoolsusmeetmed rakendamata, kui Kliendi näol on tegemist kohaliku riikliku taustaga isikuga ning puuduvad 39ue tavapärasest kõrgemale riskile viitavad asjaolud.

#### 4.14 Rahvusvaheliste finantssanktsioonide rakendamine ja nende täitmise kontrollimine

**Rahvusvaheline sanktsioon või Vabariigi Valitsuse sanktsioon** on välispoliitiline meede, mille kehtestab EL, ÜRO või Vabariigi Valitsus. Tegu on mittesõjalise meetmega, mida rakendatakse eesmärgiga säilitada või taastada rahu, hoida ära konflikte ja tugevdada rahvusvahelist julgeolekut, toetada ja tugevdada demokraatiat ning järgida õigusriigi põhimõtteid, inimõigusi ja rahvusvahelist õigust. Meetmed võivad olla (1) mittemajanduslikud ja (2) majanduslikud. Majanduslikud meetmed võib jaotada omakorda (a) rahvusvahelisteks

country, and search for and verify data available on the Internet.

The establishment of a business relationship with a politically exposed person is decided by the Management Board or compliance officer of Aqdigital. The Staff verifying the data informs the Management Board where a customer or beneficial owner later proves to be or becomes a politically exposed person.

In business relationships established with a politically exposed person, enhanced control is exercised regularly. Regular enhanced control must also be exercised after a politically exposed person has ceased to be a politically exposed person where, based on the risk-based approach, the person still entails a heightened risk.

Additional due diligence measures are applied to a politically exposed person at least 12 months after the person has stopped performing the prominent public functions conferred upon them.

**Local politically exposed person** means a person who is or who has been entrusted with prominent public functions in Estonia, another contracting state of the European Economic Area or an institution of the European Union. In the case of a local politically exposed person, usually the same additional due diligence measures as in the case of a politically exposed person are applied. However, Aqdigital OÜ has the right to omit the aforementioned additional due diligence measures where the customer is a local politically exposed person but other factors referring to a higher-than-ordinary risk are absent.

#### 4.14 Implementation of international financial sanctions and control of their implementation

**An international sanction or a sanction of the Government of the Republic** is a foreign policy measure established by the EU, the United Nations or the Government of the Republic. It is a non-military measure implemented with the aim of maintaining or restoring peace, preventing conflicts and strengthening international security, supporting and strengthening democracy and observing the principles of the rule of law, human rights and international law. Measures can be (1) non-economic and (2) economic. Economic measures can be further divided into (a) international financial sanctions and (b) trade sanctions.

**Person subject to an international sanction** means a natural person or a legal entity, authority, civil law partnership or legal arrangement explicitly specified in a legal instrument establishing or

finantssanktsioonideks ja (b) kaubanduslikeks sanktsioonideks.

**Rahvusvahelise sanktsiooni subjektiks** on füüsiline või juriidiline isik, asutus, seltsing või mis tahes muu üksus, kes on otseselt nimetatud rahvusvahelist sanktsiooni kehtestavas või rakendavas õigusaktis ja kelle suhtes võetakse rahvusvahelist sanktsiooni kehtestavas õigusaktis ettenähtud meetmeid.

Äriühing määrab rahvusvaheliste finantssanktsioonide rakendamise eest vastutavat isikut ja selleks on äriühing kontaktisik Yevhen Diedukhov (edaspidi rahvusvahelise finantsantsiooni rakendamise eest vastutav isik või ka RsanS-i eest vastutav isik). Sellel isikul peavad olema vajalikud oskused ja teadmised rahvusvaheliste finantssanktsioonide rakendamise kohta. RsanSi eest vastutav isik määratakse juhatuse otsusega ja kandidatuur kooskõlastatakse Rahapesu andmebürooga. Rsansi eest vastutav isik vastutab finantssanktsiooni valdkonnas kehtivate normatiivsete sätete järgimise ja finantssanktsioonidest tulenevate meetmete võtmise eest, samuti sanktsiooni rikkumisest või võimalikest sanktsiooni rikkumistest teatamise eest.

Äriühing rakendab finantssantsiooni hoolsusmeetmed:

- Ärisuhte loomisel;
- Tehingu tegemisel;
- Ärisuhte ajal ja ärisuhte seire korral;
- Finantssantsiooni rikkumise riski või kahtluse korral.

Personal peab pöörama erilist tähelepanu Äriühinguga ärisuhtes oleva või tehingut või toimingut tegeva isiku, samuti ärisuhte loomist või tehingu või toimingu tegemist kavandava isiku tegevusele ja asjaoludele, mis viitavad võimalusele, et isik on rahvusvahelise finantssanktsiooni subjekt.

Personal peab:

- pöörama täiendavat hoolsust ärisuhte loomisel ja tehingute tegemisel kliendi ja tehingu asjaolude suhtes (sh tehingu teise osapoole suhtes);
- jälgima oma tegevuses sanktsioonide alast informatsiooni ja vastavaid nimekirjasid

applying the international sanction and against whom measures provided for in the legal instrument establishing the international sanction are taken.

The company appoints a person responsible for the implementation of international financial sanctions, and it is company's compliance officer Yevhen Diedukhov (hereinafter the person responsible for the implementation of international financial sanctions or also the person responsible for RSanS). This person must have the necessary skills and knowledge of the implementation of international financial sanctions. The person responsible for RSanS is appointed by the Company's member of the board decision and the candidant should be confirmed with the Financial Intelligence Unit. The person responsible for RSans is responsible for complying with the normative provisions in the field of financial sanctions and taking measures resulting from financial sanctions, as well as for reporting sanction violations or possible sanction violations.

The company implements financial sanction due diligence measures:

- When establishing a business relationship;
- When making a transaction;
- During the business relationship and in case of monitoring the business relationship;
- In case of risk or suspicion of financial sanctions violation.

The Staff must pay special attention to the activities of a person having a business relationship with the Company or making a transaction or an act with the Company or planning the establishment of a business relationship or the making of a transaction or act with the Company as well as to factors referring to the possibility that the person is subject to an international financial sanction.

The Staff must:

- upon establishment of a business relationship and making transactions, exercise special care towards the customer and the circumstances of the transaction (incl. with regard to the other party to the transaction);
- in its activities, take notice of information on sanctions and respective lists on the website of the FIU (or use direct sources to that end<sup>9</sup>)<sup>10</sup>;
- report to the FIU on identifying a person subject to a financial sanction and on imposing the financial sanction on the basis thereof;



<p>RAB veebilehel (või kasutama selleks otseallikaid<sup>9</sup>)<sup>10</sup>;</p> <ul style="list-style-type: none"> <li>• teavitama finantssantsiooni subjekti tuvastamisest ja selle alusel finantssanktsiooni rakendamisest RAB-i;</li> <li>• finantssanktsiooni subjekti kahtluse korral koguma täiendavat informatsiooni (sh kliendilt);</li> <li>• isiku või tehingu asjaolude ja teise osapoole suhtes finantssanktsiooni subjekti kahtluse säilimisel peale täiendava informatsiooni kogumist teavitama kahtlusest (ka juhul, kui täiendavat informatsiooni ei õnnestu koguda) RAB-i<sup>11</sup>, seniks keeldudes edasiste tehingute tegemisest ja/või ärisuhte loomisest;</li> <li>• teavitama RAB-i ärisuhte loomise või tehingu teostamise keeldumisest juhul kui keeldumise aluseks oli isiku, riigi, tehingu või tehingu aluseks oleva kauba võimalik puutumus rahvusvahelise sanktsioonirežiimiga</li> <li>• teavitama RAB-i olukorrast, kui on tekkinud kahtlus, et isik on rahvusvahelise finantssanktsiooni subjekti otsese või kaudse kontrolli all;</li> <li>• teostama finantssanktsioonide tuvastamiseks kontrole;</li> <li>• säilitama finantssanktsiooni kahtluste, rakendamiste ja vastavate kontrollidega seotuid andmeid.</li> </ul> <p>Juhul kui Personalil on kahtlus või ta teab, et Äriühinguga ärisuhtes olev või tehingut tegev isik on rahvusvahelise sanktsiooni 41. ülesand, annab Personal rahvusvahelise finantssanktsiooni subjekti tuvastamisest, sellekohasest kahtlusest ja võetud meetmetest viivitamatult teada Rahapesu andmebüroole. <u>Sellises olukorras on Personalil keelatud luua ärisuhtet sellise isikuga või teostada tehingut ja sellest asjaolust peab viivitamatult teavitama Äriühingu juhatust ja kontaktisikut.</u></p>	<ul style="list-style-type: none"> <li>• in the event of suspicion that a person is subject to a financial sanction, gather additional information (incl. from the customer);</li> <li>• if the suspicion of the applicability of financial sanctions to a person or the circumstances of a transaction and another party persist after gathering additional information (also where no additional information can be gathered), report to the FIU<sup>19</sup> on the suspicion, refusing to make further transactions and/or establish a business relationship until further notice;</li> <li>• report to the FIU on refusal to establish a business relationship or make a transaction if the basis for the refusal was a possible link between the person, state, transaction or goods that were the object of the transaction and an international sanction regime;</li> <li>• inform the FIU about a situation where there is reason to suspect that a person is under the direct or indirect control of a person who is subject to an international financial sanction;</li> <li>• carry out checks for the purpose of identifying financial sanctions;</li> <li>• retain data related to financial sanction suspicions, impositions and checks.</li> </ul> <p>If the Staff suspects or knows that a person having a business relationship with the Company or making a transaction with the Company is subject to an international sanction, the Staff immediately informs the Financial Intelligence Unit of identifying the person subject to the international financial sanction, the respective suspicions and the measures taken. <u>In such a situation, the Staff is prohibited to establish a business relationship with the person or to make a transaction with the person and must immediately inform the Management Board and compliance officer of the Company of the fact.</u></p> <p>If the Staff suspects or knows that a person in a business relationship or transaction with the Company is subject to an international sanction, the following due diligence measures must be taken:</p> <ul style="list-style-type: none"> <li>• Collect additional information about whether the person with whom you intend to do business or</li> </ul>
--	--

<sup>9</sup> EL kehtestatud sanktsioonide ülevaade: <https://www.sanctionsmap.eu/#/main>

<sup>9</sup> Overview of sanctions imposed by the EU: <https://www.sanctionsmap.eu/#/main>

<sup>10</sup> Finantssanktsioonide otsing: <https://www.politsei.ee/et/rahapesu>

<sup>10</sup> Financial sanctions search: <https://www.politsei.ee/en/money-laundering>

<sup>11</sup> Teavitama RAB-i: <https://fiu.ee/saada-teade#saada-teade>

<sup>19</sup> Report to the FIU: <https://fiu.ee/saada-teade#saada-teade>

Juhul kui Personalil on kahtlus või ta teab, et Äriühinguga ärisuhtes olev või tehingut tegev isik on rahvusvahelise sanktsiooni subjekt, tuleb rakendada järgmised hooldusmeetmed:

- koguda lisateavet selle kohta, kas temaga ärisuhtes olev või seda kavandav isik on finantssanktsiooni subjekt või kavandatav või tehtav tehing või toiming rikub finantssanktsiooni, ning kontrollib seda lisadokumentide, andmete või teabe põhjal, mis pärineb usaldusväärsest ja sõltumatust allikast;
- koguda lisateavet ärisuhte, tehingu või toimingu eesmärgi ja olemuse kohta ning kontrollib seda lisadokumentide, andmete või teabe põhjal, mis pärineb usaldusväärsest ja sõltumatust allikast.

Informatsiooni finantssanktsiooni jõustumise, muutmise või lõppemise kohta saab kontrolli Rahapesu andmebüroo kodulehel<sup>12</sup>.

Äriühing teostab **iga Kliendi osas rahvusvahelise finantssanktsiooni kontrolli**, mida teeb Äriühingule verifitseerimise partner Sum and Substance.

Kui Klient ei ole läbinud Sum and substance poolt sanktsioonide nimekirjade kontrolli, on keelatud temaga ärisuhtet luua või tehingut teha. Kui kontrolli tulemusena on tekkinud kahtlus selles, et klient on sanktsioonisubjekt või on see kinnitamist leidnud, tuleb esitada vastav ISR teade RAB-ile ning tehingute tegemine või ärisuhte loomine/jätkamine sellise Kliendiga on rangelt keelatud.

Rahvusvahelise finantssanktsiooni rakendamise vajaduse kahtluse korral ei tohi tehingut lõpuni teha. Tehingut tohib teha, kui RAB annab selleks kirjaliku loa vastavalt RSanS sätestatud erandi kohta sätestatu alusel. Rahvusvaheline finantssanktsioon on ainuke teate liik, mille esitamisel on kohustatud isikul õigus teate esitamisest teavitada isikut ennast.

Äriühing kohaldab rahvusvahelise finantssanktsiooni kui:

who intends to do so is a subject of a financial sanction or a proposed or committed breach of the financial sanction, and verifies it from additional documents, data or information from a reliable and independent source;

- Collect additional information about the purpose and nature of the business relationship, transaction, or transaction and verify it based on additional documents, data, or information from a reliable and independent source.

Information on the entry into force, amendment or termination of a financial sanction is available on the website of the Financial Intelligence Unit<sup>20</sup>.

**The Company will perform an international financial sanction review of each Client by Sum and Substance**, the Company's verification partner.

If the Client has not passed the check of the sanctions lists by Sum and substance, it is prohibited to establish a business relationship or enter into a transaction with the Client. If, as a result of the inspection, there is a suspicion that the Client is the subject of a sanction or has been confirmed, the relevant ISR notice must be submitted to the FIU and the conclusion of transactions or the establishment / continuation of a business relationship with such Client is strictly prohibited.

In case of doubt as to the need to apply an international financial sanction, the transaction may not be completed. The transaction may be executed if the RAB gives written permission in accordance with the provisions of the exemption provided by the RSanS. An international financial sanction is the only type of notice upon submission of which the obligated person has the right to notify the person of the submission of the notice.

A company applies an international financial sanction if:

- identifies the subject of the targeted financial sanction;
- the transaction or action he plans or performs violates the financial sanction;
- doubts whether a person in a business relationship with Company or who plans to do so is the subject of a targeted financial sanction;
- doubts whether the transaction or action he is planning or performing violates the financial sanction;
- after the application of due diligence measures, it is not possible to determine whether the person

<sup>12</sup> Uudised finantssanktsioonide kohta: <https://fiu.ee/rahvusvahelised-sanktsioonid/rahvusvahelised-finantssanktsioonid>

<sup>20</sup> Information about sanctions: <https://fiu.ee/rahvusvahelised-sanktsioonid/rahvusvahelised-finantssanktsioonid>

- tuvastab sihipärase finantssanktsiooni subjekti;
- tema kavandav või tehtav tehing või toiming rikub finantssanktsiooni;
- kahtleb, kas temaga ärisuhtes olev või seda kavandav isik on sihipärase finantssanktsiooni subjekt;
- kahtleb, kas tema kavandav või tehtav tehing või toiming rikub finantssanktsiooni;
- hoolsusmeetmete kohaldamise järel ei ole võimalik kindlaks teha, kas temaga ärisuhtes olev või seda kavandav isik on sihipärase finantssanktsiooni subjekt või juhuti tehtavat tehingut kavandav isik rikub finantssanktsiooni.

Äriühing võib külmutada kliendi vahendid finantssanktsiooni kohaldamise korral või kui RAB annab selleks vastava juhise.

Äriühing kogub ja säilitab andmed, mis on seotud:

- kontrollidega, kas temaga ärisuhtes olev või seda kavandav isik on finantssanktsiooni subjekt;
- kontrollidega, kas kavandav või tehtav tehing või toiming rikub finantssanktsiooni;
- finantssanktsiooni kohaldamisega ja
- Rahapesu Andmehüroo teavitamisega.

Samuti tuleb säilitada andmed, mis on kogutud hoolsusmeetmete täitmisel. Andmed säilitatakse muu hulgas viisil, mis võimaldab ammendavalt ja viivitamata vastata järelevalveasutuste või muude selleks õigustatud isikute päringutele.

Lisaks eeltoodule tuleb Personalil juhendada RAB-i kodulehel avaldatud juhendist „Rahapesu andmehüroo juhend rahvusvaheliste finantssanktsioonide rakendamiseks“<sup>13</sup>.

#### **4.15 Uute ja olemasolevate tehnoloogiatega ning teenuste ja toodetega, sealhulgas uute või ebatraditsiooniliste müügikanalite ning uute või arenevate tehnoloogiatega kaasnevate riskide tuvastamine ja riskide juhtimine**

Enne uue teenuse või -toote, uute või ebatraditsiooniliste müügikanalite pakkumist Klientidele või uute või arenevate tehnoloogiate kasutuselevõttu hindab Äriühingu juhatus sellega kaasnevaid rahapesu ja terrorismi rahastamise riske. Selleks kaardistab Äriühingu juhatus iga uue

having a business relationship with him or planning to do so is the subject of a targeted financial sanction or a person planning an occasional transaction violates the financial sanction.

The company may freeze the client's funds in case of application of a financial sanction or if the FIU issues/provides a corresponding instruction.

The company collects and stores data related to:

- with checks, whether the person who has a business relationship with him or is planning to do so is the subject of a financial sanction;
- with checks whether the planned or performed transaction or action violates the financial sanction;
- with the application of a financial sanction and
- Notices to the Financial Intelligence Unit.

Data collected during due diligence must also be retained. The data is stored, among other things, in a way that enables exhaustive and immediate responses to requests from supervisory authorities or other authorized persons.

In addition to the above, the Staff should follow and take into account the FIU guidance “The Financial Intelligence Unit for the Application of International Financial Sanctions”<sup>21</sup>.

#### **4.15 Identification and management of risks relating to new and existing technologies, and services and products, including new or non-traditional sales channels and new or emerging technologies**

Before providing customers with a new service or product or new or non-traditional sales channels or before introducing new or emerging technologies, the Management Board of the Company assesses the related risks of money laundering and terrorist financing. To that end, the Management Board of the Company maps the risks related to each new product, service, technology or sales channel. Upon assessment of risks, the actual as well as potential risks are analysed and, where necessary, additional information on the risks and the measures of mitigating them is collected.

As a result of mapping risks, the Management Board of the Company assesses the likelihood of

<sup>13</sup> <https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-rahvusvahelis>

<sup>21</sup> <https://fiu.ee/en/guidelines#guidelines-for-the-i>

toote, teenuse, tehnoloogia või müügikanaliga kaasnevaid riske. Riskide hindamisel analüüsitakse nii tegelikke kui ka potentsiaalseid riske ja vajadusel kogutakse täiendavat informatsiooni riskide ja nende maandamise meetmete kohta.

Riskide kaardistamise tulemusena hindab äriühingu Juhatus riskide realiseerumise tõenäosust, pöörates tähelepanu nii riske suurendavate kui ka vähendavatele asjaoludele. Seejärel hindab Äriühing, millised konkreetset meetmed on kõige sobilikumad ja optimaalsemad riskide maandamiseks ning korraldab vajadusel vastumeetmete ellurakendamise.

Äriühing hindab, kas vastumeetmete kohaldamisega on võimalik 44ue uute finantsteenuste või – toodete, uute või ebatraditsiooniliste müügikanalite või uute või arenevate tehnoloogiate kaasnevaid rahapesu ja terrorismi rahastamise riske selliseks, et need vastaksid Äriühingu Riskiisule.

Uue finantsteenuse või -toote, uute või ebatraditsiooniliste müügikanalite pakkumist Klientidele või uute või arenevate tehnoloogiate kasutuselevõttu võib alustada üksnes juhul, kui kaasnevad rahapesu ja terrorismi rahastamise 44uesti on kooskõlas Äriühingu Riskiisuga või on neid võimalik 44ue vastumeetmete rakendamisega aktsepteeritava tasemeni.

Eelnimetatud riskihinnangu argumendid ja tulemused dokumenteeritakse.

#### **4.16 KYC- ja KYT-partnerile hoolsuskohustuse delegerimise kord**

Äriühingul on õigus osa hoolsuskohustuse täitmisest üle anda kvalifitseeritud kolmandale poolele (KYC- ja KYT-partner). Selline kolmas pool tuleb hoolikalt valida.

AQDigital OÜ peab eelkõige arvestama:

- üleandmise mõju ettevõtte äritegevusele ja võimalikke riske;
- aruandlus- ja järelevalvekorda, mida kohaldatakse alates tegevuse üleandmise lepingu algusest kuni selle lõppemiseni, sealhulgas tegevuse üleandmise kirjelduse koostamist, tegevuse üleandmise lepingu sõlmimist, lepingu täitmist kuni selle lõppemiseni ning lepingu lõpetamise situatsiooniplaane ja strateegiat;
- KYC- ja KYT-partneri valimise ja hindamise korda ja meetodikat.

Äriühing peab tagama, et kolmas pool on võimeline täitma rahapesu ja terrorismi rahastamise tõkestamise seaduse (RahaPTS) nõudeid ning on usaldusväärne ja vajaliku kvalifikatsiooniga. Eelkõige peab Äriühing

materialisation of the risks, paying attention to both risk-increasing as well as risk-reducing factors. Thereafter, the Company assesses which specific measures are the most suitable and optimal for mitigating the risks and organises the application of counter-measures, where necessary.

The Company assesses whether the application of the counter-measures can mitigate the risks of money laundering and terrorist financing related to the new financial services or products, new or non-traditional sales channels or new or emerging technologies to such an extent that these correspond to the Company's risk appetite.

The provision of customers with a new financial service or product or new or non-traditional sales channels or the introduction of new or emerging technologies may be commenced only if the resulting risks of money laundering and terrorist financing correspond to the Company's risk appetite or can be reduced to an acceptable level by applying counter-measures.

The arguments and results of the aforementioned risk assessment are documented.

#### **4.16 Procedure for delegating due diligence to KYC and KYT partner**

Company is entitled to transfer some of the due diligence function to the qualified third party (KYC and KYT partner). Such third party must be chosen carefully.

In particular, AQDigital OÜ must take into account:

- the effect of the transfer on the Company's business and emerging risks;
- the reporting and monitoring procedure applied from the beginning to the end of the activity transfer agreement, including preparation of the description of the activity transfer, conclusion of the activity transfer agreement, execution of the agreement until its expiration, contingency plans and strategies for terminating the agreement;
- the procedure and methodology of selecting and evaluating KYC and KYT partner.

Company has to ensure the ability of third party to fulfill the requirements of MLTFPA, as well as the reliability and necessary qualification. Especially Company has to ensure that chosen third party is able to identify situations of a suspicious and unusual nature which could be signs of money laundering or terrorist financing.

In order to delegate some of the due diligence functions, AQDigital concludes a written contract with KYC/KYT partner.

Such contract must ensure:

tagama, et valitud kolmas pool on võimeline tuvastama kahtlasi ja ebatavalisi olukordi, millel on rahapesu või terrorismi rahastamise tunnuseid.

Hoolsuskohustuste delegeerimiseks sõlmib AQDigital KYC-/KYT-partneriga kirjaliku lepingu.

Lepinguga tuleb tagada:

- õiguste ja kohustuste jaotus (nt andmete säilitamine);
- et tegevuse üleandmine ei takista ettevõtet täita RahaPTS-is sätestatud kohustusi;
- et KYC-/KYT-partner täidab kõiki delegeeritud hoolsuskohustusi;
- et tegevuse üleandmine ei takista Äriühingu üle järelevalve tegemist;
- partneri vajalike teadmiste ja oskuste tase ning selleks rakendatavad meetmed, sealhulgas korrapärane koolitus;
- et Äriühingul oleks piiramatult õigus kontrollida RahaPTS-i nõuete täitmist;
- et RahaPTS-i nõuete täitmiseks kogutavad dokumendid ja andmed on kättesaadavad AQDigital OÜ nõudmisel;
- et Äriühingul on õigus lõpetada leping, kui KYC-/KYT-partner ei ole täitnud lepingulisi kohustusi või ei ole neid nõuetekohaselt täitnud.

Äriühing ei tohi delegeerida tegevust kolmandale poolele, kes on asutatud suure riskiga riigis.

## 5 EBAHARILIKE TEHINGUTE TUVASTAMINE

Äriühingu Personal kohustub analüüsima võimalikku rahapesukahtlusega tehingu tuvastamist, kui ilmnevad järgmised klientide tunnused oma tavapärase töötegevuse käigus:

- isik soovib kasutada teenuseid, kuid soovib säilitada oma anonüümsust ning varjata vahendite (illegaalset) päritolu;
- isik ei soovi avaldada tegelikke kasusaajaid;
- isiku suhtes, kes soovib kasutada virtuaalvääringute raha vastu vahetamise või virtuaalvääringute rahakotiteenuseid, eksisteerib variisiku kahtlus (nt sotsiaalne välimus või taust ei vasta tellitava teenuse või äritegevuse iseloomule, isik ei oska selgitada tellitavat teenust või ei tea fakte ettevõtte äritegevuse kohta vms);
- isik soovib läbi virtuaalvahendite raha vastu vahetamise teenuse pakkuja teha tehinguid, millel puudub majanduslik 45ues ja mille põhjal tekib kahtlus, et ettevõtte puudub reaalse majandustegevus;

- distribution of rights and obligations (e.g. data storage);
- that the transfer of activity does not prevent the Company's fulfillment of the obligations set out in MLTFPA;
- that the KYC/KYT partner fulfills all delegated due diligence obligations;
- that the transfer of activity does not prevent the supervision of the Company;
- the necessary level of knowledge and skills of the partner and the set of measures applicable for this purpose, including regular training;
- the Company's unrestricted right to check compliance with the requirements of MLTFPA;
- Documents and data collected to fulfill the requirements of MLTFPA are available upon AQDigital OÜ request;
- the Company has the right to terminate the contract if the KYC/KYT partner has failed to fulfill contractual obligations or has not fulfilled them properly.

The Company must not delegate activities to third party which is established in a High-risk country.

## 5 IDENTIFICATION OF UNUSUAL TRANSACTIONS

The Staff of the Company undertakes to analyse the identification of a potential transaction suspected of money laundering if the following customer characteristics become evident in the course of their ordinary work:

- the person wishes to use the services, but also to remain anonymous and conceal the (illegal) origin of the funds;
- the person does not wish to disclose the beneficial owners;
- the person who wishes to use the services of exchanging virtual currencies for fiat currencies or the virtual currency wallet services is suspected of being a front (e.g. their social appearance or background does not correspond to the nature of the commissioned service or business activity, the person cannot explain the service ordered or does not know facts about the activities of a business, etc.);
- the person wishes, through the provider of the service of exchanging virtual funds for a fiat currency, to make transactions that lack any economic reason and on the basis of which it can be suspected that the business lacks actual economic activities;

- isik keeldub tehingute kohta selgituste andmisest või ei ole antud selgitused ning dokumendid usutavad;
- isik soovib läbi virtuaalvahendite raha vastu vahetamise teenuse või rahakotiteenuse pakkuja sooritada tehinguid suurtes summades (üle 10 000 euro) sularahas ja ei soovi esitada andmeid vara päritolu kohta;
- isik soovib sooritada tehinguid virtuaalvääringutega summas üle 32 000 eurot ja ei soovi või ei anna veenvaid andmeid vara päritolu kohta;
- isik pöördub Aqdigital OÜ poole ettepanekuga, mis oma olemuselt viitab rahapesule;
- isik maksab virtuaalvääringu eest ebaharilikult kontolt (s.t. tekib kahtlus, et konto ei kuulu temale);
- isik kasutab pidevalt erinevaid sidevahendeid ja kanaleid kontakteerumiseks;
- isik osutab ise tegevusluba eeldavat teenust tegevusluba omamata;
- riikliku taustaga isik (PEP) on ostnud või müünud virtuaalvääringuid suures ulatuses, üle 15 000 euro väärtuses;
- virtuaalvääringu tehingu puhul kasutatakse isiku identifitseerimist takistavaid tehnilisi vahendeid;
- virtuaalvääringu eest ostetakse vara rohkem kui 100 000 euro väärtuses;
- isik maksab virtuaalvääringute eest offshore piirkonna konto kaudu;
- isik kogub või kannab rahalisi vahendeid või virtuaalvääringut üle isikule, kes on seotud terroristlike organisatsioonidega;
- isik kannab rahalisi vahendeid või virtuaalvääringut üle isikule või saab vahendeid selliselt isikult, kes tegutseb kõrge terrorismihuga piirkonnas.

Kui esineb ükskõik milline eelnimetatud tunnustest, kohustub töötaja rakendama täiendavad hooldusmeetmeid ja teavitama äriühingu Juhatus ja Kontaktisikut, kes omakorda teavitab sellest Rahapesu andmebürood. Rahapesu andmebüroo teavitamine on vajalik ka siis, kui faktiliselt teenuse osutamist kliendile ei toimu ja/või ärisuhet ei looda.

- the person refuses to give explanations on the transactions or the given explanations and documents are not plausible;
- the person wishes, through the provider of the service of exchanging virtual funds for a fiat currency or the wallet service, to make transactions in large sums (over 10,000 euros) in cash and does not wish to submit information on the origin of the assets;
- the person wants to conclude transactions in virtual currencies in an amount that exceeds 32,000 euros and does not want or does not give convincing data regarding the origin of the assets;
- the person contacts AQdigital OÜ with a proposal that has the characteristics of money laundering;
- the person pays for a virtual currency from an unusual account (i.e. there is a reason to suspect that the person is not the account holder);
- the person constantly uses different means of communication and channels to make contact;
- the person provides a service that calls for an authorisation, but the person does not have any authorisation;
- a politically exposed person (PEP) has purchased or sold virtual currencies on a large scale, exceeding the value of 15,000 euros;
- in the case of a virtual currency transaction, technical means impeding the identification of the person are used;
- assets worth over 100,000 euros are purchased for a virtual currency;
- the person pays for virtual currencies via an offshore account;
- the person collects or transfers funds or a virtual currency to a person who is linked to terrorist organisations;
- the person transfers funds or a virtual currency to a person or receives funds from a person who operates in a region if there is a high risk of terrorism.

If any one of the aforementioned characteristics exists, the employee is required to apply additional due diligence measures and notify the Management Board and compliance officer of the Company and the Management Board, in turn, reports to the Financial Intelligence Unit. Reporting to the Financial Intelligence Unit is also necessary where no service is actually rendered to the customer and/or no business relationship is established.



## 6 PIIRANGUD TEHINGUTE TEOSTAMISEL

Ärisuhte loomine või tehingute tegemine on keelatud:

1. Kui tekib ärisuhte hoolsusmeetmete käigus kogutud dokumentidele tuginedes kahtlus, et tegemist võib olla rahapesu või terrorismi rahastamisega või selle katsega;
2. Kui tekib kahtlus, et isik on rahvusvahelise sanktsiooni 47.ülesti;
3. Kui klient soovib arveldada sularahas;
4. Kui klient ei esita hoolsusmeetmete täitmiseks nõutavaid dokumente ja teavet (sh teave päritolu riigi, tegevusala, tegeliku kasusaaja vms kohta);
5. Kui kliendi poolt esitatud andmete ja dokumenti põhjal tekib kahtlus, et tegemist võib olla rahapesu või terrorismi rahastamise või selle katsega ja täiendavate hoolsusmeetmete rakendamisel kahtlus ei likvideeru;
6. Kui Äriühingu nõudmise korral ei esita klient vara legaalselt päritolu tõendavaid dokumente/andmeid või elukoha tõendi või mõne muu nõutava dokumendi;
7. Kui kliendil on edukalt läbimata verifitseerimise protseduur.

Lisaks eeltoodule on keelatud tehingute tegemine klientidega:

1. kes on sanktsioonide nimekirjas;
2. kes on USA embargo sanktsioonide nimekirjas;
3. Kes on selle riigi kodanik või elanik või resident, kus ei ole lubatud virtuaalvääringutega kauplemine;
4. Kes on selle riigi kodanik või elanik või resident, mis on kõrge riskiga riigi või keelatud riikide nimekirjas (lisa 4);
5. Kes on selle riigi kodanik või elanik või resident, kus virtuaalvääringutega kauplemine eeldab täiendavate tegevuslubade olemasolu.

AQdigital OÜ-l ega Personalil ei ole lubatud :

1. Teha tehingut kliendiga, kelle isikusamasus ei ole tuvastatud Juhendi kohaselt;
2. Teha tehinguid anonüümsete või fiktiivsete isikutega, kes kasutavad teisi nimesid või valenime;
3. Teha tehinguid isikutega, kellel on variisiku tunnused;

## 6 RESTRICTIONS ON TRANSACTIONS

It is prohibited to establish a business relationship or make a transaction:

1. in a situation where, based on documents collected in the course of application of due diligence measures to a business relationship, money laundering or terrorist financing or an attempt thereof is suspected;
2. if suspicions arise that the person is subject to an international sanction;
3. if the customer wishes to settle in cash;
4. if the customer does not submit the documents and information required for compliance with due diligence measures (incl. information on the country of origin, field of activity, beneficial owner, etc.);
5. if, based on the data and documents submitted by the customer, there is suspicion of money laundering or terrorist financing or an attempt thereof, and the application of additional due diligence measures does not eliminate the suspicion;
6. if a customer fails to submit the documents/data certifying the legal origin of the assets or proof of residential address or any other document requested by the Company;
7. if the customer has not passed the verification procedure successfully.

In addition to the above, it is prohibited to make transactions with customers:

1. who are included in the list of sanctions;
2. who are included in the US embargo sanctions list;
3. who are citizens or residents of the country where trade in virtual currencies is not allowed;
4. who are citizens or residents of the country included in the list of high-risk or prohibited countries (Annex 4);
5. who are citizens or residents of the country where trade in virtual currencies presumes the existence of additional authorisations.

AQdigital OÜ or the Staff is not allowed to:

1. make a transaction with a customer whose identity has not been established in accordance with the Guidelines;
2. make transactions with anonymous or fictitious persons who use aliases or false names;
3. make transactions with persons who have the characteristics of a front;
4. make transactions with persons who hide data or submit false data;

4. Teha tehinguid isikutega, kes varjavad andmeid või esitavad valeandmeid;
5. Teha tehinguid isikutega, kellel on eelnev rahapesu või terrorismi rahastamise kahtlus;
6. Teha tehinguid isikutega, kes soovivad arveldada sularahas;
7. Teha tehinguid isikutega, kes on sanktsioonide või embargo nimekirjas.

Kui esineb üks asjaolu, mis ei võimalda tehingu tegemist või ärisuhte loomist Kliendiga, siis tuleb 48uest maksimaalselt võimalikke andmeid tema tausta ja vara päritolu kohta, fikseerida andmeid, teavitada Äriühingu Juhatust ja Kontaktisikut, kes otsustab teate esitamise vajalikkust RAB-ile.

## 7 ÄRISUHTE LOOMISEST KEELDUMISE JA ÄRISUHTE LÕPETAMISE ÜLDINE KORD

Äriühingul on õigus keelduda ärisuhte loomisest või lõpetada ärisuhe, kui:

- isikusamasuse tuvastamisel kogutud teavet ei ole võimalik usaldusväärsest ja sõltumatust allikast kontrollida (ptk 4.2 „Isikusamasuse tuvastamine füüsilise isiku puhul“);
- klient ei ole nõus isikusamasuse tuvastamiseks vajalikke andmeid uuendama (ptk 4.2 „Isikusamasuse tuvastamine füüsilise isiku puhul“);
- kliendi isikusamasuse tuvastamine ei õnnestu infotehnoloogiliste vahendite abil või tekkis kahtlus kliendi esitatud andmete õigsuses ja vahetu kohtumine ei ole võimalik (ptk 4.5 „Isikusamasuse tuvastamine infotehnoloogiliste vahendite abil“);
- ei ole võimalik välja selgitada tegelikku kasusaajat (ptk 4.6 „Tegeliku kasusaaja tuvastamine“);
- kliendi suhtes kohaldatakse rahvusvahelist sanktsiooni või ta ei ole läbinud Sumsubi sanktsioonikontrolli (ptk 4.14 „Rahvusvaheliste finantssanktsioonide rakendamine ja nende täitmise kontrollimine“);
- ärisuhte loomine või tehingute tegemine on 6. peatüki („Piirangud Tehingute Teostamisel“) kohaselt keelatud.

Ärisuhte loomisest keeldumise korral rakendatakse üldjuhul järgmist korda.

1. Kui töötajad (I kaitseliin) leiavad asjaolusid, mis välistavad ärisuhte loomise, peavad nad ise lõpetama edasised tegevused ärisuhte loomiseks sellise isikuga.
2. Töötajad peavad viivitamata, kuid mitte hiljem kui 24 tunni pärast, teatama

5. make transactions with persons suspected of money laundering or terrorist financing before;
6. make transactions with persons who wish to settle in cash;
7. conclude transactions with persons entered in the list of sanctions or embargo.

If there is a factor that does not allow for making a transaction or establishing a business relationship with a customer, as much data as possible on the customer's background and the origin of the assets must be obtained, the data must be recorded, the Management Board or compliance officer of the Company must be notified, and the Management Board and the compliance officer, who decides whether it is necessary to report to the FIU.

## 7 GENERAL PROCEDURE OF REFUSAL TO ESTABLISH BUSINESS RELATIONSHIP AND TERMINATION OF BUSINESS RELATIONSHIP

The Company is empowered to refuse establishing business or terminate business relationship with customer in several cases:

- Information gathered upon identification cannot be verified from a credible and independent source (Chapter 4.2 Identification of a natural person);
- Customer is not willing to update data required for identification (Chapter 4.2 Identification of a natural person);
- Customer cannot be identified using information technology means or there are doubts about the correctness of the data given by the customer and the face-to-face meeting is not possible (Chapter 4.5 Identification of a person using information technology means);
- It is not possible to identify the beneficial owner (Chapter 4.6 Identification of the beneficial owner);
- Customer is subject to international sanction or has not passed Sum & Substance sanction check (Chapter 4.14 Implementation of international financial sanctions and Control of their implementation);
- When it is prohibited to establish business relationship or make a transaction according to the Chapter 6 Restrictions On Transactions.

Upon refusal to establish business relationship, the following procedure is generally applied:

1. If Staff (I line of defence) finds circumstances which preclude



järelevalveametnikule või juhatuse liikmele asjaoludest, mis välistavad ärisuhte loomise. Samas peab Personal tagama, et kõik asjakohased andmed kogutakse ja säilitatakse nõutaval viisil (8. peatüki „Aruandekohustus“ ja 9. peatüki „Andmete kontrollimine ja säilitamine“ kohaselt).

3. Kontaktisik ja/või juhatus hindavad töötajate kogutud andmeid, koguvad vajaduse korral lisateavet ja otsustavad, kas esineb rahapesu, terrorismi rahastamise või muude asjaolude kahtlus, mis nõuab aruande esitamist rahapesu andmebüroole. Selline hinnang tuleb teha kahe tööpäeva jooksul.

Äriühing lõpetab ärisuhte Kliendiga:

1. Kasutajatingimustes sätestatud juhtudel;
2. Kui Kliendi suhtes ei ole võimalik rakendada nõutud hoolsusmeetmeid;
3. Kui kliendi suhtes on tekkinud kahtlus, et tegemist on rahapesu või terrorismirahastamisega;
4. Kui klient on sanktsioonisubjekt.

Ärisuhte lõpetamisel rakendatakse üldjuhul järgmist korda.

1. Kui töötajad (I kaitseliin) leiavad asjaolusid, mis annavad alust ärisuhte lõpetamiseks, peavad töötajad ise lõpetama kõik edasised tegevused ja tehingud kliendi/klientidega ning teatama sellest viivitamata, kuid mitte hiljem kui 24 tunni pärast, järelevalveametnikule või juhatusele.
2. Kui järelevalveametnik või juhatus (II kaitseliin) leiab asjaolusid, mis annavad alust ärisuhte lõpetamiseks, peab järelevalveametnik või juhatus andma töötajatele viivitamata korralduse peatada kõik edasised tegevused ja tehingud kliendi/klientidega.
3. Kontaktisik või juhatus hindab kahe tööpäeva jooksul, kas ärisuhte lõpetamise aluseks olevatest asjaoludest tuleb teatada rahapesu andmebüroole.
4. Kui kontaktisik või juhatus otsustab ärisuhte lõpetada, teavitatakse Personal sellest otsusest ja nad on kohustatud teavitama klienti 10 päeva ette konto sulgemisest. Selle tähtaja möödumisel, Personal kohustub sulgema konto ja piirama ligipääsu teenustele, kui Rahapesu Andmebüroo ei nõua esitatud teate tulemusena, et kliendi suhtes rakendatakse muid meetmeid. Seejuures kliendisuhete

establishment of business relations, Staff itself has to stop further actions towards establishment of business relations with such person.

2. Staff have to report to Compliance officer or Management Board immediately, but no longer than during 24 hours about finding circumstances which preclude establishing of business relationship. At the same time, according to this Rules Staff must ensure that all related data is collected and stored in the required manner (according to Chapter 8 Duty to Report and Chapter 9 Collection, Verification and Retention of Data).
3. Compliance officer and/or Management Board assess data gathered by the Staff, collect additional information if needed and decides whether suspicion of money laundering, terrorist financing or other circumstances exist which requires to submit report to the FIU. Such assessment is to be done within two working days.

The company terminates the business relationship with the Client:

1. In the cases regulated in the user Terms and Conditions;
2. If it is not possible to apply the required due diligence measures to the Customer;
3. If there is a suspicion that the customer is involved in money laundering or terrorist financing;
4. If the client is a subject to sanctions.

Upon termination of business relationship, the following procedure is generally applied:

1. If Staff (I line of defence) finds circumstances which are ground for termination of business relationship, Staff itself has to suspend any further actions, transactions of customer/-s and immediately, but no longer than 24 hours report to Compliance officer or Management Board.
2. If Compliance officer or Management Board (II line of defence) find circumstances which are ground for termination of business relationship, Compliance officer or Management Board must immediately instruct Staff to suspend any further actions, transactions of the customer/-s.
3. Compliance officer or Management Board assess whether the circumstances which are ground for termination of business relationship are subject for reporting to the FIU within two working days.

lõppemisel järgitakse avaldatud Platvormi Kasutajatingimusi<sup>14</sup>.

5. Kui seejuures kliendil jäävad vahendeid Äriühingu platvormil, kohustub Äriühing tagastama vahendeid kliendi kuuluvale pangakontole, mis asub Euroopa Majanduspiirkonnas või rahakotti aadressile, kust vahendid on algselt tulnud. Juhul kui Äriühing soovib tagastada vahendile muule kontole või aadressile, tuleb teavitada sellest Rahapesu Andmebürood vähemalt seitse tööpäeva ette ja jälgida, et Rahapesu Andmebüroo ei seaks käsutamise piirangut varale või tehingu peatamist.

Teatud juhtudel võivad töötajad rahapesu andmebürood otse teavitada (vt 8. peatükk „Teatamiskohustus“).

## 8 TEATAMISKOHUSTUS

Personal on kohustatud olukorras, kus suhetes Kliendiga ilmnevad asjaolud:

1. mis on ebaharilikud või mille puhul Personalil tekib rahapesu või terrorismi rahastamise kahtlus;
2. mis keelavad või ei võimalda ärisuhte loomist või tehingu tegemist vastavalt Juhendile

viivitamatult teatada sellest Kontaktisikut, kes otsustab ja vastutab informatsiooni viivitamatu edastamise eest Rahapesu andmebüroole.

Äriühing lähtub teatamiskohustuse täitmisel RAB-I juhendist „Juhend kahtlaste tehingute tunnuste kohta”.<sup>15</sup>

Kontaktisik või juhatus ise peab RAB-I teavitama viivitamata, kuid mitte enam kui kahe tööpäeva jooksul rahapesu kahtluse tuvastamisest arvates. Personalil on õigus koheselt ise edastada RAB-ile teate kahtlusest rahapesu või terrorismi rahastamises juhul, kui:

1. kliendil on eelnev rahapesu ja/või terrorismi rahastamise kahtlus;
2. klient on keeldunud hoolsuskohustuse täitmisel andmete esitamisest või on

4. If there is a decision made by Compliance officer or Management Board to terminate business relationship, the Staff is informed of the decision and is obliged to notify the Customer 10 days in advance before cancelation of the account. After before mentioned deadline the Staff should cancel customer access to the service and account. Unless any other actions are required towards the customer by the FIU as the result of submitted report. In addition to that business relationship cancelation should be done according published Terms and Conditions of the Platform.<sup>22</sup>

5. If the customer still has funds on the Company's platform and business relationship is ended, the Company undertakes to return the funds to the customer's bank account located in the European Economic Area or to the wallet address from which the funds originally came. In the event that the Company wishes to return the assets to another account or wallet address, the FIU must be notified of this at least **seven working days** in advance and ensure that the FIU does not restrict the use of the asset or suspend the transaction.

In certain cases Staff can report directly to the FIU (see Chapter 8 Duty to Report).

## 8 DUTY TO REPORT

In a situation where:

1. unusual circumstances become evident in a relationship with a customer or whereby the Staff has a reason to suspect money laundering or terrorist financing, or
2. circumstances prohibiting or precluding, in accordance with the Guidelines, the establishment of a business relationship or the making of a transaction become evident,

the Staff must immediately inform the compliance officer of this, and the latter decides on and is responsible for reporting it to the Financial Intelligence Unit without delay.

Upon performance of the duty to report, the Company adheres to the “Guidelines on the

<sup>14</sup> Kasutajatingimused on kättesaadavad siin: [https://aqdigital.exchange/en/terms\\_and\\_conditions](https://aqdigital.exchange/en/terms_and_conditions)

<sup>15</sup> Kättesaadav kodulehel: <https://www.politsei.ee/files/Rahapesu/juhend-kahtlaste-tehingute-tunnuste-kohta-en.pdf?3e4fc8c9fe>

<sup>15</sup> Available on the website: <https://www.politsei.ee/files/Rahapesu/juhend-kahtlaste-tehingute-tunnuste-kohta-en.pdf?3e4fc8c9fe>

<sup>22</sup> Terms and Conditions are available on the website: [https://aqdigital.exchange/en/terms\\_and\\_conditions](https://aqdigital.exchange/en/terms_and_conditions)

<p>esitanud valeandmeid ja on põhjust arvata, et viivitamatu toimetama jätmine võib endaga kaasa tuua negatiivseid tagajärgi;</p> <ol style="list-style-type: none"> <li>3. klient on esitanud võltsitud dokumente ja kasutab võõra isiku nime;</li> <li>4. klient on rahvusvahelise sanktsiooni 51uestio.</li> </ol> <p>Personal peab muuhulgas teatama Äriühingu juhatusele või Kontaktisikule järgmistest asjaoludest:</p> <ol style="list-style-type: none"> <li>1. kui ärisuhte loomine, tehing või toiming või teenuse osutamine jääb teostamata;</li> <li>2. ärisuhte loomisest või tehingu tegemisest keeldutakse hoolsusmeetmete kohaldamise võimatuse tõttu;</li> <li>3. ärisuhte loomisest või tehingu tegemisest keeldutakse, sest isiku kapitali moodustavad esitaja aktsiad või 51ue esitajaväärtpaberid;</li> <li>4. Klient ei esita, vaatamata sellekohasele nõudmisele, dokumente ja asjakohast teavet või tehingu objektiks oleva vara päritolu tõendavaid andmeid või dokumente või esitatud andmete ja dokumentide põhjal tekib kahtlus, et tegemist võib olla rahapesu või terrorismi rahastamisega;</li> </ol> <p>Kontaktisik analüüsib (ja vajadusel kogub juurde) Personali poolt edastatud infot rahapesu või terrorismi rahastamise kahtluse kohta ja edastab ise, või volitab selleks 51ue isikut, teate RAB-ile. RAB-ile esitatava teate koostamisel ja edastamisel lähtutakse Rahapesu andmebüroole esitatava teate sisu ja vormi ning teate esitamise juhendist.<sup>16</sup> Aqdigital OÜ juhatuse säilitab kirjalikku taasesitamist võimaldavas vormis Personalilt laekunud teated kahtlaste ja ebaharilike tehingute kohta, samuti nende teadete analüüsimiseks kogutud informatsiooni ja 51ue seonduvad dokumendid ning Rahapesu andmebüroole edastatavad teated, koos teate edastamise aja ja edastanud töötaja andmetega.</p> <p>Klienti või tehingus osalevat isikut (sh tema esindajat ja muid seotud isikuid), kelle kohta tekkinud kahtlusest Rahapesu andmebürood informeeritakse, on <u>rangelt keelatud</u> sellest teavitada.</p> <p>Teade edastatakse rahapesu andmebüroole digitaalselt, kasutades rahapesu andmebüroo kodulehel olevat vormi (link „Saada teade“)<sup>17</sup> või rahapesu andmebürooga kokkulepitud vormingut (XML-vorming). Teate edastamine rahapesu andmebürooga kokkulepitud vormingus toimub infosüsteemide andmevahetuskihi X-tee süsteemi kaudu.</p>	<p>Characteristics of Suspicious Transactions” established by the FIU<sup>14</sup>.</p> <p>The compliance officer or the Management Board itself must inform the FIU immediately but no later than within two working days of the detection of the suspicion of money laundering.</p> <p>The Staff has the right to report to the FIU directly on the suspicion of money laundering or terrorist financing where:</p> <ol style="list-style-type: none"> <li>1. a prior suspicion of money laundering and/or terrorist financing is known regarding the customer;</li> <li>2. the customer has refused to submit data upon performance of the due diligence duty or has given false information and there is a reason to believe that failure to take immediate action could bring about negative consequences;</li> <li>3. the customer has submitted forged documents and uses the name of another person;</li> <li>4. the customer is subject to an international sanction.</li> </ol> <p>The Staff must inform the Management Board of the Company or the compliance officer of the following circumstances, among others:</p> <ol style="list-style-type: none"> <li>1. a business relationship cannot be established, a transaction or operation cannot be made or a service cannot be provided;</li> <li>2. the establishment of a business relationship or the making of a transaction is refused due to the impossibility of the application of the due diligence measures;</li> <li>3. the establishment of a business relationship or the making of a transaction is refused, because the person’s capital comprises bearer shares or other bearer securities;</li> <li>4. the customer does not, in spite of a respective request, submit documents and relevant information or data or documents proving the origin of the assets constituting the object of the transaction or, based on the submitted data and documents, there is a reason to suspect money laundering or terrorist financing.</li> </ol> <p>The compliance officer analyses (and, where necessary, collects) information communicated by the Staff regarding the suspicion of money laundering or terrorist financing and reports it to the FIU itself or authorises another person to do it. Upon drawing up and sending a report to the FIU, the instructions on the substance and form of a</p>
--	---

<sup>16</sup> <https://www.riigiteataja.ee/akt/101122017020>

<sup>17</sup> Elektroniliselt on võimalik esitada teate siin: <https://rabis-web.politsei.ee/#/>

<sup>17</sup> Electronic reports can be submitted here: <https://rabis-web.politsei.ee/#/>

Küsimuste korral tuleb pöörduda Rahapesu andmebüroo poole:  
Address: Pronksi 12, Tallinn, 10416  
e-post: [info@fiu.ee](mailto:info@fiu.ee)  
telefon: (+372) 696 0500

## 9 ANDMETE KOGUMINE, KONTROLLIMINE JA SÄILITAMINE

Aqdigital OÜ kogub ja säilitab andmed Kliendi ja temaga seotud isikute kohta, mida saab teada hoolsuskohustuste täitmisel.

Registreeritakse kõikide tehingute või etappide sisu, aeg või periood, summa, valuuta, konto- või virtuaalvaluuta rahakoti number. Isikusamasuse tuvastamisel ja esitatud teabe kontrollimisel registreeritakse vastav toiming kontrollimise läbiviimise kuupäeva või ajavahemiku seisuga.

Tehingu ja Kliendi kohta registreeritakse andmeid vastavalt riskiastme määramise otsusele.

Aqdigital OÜ säilitab isikusamasuse tuvastamise ja esitatud teabe kontrollimise aluseks olevate dokumentide originaale või koopiaid ja ärisuhte loomise aluseks olevaid dokumente viis aastat pärast ärisuhte lõppemist.

Aqdigital OÜ säilitab dokumente ja andmeid Klientide kohta viisil, mis võimaldab ammendavalt ja viivitamata vastata rahapesu andmebüroo või muude riigiasutuste päringutele, muu hulgas selle kohta, kas Äriühingul on või on eelmise viie aasta jooksul olnud ärisuhe päringus nimetatud isikuga ning milline on või oli selle suhte olemus.

Personalil on kohustus säilitada:

1. Koopiat isikut tõendavast dokumendist;
2. Päringute vastuseid andmebaasidest, mis on tehtud andmete kontrollimiseks;
3. Klientide poolt täidetud ankeedid;
4. Kõik 52ue dokumendid või andmed, mis on klient esitanud seoses hoolsuskohustuste täitmisega;
5. Otsuse riskiastme määramise kohta;

report to be submitted to the Financial Intelligence Unit and the reporting instructions are followed<sup>12</sup>. The Management Board of Aqdigital OÜ retains in a format that can be reproduced in writing all the reports received from the Staff about suspicious and unusual transactions as well as any information collected for analysing these reports and other related documents and any reports forwarded to the Financial Intelligence Unit along with information about the time of the forwarding of the report and the employee that forwarded it.

It is strictly prohibited to notify a customer or a person participating in a transaction (incl. their representative and other related parties) with respect to whom a suspicion is being communicated to the Financial Intelligence Unit.

The report is forwarded to the Financial Intelligence Unit digitally, using the form on the website of the Financial Intelligence Unit (the "Send notification" link)<sup>13</sup> or the format agreed with the Financial Intelligence Unit (XML format). A report in a format agreed with the Financial Intelligence Unit is forwarded via the information systems data exchange layer (X-road).

In the event of questions, the Financial Intelligence Unit must be contacted, using the following contact details:

Address: Pronksi 12, Tallinn, 10416;  
email: [info@fiu.ee](mailto:info@fiu.ee);  
telephone: (+372) 696 0500.

## 9 COLLECTION, VERIFICATION AND RETENTION OF DATA

Aqdigital OÜ collects and retains data on a customer and persons related to the customer, which are learned upon performance of the due diligence duties.

The substance, time or period, amount, currency, account number or virtual currency wallet number of all transactions or steps are registered. Upon identification of a person and verification of submitted information, the respective step is registered as of the date or period of carrying out the verification.

Data on a transaction and a customer are registered based on a risk level determination decision.

Aqdigital OÜ retains the originals or copies of the documents which serve as the basis for identification of persons and verification of submitted information, and the documents serving as the basis for the establishment of a business relationship for five years after the termination of the business relationship.

Aqdigital OÜ retains the documents and data on customers in a manner that allows for exhaustively and immediately replying to the enquiries of the

<p>6. Kliendi nõusolekud ja kinnitused (sh. Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise kohta);</p> <p>7. Teade rahapesu kahtluse kohta, mis edastatakse Äriühingu juhatusele või RAB-ile või terrorismi rahastamise kahtluse kohta, sealhulgas andmed, millel aruanne põhines;</p> <p>8. Otsused/hinnangud selle kohta, miks on jäänud isikuga ärisuhe loomata või tehing tegemata;</p> <p>9. Otsused/hinnangud selle kohta, miks on jäänud isikuga ärisuhe loomata või tehing tegemata;</p> <p>10. Teave ärisuhte lõpetamise asjaolude kohta hoolsusmeetmete rakendamise võimatuse tõttu.</p> <p>11. ärisuhte monitooringu käigus andmete ja dokumentide kogumine;</p> <p>12. kirj vahetus kliendiga, mis on seotud AQDigital OÜ poolt RahaPTS täitmisega.</p> <p>Isikut tõendava dokumendi kehtivust tuleb kahtluse korral kontrollida Politsei- ja Piirivalveameti kodulehelt <a href="https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/">https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/</a> Aqdigital OÜ säilitab hoolsuskohustuse täitmise käigus saadud andmeid turvalises renditud serveris Hetzner <a href="https://www.hetzner.com">https://www.hetzner.com</a>, mis asub Saksamaal. Seejuures andmete säilitamisel ja töötlemisel arvestatakse kõiki GDPR-ist<sup>18</sup> tulenevaid tingimusi ja reegleid. Samuti hoolsuskohtuste täitmise käigus saadud andmeid hoitakse ja säilitatakse verifitseerimise ja KYT teenuseid osutatava partneri Sum&amp;Substance serverites. Kuid Äriühing võib kasutada ka muid turvalisi servereid andmete säilitamiseks. Andmeid, mis on seostatud rahapesu ja terrorismirahastamise kahtlusega säilitatakse viisil, mis ei võimalda sellega tutvumist kellelegi peale Äriühingu Juhatust või Juhatuse poolt volitatud isikut.</p> <p>Aqdigital kustutab eelnimetatud säilitatud andmed 5 aasta möödumisel, kui asjaomast valdkonda reguleerivatest õigusaktidest ei tulene teistsugust korda. Pädeva järelevalveasutuse ettekirjutuse alusel võib rahapesu või terrorismi rahastamise tõkestamise, avastamise või uurimise seisukohast olulisi andmeid säilitada kauem, kuid mitte rohkem kui viis aastat pärast esmase tähtaja möödumist. Isikuandmete kaitse on äärmiselt oluline ja Personal on kohustatud jälgima seadusest tulenevaid reegleid seoses isikuandmete kaitsega. Kõik kliendi kohta saadud andmed seoses tööülesannete täitmisega on konfidentsiaalsed ega kuulu avaldamisele kolmandatele isikutele.</p>	<p>Financial Intelligence Unit or those of other public authorities, among other things, regarding whether the Company has or has had in the preceding five years a business relationship with the given person and what is or was the nature of the relationship. The Staff is required to retain:</p> <ol style="list-style-type: none"> <li>1. a copy of the identity document;</li> <li>2. responses to queries made to databases for the purpose of verifying data;</li> <li>3. questionnaires filled in by customers;</li> <li>4. all other documents or data that a customer has submitted in connection with the performance of the due diligence duties;</li> <li>5. the decision on determining the risk level;</li> <li>6. the consents and warranties of a customer (incl. on identifying the customer using information technology means);</li> <li>7. a report sent to the Management Board of the Company or to the FIU on suspected money laundering or terrorist financing, including the data which was the basis for such report;</li> <li>8. decisions on/estimates of the reasons for refusal to establish a business relationship or make a transaction with the person;</li> <li>9. information related to the impossibility of applying due diligence measures via KYC and/or KYT Partner or via using other information technology means;</li> <li>10. information about the circumstances of termination of business relationship because of impossibility of applying due diligence measures;</li> <li>11. data and documents collected during business relations monitoring;</li> <li>12. correspondence with customer which relates to enforcing of MLTFPA by AQDigital OÜ.</li> </ol> <p>When in doubt, the validity of the identity document must be verified on the website of the Police and Border Guard Board: <a href="https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/">https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/</a> AQdigital OÜ retains the data received in the course of performance of the due diligence obligation on the secure server Hetzner <a href="https://www.hetzner.com">https://www.hetzner.com</a>, which is located in Germany. Upon retention and processing of data, any and all terms and conditions and rules arising from the GDPR<sup>14</sup> are adhered to. The data also obtained during the performance of the due diligence obligation are kept and stored on the servers of the verification and KYT service provider Sum&amp;Substance. However, the Company may also use other secure servers for data storage. Data associated with a suspicion of money laundering and terrorist financing are retained in a</p>
---	--

<sup>18</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679>



Aqdigital võib kogutud isikuandmeid töödelda üksnes rahapesu ja terrorismi rahastamise tõkestamise eesmärgil ning neid andmeid ei tohi töödelda viisil, mis ei vasta eelnimetatud eesmärgile.

Enne ärisuhte loomist või tehingu tegemist on oluline esitada kliendile isikuandmete töötlemist puudutava teabe.

Isikuandmete kogumise, töötlemisel ja säilitamisel tuleb lähtuda:

- a) Seaduslikkuse põhimõttest- s.t. isikuandmeid kogutakse ja töödeldakse täpselt vastavalt õiguspärastele eesmärkidele;
- b) Minimaalsuse põhimõttest- s.t. võimalikust väheste andmete kogumist
- c) Andmekvaliteedi põhimõttest- s.t. kogutud andmete ajakohastamist
- d) Piiratud säilitamise põhimõttest- s.t. andmeid ei tohi säilitada kauem, kui vaja
- e) Turvalisuse põhimõttest- s.t. andmete säilitamine peab olema turvaline, kasutades vajalikke tehnilise ja korralduslike meetmeid.

Isikuandmete kogumise, säilitamise, töötlemise või kustutamise küsimuste korral tuleb pöörduda Äriühingu Juhatusesse poole.

## 10 KOOLITUSKOHUSTUS

Juhendi täitmine on kohustuslik kõikidele Äriühingu töötajatele, kellele tööülesannete hulka kuulub suhtlus klientidega, ärisuhte loomine, tehingute tegemine ja andmete säilitamine.

Juhatus peab tagama Personalile, kelle tööülesannete hulka kuulub hoolsuskohustuste täitmine, regulaarse koolituse RahaPTS-ist tulenevate nõuete kohta. Koolitusel peab andma teavet eelkõige kohustatud isiku kohustuste kohta tulenevalt RahaPTS-ist, isikusamasuse tuvastamise ja andmete kogumise/säilitamise kaasaaegsetest meetoditest ja riskide hindamisest.

Juhatus peab tagama, et Personal osaleks vähemalt iga kahe aasta 54. ühesti või vajadusel segedamini eelnimetatud koolitusel. Uus töötaja peab läbima koolituse enne faktilist tööülesannete täitmist seoses hoolsusmeetmete rakendamisega ja klientide tuvastamisega, kuid mitte hiljem kui

manner that does not allow for accessing it by anyone besides the Management Board of the Company or a person authorised by the Management Board.

AQdigital deletes the retained data after the expiry of a period of five years, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of money laundering or terrorist financing may be retained for a longer period, but not for more than five years after the expiry of the first time limit.

The protection of personal data is of utmost importance and the Staff is required to adhere to the statutory rules related to personal data protection. The data obtained on the customer in connection with the performance of the employment duties are confidential and not subject to disclosure to third parties.

AQdigital may process the collected personal data solely for the purpose of preventing money laundering and terrorist financing and the data should not be processed in a manner that does not serve the aforementioned purpose.

Before the establishment of a business relationship or making a transaction it is important to submit to the customer information concerning the processing of personal data.

Upon collection, processing and retention of personal data, the following must be adhered to:

- a) the principle of lawfulness, i.e. personal data are collected and processed in strict accordance with legitimate purposes;
- b) the principle of minimalism, i.e. as little data as possible are gathered;
- c) the principle of data quality, i.e. the updating of the collected data;
- d) the principle of limited retention, i.e. data may not be retained for longer than necessary;
- e) the principle of security, i.e. data storage must be secure, using necessary technical and organisational measures.

In the event of questions concerning the collection, retention, processing or deletion of personal data, the Management Board of the Company must be addressed.

## 10 TRAINING OBLIGATION

The Guidelines must be followed by all the employees of the Company whose employment duties include communication with customers, establishing business relationships, making transactions and retaining data.

ühe kuu möödumisel pärast tööle asumisest. Koolituse korraldamine võib olla organiseeritud Äriühingu Juhatus või muu pädeva isiku poolt, kellel on olemas vajalikud teadmised ja oskused. Uuele töötajale, keda on kohustus koolitada, tutvustab Juhendit Juhatus või muu volitatud isik pärast töölepingu või muu võlaõigusliku lepingu sõlmimist vähemalt ühe nädala jooksul arvates uue töötaja tööle asumisest. Juhendiga tutvumist kinnitab töötaja allkirjaga.

Juhul kui käesolevas Juhendis tehakse muudatused, siis tuleb tutvustada tehtud muudatused Äriühingu Personalile, kes puutub oma tööülesannete täitmisel kokku Juhendist tulenevate kohustuste täitmisega, kahe nädala jooksul alates muudatuse tegemisest. Personal kinnitab juhendiga tutvumist oma allkirjaga.

## 11 JÄRELEVALVE JA SISEKONTROLLIMEETMED

Käesolevas Juhendis sisalduvate protseduurireeglite täitmise kontrollimise eest vastutab Äriühingu juhatus, kontaktisik ja siseaudiitor. Kontaktisik kontrollib Juhendi ajakohasust **vähemalt üks kord aastas** ja vajadusel täiendab seda või kehtestab uued protseduurireeglid. Juhendi muutumisel/täiendamisel/kontrollimisel teeb Kontaktisik märge järgmise kontrolli tähtaja kohta. Juhendi uuendamine peab olema kooskõlastatud ja kinnitatud Juhatus poolt.

Kontaktisik on kohustatud analüüsima töö jälgimise ja nõuete täitmise kontrollimise tulemused ning hindama Personali koolitusvajadusi.

Juhatus korraldab vähemalt kord aastas sisekontrolli Juhendist ja RahaPTS-ist tulenevate nõuete täitmise osas (edaspidi Siseaudit), mida teostab sertifitseeritud Siseaudiitor. Siseaudiitor koostab seejärel selle kohta kontrolliaruande (edaspidi Kontrolliaruanne või Siseauditi aruanne). Sisekontroll või siseaudit peab olema teostatud isiku või üksuse poolt, kellel on olemas vastav kompetents ja haridus ning laitmatu ameti- ja/või ärialane reputatsioon. Siseaudiitorile kohaldatakse audiitoritegevuse seaduses atesteeritud siseaudiitori kohta sätestatud nõudeid ja tegevuse õiguslikke aluseid. Siseaudiitor ei või täita ülesandeid, mis põhjustavad või võivad põhjustada huvide konflikti. Siseaudiitor peab olema kursis rahapesu ja terrorismi rahastamise

The Management Board must provide the Staff whose employment duties include performance of the due diligence duties with regular training in requirements arising from the MLTFPA. The training must provide information, above all, on the duties of the obliged entity under the MLTFPA, the modern methods of identification and collection/retention of data as well as risk assessment.

The Management Board must ensure that the Staff participates in the training at least once every two years or more frequently, where necessary. A new employee must complete the training before the actual performance of employment duties related to the application of due diligence measures and identification of customers, but not later than after one month has passed from commencement of work. The training may be organised by the Management Board of the Company or another competent person who has the required knowledge and skills.

The Management Board or another authorised person introduces the Guidelines to a new employee who needs to be trained within no more than a week after the new employee commences work under an employment contract or another contract under the law of obligations. The employee certifies with their signature that they have read the Guidelines.

If the Guidelines are amended, the amendments must, within two weeks after making the amendments, be introduced to the Staff of the Company engaged in the performance of the duties arising from the Guidelines upon performing their employment duties. The Staff members certify with their signature that they have examined the Guidelines.

## 11 SUPERVISION AND INTERNAL CONTROL MEASURES

The Management Board, the compliance officer and internal auditor of the Company are responsible for checking that the rules of procedure contained in these Guidelines are followed. The compliance officer reviews the Guide **at least once a year** and, where necessary, updates it or establishes new rules of procedure. Upon amendment/supplementation/review of the Guidelines, the compliance officer adds a notation on the deadline for the next review. Any updates to the Guidelines must be approved by the Management Board.

The compliance officer must analyse the results of monitoring work and verification of compliance with the requirements and assess the training needs of the Staff.

tõkestamise valdkonna regulatsiooniga nii üldisel tasemel kui ka kohustatud isiku kontekstis. Äriühingu osanik määrab siseaudiitorit. Siseaudiitorile tagab Äriühing kõik tema ülesannete täitmiseks vajalikud õigused ja töötingimused, sealhulgas õiguse saada selgitusi ja teavet Äriühingu juhtidelt ja töötajatelt ning jälgida avastatud puuduste kõrvaldamist ja tehtud ettepanekute täitmist.

Koostatud kontrolliaruanne (siseauditi aruanne) peab sisaldama vähemalt järgmist teavet:

- kontrolli eesmärk;
- kontrolli teostamise aeg;
- kontrolli teostaja nimi ja ametinimetus;
- läbiviidud kontrolli kirjeldus;
- kontrollimise tulemuste analüüs või teostatud kontrolli üldised järeldused;
- järgmise kontrolli läbiviimise aeg.

Sisekontrolli läbiviimisel hinnatakse muu hulgas:

1. Kas Äriühingu juhtimisraamistik (Juhend) on piisav rahapesu ja terrorismi rahastamise tõkestamiseks;
2. Kas Äriühingu tegevus on kooskõlas kehtivate rahapesu ja terrorismi rahastamise õigusaktidega ja juhenditega;
3. Kas Personal rakendab Juhendis ja õigusaktides sätestatud reegleid õigesti ja efektiivselt;
4. Kas Äriühingu meetodid on asjakohased ja vastavad järelevalveasutuste (RAB) ootustele;
5. Kas meetodid on piisavad Äriühingu riskiisu arvestades ja riskide efektiivselt juhtimiseks.

Seejuures sisekontrolli läbiviimise meetodid peavad arvestama Äriühingu suurust, tegevust ja osutatavate teenuste eripära, keerukuse astet ja riskiisu. Meetmed peavad olema piisavad ja proportsionaalsed selleks, et täita sisekontrolli eesmärki.

Kui kontrollimisel ilmnevad puudused Juhendis või selle praktilisel rakendamisel, lisatakse kontrolliaruandesse puuduste kirjeldused koos sellega seonduvate võimalike ohtude analüüsiga. Samuti nähakse ette puuduste kõrvaldamiseks aeg, puuduste kõrvaldamiseks soovitavalt kasutatavad meetmed ja järelkontrolli teostamise aeg.

Äriühingu juhatus otsustab koos siseaudiitoriga siseauditi läbiviimise vajadust ja perioodilisust. Äriühingu juhatus koostab koos siseaudiitoriga kinnitavad majandusaasta kohta koostatud sisekontrolli läbiviimise kava või plaani. Kui siseaudiitor märkab õigusrikkumist või klientide

The Management Board organizes at least once a year an internal control (internal audit) whether the Staff follows the requirements arising from the Guidelines and the MLTFPA which should be done by certified internal auditor, and draws up an audit report about this thereafter (hereinafter Audit report or internal control report).

Internal control or internal audit must be performed by a person or entity with the appropriate competence and education and an impeccable professional and / or business reputation. The requirements and legal bases for the activities of a certified internal auditor in the Auditing Act apply to the internal auditor. The internal auditor shall not perform any duties which give rise to or may give rise to a conflict of interests. The internal auditor must be aware of the regulations in the field of prevention of money laundering and terrorist financing both in the general level and in the context of the obligated person. The shareholder of the company shall appoint an internal auditor.

The Company shall grant the internal auditor all rights and working conditions necessary for the performance of his / her duties, including the right to receive explanations and information from the Company's managers and employees, and to monitor the elimination of identified deficiencies and compliance with the proposals made.

The audit report must include at least the following information:

- the purpose of the inspection;
- the time of the inspection;
- the name and position of the person who performed the inspection;
- a description of the inspection carried out;
- an analysis of the inspection results or general conclusions arising from the inspection;
- the deadline for the next inspection.

The internal control shall assess, inter alia:

1. Is the Company's governance framework (the Guidance) sufficient to prevent money laundering and terrorist financing;
2. Whether the Company operates in accordance with applicable money laundering and terrorist financing legislation and guidelines;
3. Does the Staff apply the rules set out in the Manual and legislation correctly and effectively;
4. Whether the Company's methods are appropriate and meet the expectations of the supervisory authorities (RAB);
5. Whether the methods are adequate given the Company's risk appetite and effective risk management.

In doing so, the methods of performing internal control must take into account the size of the Company, its activities and the specifics of the



huvide kahjustamist, peab ta sellest teavitama Äriühingu juhatus ja ka Rahapesu andmebürood.

Äriühing jälgib ja rakendab oma sisekontrolli süsteemis kolme kaitseliini põhimõtet.

Seejuures igale kaitseliinile on määratud erinevad ülesanded rahapesu ja terrorismi rahastamise tõkestamise eesmärgil ning iga kaitseliinil on teatud sõltumatus ning piisavalt ressursse tõhusaks toimimiseks.

**I kaitseliini** funktsiooniks on hoolsusmeetmete kohaldamine ärisuhte ja juhuti tehingu tegemisel ning hoolsusmeetmete kohaldamine ärisuhte kestel. I kaitseliini kuuluvad kohustatud isiku struktuuriüksused ja töötajad, kelle tegevusega riskid kaasnevad ja kes neid riske, nende spetsiifikat ja ulatust tuvastama ning hindama peavad ning kes neid riske oma tavapärase tegevusega – eelkõige hoolsusmeetmete kohaldamisega – juhivad. Seejuures kuuluvad I kaitseliinile kohustatud isiku tegevuse ja teenuse osutamisega kaasnevad 57uesti, nad on nende riskide haldajad (omanikud) ja vastutavad nende eest. AQDigital OÜ esimese Kaitseliini ülesanded täidavad kuusupport and compliance team liikmed.

I kaitseliini ülesandeks on omada head teadmist kliendist, tema tegevuse ja äritegevuse spetsiifikast. Selliselt peavad I kaitseliini töötajad olema kursis või ennast kurssi viima klientide erinevate äritegevuste spetsiifikaga ja nendega seotud riskidega, kui kohustatud isik on otsustanud teenust sellistele klientidele osutada. Eesmärgiks on tuvastada kliendi tegevuses kahtlastele või ebaharilikele tehingutele või mõistlikule majanduslikule eesmärgile mittevastavad või sellistele asjaoludele viitavad tehingud, et need edasiseks analüüsiks suunata II kaitseliinile.

**II kaitseliin** koosneb riskijuhtimise ja vastavuskontrolli funktsioonist. Neid funktsioone teostab kontaktisik OÜ AQDigital. Vastavuskontrolli funktsiooni eesmärk on tagada kohustatud isiku vastavus kehtivatele õigusaktidele, juhenditele jms dokumentidele ning hinnata õigusliku või regulatiivkeskkonna mis tahes muudatuste võimalikku mõju kohustatud isiku tegevusele ja vastavuskontrolli raamistikule.

Vastavuskontrolli ülesandeks on aidata I kaitseliinil kui riski omajatel defineerida kohad, kus 57uesti esinevad (näiteks kahtlaste ja ebaharilike tehingute analüüs, milleks vastavuskontrolli töötajatel on vastavad kutseoskused, isikuomadused jne), ja aidata I

services provided, the degree of complexity and the risk appetite. The measures must be adequate and proportionate to achieve the objective of internal control.

Should any deficiencies in the Guidelines or its practical implementation become evident upon inspection, descriptions of the deficiencies are added to the inspection report along with an analysis of possible threats associated therewith. The report must also specify a deadline and the recommended measures for the elimination of the deficiencies, as well as the time of a follow-up control.

The management board of the company, together with the internal auditor, decides on the need and periodicity of the internal audit. The management board of the company, in conjunction with the internal auditor, shall approve the plan or plan for the performance of internal control prepared for the financial year. If the internal auditor notices an offense or damage to the interests of clients, he or she must inform the Management Board of the Company and also the Financial Intelligence Unit.

The company monitors and implements the principle of three lines of defense in its internal control system.

At the same time, each line of defense is assigned different tasks to prevent money laundering and terrorist financing, and each line of defense has a degree of independence and sufficient resources to operate effectively.

The function of **the first line of defense** is to apply due diligence measures in the course of the business relationship and occasionally the transaction, and to apply due diligence measures during the business relationship. Line I includes the obligated person's structural units and employees whose activities involve risks and who must identify and assess these risks, their specificity and extent, and who manage these risks through their normal activities, in particular the application of due diligence measures. At the same time, the risks associated with the activities and provision of services of the obligated person belong to the first line of defense, they are the managers (owners) of these risks and are responsible for them. The tasks of the first Defense Line of AQDigital OÜ are performed by the members of support and compliance team.

The task of the first line of defense is to have a good knowledge of the customer, the specifics of his or her activities and business. Thus, the employees of the defense line I must be aware of

kaitseliinil efektiivselt neid riske juhtida. II kaitseliin ei tegele riskide võtmisega.

**III kaitseliini** moodustab sõltumatu ja tõhus siseauditi funktsioon. Siseauditi rolli teostajaks on sertefitseeritud siseaudiitor. Siseauditi meetodid peavad vastama kohustatud isiku suurusele ning tegevuse ja osutatavate teenuste laadile, ulatusele, keerukuse astmele, sh riskiisule ja kohustatud isiku tegevusega kaasnevatele riskidele. See tähendab, et auditi tegemise regulaarsus ja hinnatavad valdkonnad peavad arvestama eelnimetatud asjaolud. Siseaudiitor lähtub samuti riskipõhisuse ja proportsionaalsuse põhimõttest.

Juhatuse ülesandeks on selgitada igale kaitseliini töötajale või täitjale tema roll ja ülesanded.

## LISA 1. RISKIASTME MÄÄRAMISE OTSUS

### RISKIASTME MÄÄRAMISE OTSUS

#### Kliendi andmed

Eesnimi	
Perekonnanimi	
Sünnikoht/asutamiskoht	
Sünniaeg/registreerimise kuupäev	
Elukoha aadress/tegevuskoht	
Kodakondsus	
E-post	
Juriidilise isiku puhul registrikood	
Juriidilise isiku puhul, tegelik kasusaaja (nimi, isikukood/sünniaeg, kontaktid, residentsus)	
Juriidilise isiku puhul, esindusõigusega isiku andmed (nimi, isikukood/sünniaeg, residentsus, kontaktid)	
Ärisuhe loomise/teingu tegemise eesmärk	

or be aware of the specifics of the different business activities of the customers and the risks associated with them, if the obligated person has decided to provide the service to such customers. The purpose is to identify transactions that are suspicious or unusual in the customer's operations or that do not correspond to a reasonable economic purpose or that indicate such circumstances, in order to direct them to Defense Line II for further analysis.

**Line of defense II** consists of a risk management and compliance function. These functions are performed by the contact person OÜ AQDigital. The purpose of the compliance check function is to ensure the compliance of the obligated person with the applicable legislation, instructions and similar documents and to assess the possible impact of any changes in the legal or regulatory environment on the obligated person's activities and the compliance control framework.

The role of compliance control is to help Line I as risk holders to identify areas where risks exist (eg analysis of suspicious and unusual transactions, where compliance staff have the appropriate professional skills, personal qualities, etc.) and to help Line I effectively manage these risks. Line II does not take risks.

**Line of Defense III** consists of an independent and efficient internal audit function. The role of internal audit is performed by a certified internal auditor. The methods of internal audit shall be appropriate to the size of the obligated person and the nature, extent and level of complexity of the activities and services provided, including the risk appetite and the risks associated with the obligated person's activities. This means that the regularity of the audit and the areas to be assessed must take into account the above considerations. The internal auditor also follows the principles of risk-basedness and proportionality.

The task of the management board is to explain the role and tasks of each employee or executor of the defense.

## ANNEX 1. DECISION ON DETERMINATION OF RISK LEVEL

### DECISION ON DETERMINATION OF RISK LEVEL

#### Customer data

First name	
Surname	
Place of birth/place of establishment	

**Isikusamasuse tuvastamine ja KYC rakendamine**

- vahetel kohtumisel
- infotehnoloogiliste vahendite abil ja ankeedi alusel
- lisameetmena tuvastamine videointervjuu abil

**Kommentaar:**

**Riskitegurite esinemine**

Riskitegur	jah	ei
Riikliku taustaga isik		
Klient on riskiriigi kodanik, resident või elanik		
Eelnev rahapesu või terrorismi rahastamise kahtlus		
Variisiku tunnused		
Ebatavalised asjaolud ärisuhte toimimisel, sh. Keerulised, ebatavalised ja suuremahulised tehingud või ebatavaline tehingumuster, millel pole mõistlikku või majanduslikku eesmärki või mis pole konkreetse ärispetsiifika jaoks iseloomulik		
Keeruline juhtimisstruktuur, millel puhul pole võimalik välja selgitada tegeliku kasusaaja andmeid		
Klient kasutab kontakteerumiseks pidevalt erinevaid kontakte ja kanaleid		
Kliendi tegevusala on kõrgendatud riskiga		
Klient keeldub selgitama tehinguga seonduvaid asjaolusid või tema poolt esitatud andmed on ebausaldusväärsed		
Klient varjab oma vara päritolu		
Klient on rahvusvahelise sanktsiooni subjekt		

Date of birth/date of registration		
Address of place of residence/place of business		
Citizenship		
Email		
Registry code of legal person		
In the case of a legal entity, the beneficial owner (name, personal identification code/date of birth, contact details, residency)		
In the case of a legal entity, the details of the person holding the right of representation (name, personal identification code/date of birth, residency, contact details)		
Purpose of establishment of a business relationship/making of a transaction		

**Identification and application of KYC**

- face-to-face meeting
- using information technology means and based on a questionnaire
- identification via a video interview as an additional measure

**Comments:**

**Existence of risk factors**

Risk factor	Yes	No
Politically exposed person		
The customer is a citizen or resident of a high-risk country		
Prior suspicion of money laundering or terrorist financing		
Characteristics of a front		
Unusual circumstances in the way the business relationship works, incl. complex, unusual and large transactions or an unusual transaction pattern that does not have any reasonable or economic purpose or is not characteristic of the given business specifics		
A complex management structure whereby it is not possible to identify the details of the beneficial owner		
The customer constantly uses different contact details and channels for making contact		
The customer's field of activity involves a heightened risk		

**Kommentaar:**

Tulenevalt eeltoodust määran **kliendi riskikategooriaks (vali üks):**

- Madal risk (Tier 1)**  
 **Keskmine risk (Tier 2)**  
 **Kõrge risk (Tier 3)**

**Kas tehingu/ ärisuhte alustamine kliendiga on võimalik:**

- jah  
 ei

**Kommentaar** (Ei korral märgi juurde, miks tehingu tegemine/ärisuhte loomine on keelatud):

**Koostaja:**

**Kontaktisik:**

(ees- ja perekonnanimi)  
 (allkiri) (kuupäev)

## LISA 2. KLIENDI ANKEET

### Üldandmed:

Ees- ja perekonnanimi	
Sünniaeg/registreerimise kuupäev	
Sünnikoht/asutamiskoht	
Elukoha aadress/tegevuskoht	
Kodakondsus	
E-post	
Juriidilise isiku puhul registrikood	
Juriidilise isiku puhul, tegelik kasusaaja (nimi, isikukood/sünniaeg, kontaktid, residentsus)	
Juriidilise isiku puhul, esindusõigusega isiku andmed (nimi, isikukood/sünniaeg, residentsus, kontaktid)	
Juriidilise isiku puhul, esindus-/volitusõiguse alus ja kehtivus	

**Täiendavad andmed:**

The customer refuses to explain the circumstances pertaining to a transaction or the data given by the customer cannot be trusted		
The customer hides the origin of their assets		
The customer is subject to an international sanction		

### Comments:

Based on the above, I set **the customer's risk category to (choose one):**

- Low risk (Tier 1)**  
 **Medium risk (Tier 2)**  
 **High risk (Tier 3)**

**Whether the transaction can be made/business relationship established with the customer:**

- Yes  
 No

**Comments** (in the case of 'No,' give the reason why making of the transaction/establishment of the business relationship is prohibited):

**Prepared by:**

**Contact person:**

(given name and surname)  
 (signature) (date)

## ANNEX 2. CUSTOMER QUESTIONNAIRE

### General information:

First name and surname	
Date of birth/date of registration	
Place of birth/place of establishment	
Address of place of residence/place of business	
Citizenship	
Email	
Registry code of legal person	
In the case of a legal entity, the beneficial owner (name, personal identification code/date of birth, contact details, residency)	
In the case of a legal entity, the details of the person holding the right of representation	

Kas oman seost avaliku võimu esindajaga (riikliku taustaga isikuga) <input type="checkbox"/> jah <input type="checkbox"/> ei	(name, personal identification code/date of birth, residency, contact details) In the case of a legal entity, the basis for and term of validity of the right of representation/authorisation										
Juriidilise isiku puhul ärisuhte loomise/tehingute tegemise eesmärk	<b>Additional information:</b> Do I have a connection to a public authority figure (politically exposed person)? <input type="checkbox"/> Yes <input type="checkbox"/> No										
<b>Isikut tõendava dokumendi andmed:</b>											
Dokumendi liik											
Dokumendi number											
Dokumendi väljastaja riik ja asutus											
Dokumendi väljastamise kuupäev	Purpose of establishment of business relationship/conclusion of transaction in the case of legal entity										
Dokumendi aegumise kuupäev											
Täiendavalt esitatud dokumendid: <input type="checkbox"/> selfie <input type="checkbox"/> selfie koos dokumendi ja paberiga, millel on märgitud kuupäev <input type="checkbox"/> elukoha tõend <input type="checkbox"/> vara päritolu tõend <input type="checkbox"/> pangakonto väljavõte <input type="checkbox"/> tegeliku kasusaaja tõend <input type="checkbox"/> muu 61 uestion	<b>Details of identity document</b> <table border="1"> <tr> <td data-bbox="799 730 1442 763">Document type</td> <td data-bbox="1442 730 1476 763"></td> </tr> <tr> <td data-bbox="799 763 1442 797">Document number</td> <td data-bbox="1442 763 1476 797"></td> </tr> <tr> <td data-bbox="799 797 1442 831">Issuing country and authority</td> <td data-bbox="1442 797 1476 831"></td> </tr> <tr> <td data-bbox="799 831 1442 864">Date of issue</td> <td data-bbox="1442 831 1476 864"></td> </tr> <tr> <td data-bbox="799 864 1442 898">Date of expiry</td> <td data-bbox="1442 864 1476 898"></td> </tr> </table>	Document type		Document number		Issuing country and authority		Date of issue		Date of expiry	
Document type											
Document number											
Issuing country and authority											
Date of issue											
Date of expiry											
<b>Nõusolekud ja kinnitused:</b> <input type="checkbox"/> Kinnitan andmete õigsust ja olen teadlik tagajärgedest valeandmete esitamise eest. <input type="checkbox"/> Kinnitan, et ei ole seotud järgmiste tegevusaladega: ravimite müük; erootika ja täiskasvanute kaupade müük; tutvumisteenused; e-sigarettide ja tubakatoodete müük; privaat- ja personaalpangandus; valuutavahetus ja Forex trading; väärismetalli ja –kivide ost-müük; relvade ost-müük; pandimajad; äriühingud, kes pakuvad piiriülese sularaha ja väärtpaberite vedamise teenust; igasugune muu illegaalne tegevusvaldkond. <input type="checkbox"/> Nõustun andmete kogumise, töötlemise ja säilitamisega Aqdigital OÜ tingimustel. <input type="checkbox"/> Kinnitan, et sooritan identifikatsiooniprotseduurid isiklikult. <input type="checkbox"/> Nõustun Eesti õigusnormide kohaldamisega seoses identifikatsiooniprotseduuridega.	Documents additionally submitted: <input type="checkbox"/> selfie <input type="checkbox"/> selfie with the document and paper on which the date is indicated <input type="checkbox"/> proof of residential address <input type="checkbox"/> proof of funds <input type="checkbox"/> bank account statement <input type="checkbox"/> proof of beneficial owner <input type="checkbox"/> other document  <b>Consents and warranties:</b> <input type="checkbox"/> I certify that the data are correct and I am aware of the consequences of giving false information. <input type="checkbox"/> I confirm that I am not engaged in the following areas of activity: sale of medicinal products; sale of erotic and adult goods; dating services; sale of e-cigarettes and tobacco products; private and personal banking; currency exchange and Forex trading; purchase and sale of precious metals and stones; purchase and sale of weapons; pawnshops; companies that provide cross-border transportation of cash and securities; any other illegal area of activity. <input type="checkbox"/> I give my consent to the collection, processing and retention of data under the terms of Aqdigital OÜ. <input type="checkbox"/> I confirm that I complete the identification procedures in person. <input type="checkbox"/> I give my consent to the application of Estonian legislation to the identification process.										

LISA 3. RISKIPROFIILI MÄÄRAMISE JA HOOLSUSKOHUSTUSE RAKENDAMISE TABEL

(TIER'S SYSTEM AND DD MEASURES DISCRPTION)

	1 Tase (madal risk, lihtsustatud DD)	2 Tase (keskmine risk, täiustatud DD)	3 Tase (suur risk, täiustatud DD)	Keelatud/piiratud
Kriteeriumid				
Tehingu summa (igakuine)	0-15 000 EUR	15 001 – 50 000 EUR	Üle 50 001 EUR	Piirangud pole
Tehingu summa aastamäär	Kuni 15 000 EUR	Kuni 100 000 EUR	Üle 100 001 EUR	Piirangud pole
Elukohariik	EU ja EEA	Teised riigid, v.a kõrge riskiga riigid	Teised riigid, v.a kõrge riskiga riigid	Kõrge riskiga riigid
Kodakondsus	EU+ EEA	Teised riigid, v.a kõrge riskiga riigid	Teised riigid, v.a kõrge riskiga riigid	Kõrge riskiga riigid
Pikaajaline leping (kestvusleping)	Jah	Jah	Jah	Piirangud pole
Maksimale pangakonto/krediitkaardiga	Jah	Jah	Jah	Ei (sularah)
PEP	Ei	Ei	Jah	Piirangud pole
Sanktsioonid	Ei	Ei	Ei	Jah
Teave UBO kohta on avalikult kättesaadav	Jah	Ei	Ei	Piirangud pole
Hooldsuskoostuse meetmed ja kogutud teave				
Kliendi ankeet	Jah	Jah	Jah	Kui ei, siis on

ANNEX 3. TABLE FOR RISK PROFILE DETERMINATION AND APPLICATION OF DUE DILIGENCE DUTY (TIER'S SYSTEM AND DD MEASURES DISCRPTION)

	Tier 1 (low risk, simplified DD)	Tier 2 (medium risk, enhanced DD)	Tier 3 (high risk, enhanced DD)	Forbidden/Restricted
Criteria				
Transaction amount (monthly)	0-15 000 EUR	15 001 – 50 000 EUR	Over 50 001 EUR	No limits
Transaction amount annually	Up to 15 000 EUR	Up to 100 000 EUR	Over 100 001 EUR	No limits
Country of residency	EU and EEA	Other countries, excl. high risk countries	Other countries, excl. high risk countries	High risk countries
Citizenship	EU+ EEA	Other countries, excl. high risk countries	Other countries, excl. high risk countries	High risk countries
Long-term contract	Yes	Yes	Yes	No limits
Payment via bank account/credit card	Yes	Yes	Yes	No (cash)
PEP	No	No	Yes	No limits
Sanctions	No	No	No	Yes
Information about UBO is publicly available	Yes	No	No	No limits
Due diligence measures and collected information				

<p><u>(Eraisikut</u> <u>ele:</u> ees- ja perekonn animi, kodakond sus, elukoha aadress, sünnikoh t, sünniaeg 18+, e- post, kahtlustu seta kutsealal mitteosal emise kinnitus</p> <p><u>Ettevõtte</u> <u>le:</u> Nimi, registriko od, aadress, asukoht (riik), e- post, ärivaldko nd, andmed juhatuse liikme või muu ettevõtte esindaja kohta (sama, mis eraisikute puhul), äripartne rluse asutuse eesmärk</p>				<p>tehing keelatu d.</p>	<p>Client's questionair e <u>(FOR the individuals:</u> name, surname, citizenship, residential address, place of birth, date of birth 18+, e- mail, confirmatio n of non participatio n of suspicion professions</p> <p><u>FOR the company:</u> Name, registry code, address, place of establishm ent (country), e-mail, business field, data about member of the board or other company representa tive person (the same as for individuals) , aim of the business partnership establishm ent</p>	Yes	Yes	Yes	If no, the transacti on is prohibite d
<p>Dokumen di koopia (äriühing ute puhul registrika art)</p>	Jah	Jah	Jah, vajadus el notariaa lselt tõestatu d	Kui ei, siis on tehing keelatu d.	Copy of the document (registry card for the companies)	Yes	Yes	Yes, notariz ed if necess ary	If no, the transacti on is prohibite d
<p>Selfie</p>	Jah	Jah	Jah	Kui ei, siis on tehing keelatu d.	Selfie	Yes	Yes	Yes	If no, the transacti on is prohibite d
<p>Selfie + kuupäeva</p>	Jah	Jah	Jah	Kui ei, siis on					

+ dokument				tehing keelatud.	Selfie + date + document	Yes	Yes	Yes	If no, the transaction is prohibited
“Liveness” kontroll	Jah	Jah	Jah	Kui ei, siis on tehing keelatud.	Liveness check	Yes	Yes	Yes	If no, the transaction is prohibited
Video verifitseerimine	Ei	Jah	Jah	Kui ei, siis on tehing keelatud.	Video interview	No	Yes	Yes	If no, the transaction is prohibited
<i>Elukoha aadressi tõend</i> Elukoha aadressi tõendamise, kui riigis on keskne registreerimissüsteem, registreerimistunnistus VÕI värsked kommunaalmaksed 3 kuu kohta VÕI pangaväljavõtte 3 kuu kohta aadressiga, mis ei ole vanem kui 3 kuud	Ei	Jah, üks võimalus test	Jah, üks valikud tõend selle kohta, et resident uur+ pank Avaldus	Kui ei, siis on tehing keelatud.	<i>Proof of residential address, if there is a central enrollment system in the country, a certificate of enrollment OR fresh utility bill payments for 3 months OR bank statement for 3 months with the address not older than 3 months</i>	No	Yes, one of the options	Yes, one of the options of proof of residency+ bank statement	If no, the transaction is prohibited
<i>tõend rahaliste vahendite kohta</i> 1. mis tahes tõendid mis kinnitavad, tehingus kasutatud vahendite päritolu nt: müügileping, laen,	Ei, ainult siis, kui teil on kahtlusi (ebatavaline tehing selle kliendi jaoks)	Jah, üks võimalus test.	Jah, üks võimalus (vajadusel mõlemaid)	Kui ei, siis on tehing keelatud.	<i>proof of funds</i> 1. any proof of sustaining the transaction's amount : proof of sale, loan, mortgage or insurance payout documents etc. OR 2. fresh bank statement	No, only if have any doubt (unusual transaction for this client)	Yes, one of the options	Yes, one of the options (both if needed)	If no, the transaction is prohibited



hüpoteek või kindlustuse väljamakse dokumendid jne VÕI 2. värsk pangakon to väljavõte 3 kuu kohta					for 3 months				
UBO tõend	Ei (andmed peaksid olema kättesaadavad)	Jah, kui teave ei ole kättesaadav	Jah, kui teave ei ole kättesaadav (vajadusel notariaalselt tõestatud)	Kui andmeid ei esitata või ei ole võimalik UBO-d kontrollida ja tuvastada, on tehing keelatud.	Proof of UBO	No (data should be available)	Yes, if the information is not publicly available	Yes, if the information is not publicly available (notarized if needed)	If data is not provided or impossible to control and identify the UBO, the transaction is prohibited
PEP kontroll	Jah	Jah	Jah	Peaks kehtima igale kliendile, kui kontrolli ei läbita, on tehing keelatud	PEP check	Yes	Yes	Yes	Should be applicable to every client, if the check is not passed, the transaction is prohibited
Sanktsioonide kontroll	Jah	Jah	Jah	Peaks kehtima igale kliendile, kui kontrolli ei läbita, on tehing keelatud	Sanctions check	Yes	Yes	Yes	Should be applicable to every client, if the check is not passed, the transaction is prohibited
Andmete värskendamine	Üks kord kahe aasta jooksul	Kord aastas	Kaks korda aastas	-	Data update	Once per 2 years	Once a year	Twice a year	-

LISA 4. KÕRGE RISKIGA RIIKIDE NIMEKIRI  
(RISKIRIIGID)

alates 13.06.2022

*Tehingute tegemine ja ärisuhte loomine on keelatud*

1	Afganistan
2	Alzeeria
3	Araabia Ühendemiraadid
4	Burkino Faso
5	Egiptus
6	Iraak
7	Iraan
8	Jeemen
9	Jordaania
10	Kongo Demokraatlik Vabariik
11	Liibanon
12	Liibüa
13	Lõuna Sudaan
14	Mali
15	Maroko
16	Mosambiik
17	Nigeria
18	Niger
19	Pakistan
20	Palestiina omavalitsus
21	Korea Demokraatlik Vabariik (Põhja Korea)
22	Saudi Araabia
23	Venemaa Föderatsiooni Põhja Kaukaasia föderaalringkond
24	Somaalia
25	Sudaan
26	Krimi piirkond

ANNEX 4. LIST OF HIGH-RISK  
COUNTRIES (RISK COUNTRIES)

from 13.06.2022

*It is forbidden to make transactions or establish a business relationship*

1	Afghanistan
2	Algeria
3	United Arab Emirates
4	Burkina Faso
5	Egypt
6	Iraq
7	Iran
8	Yemen
9	Jordan
10	Democratic Republic of Congo
11	Lebanon
12	Libya
13	South Sudan
14	Mali
15	Morocco
16	Mozambique
17	Nigeria
18	Niger
19	Pakistan
20	Palestinian Authority
21	Democratic Republic of Korea (North Korea)
22	Saudi Arabia
23	Federal District of the North Caucasus of the Russian Federation
24	Somalia
25	Sudan
26	Crimea region

<sup>15</sup> FATF monitored jurisdictions <http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2020.html>

<sup>16</sup> EU high-risk countries <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R0855>

<sup>17</sup> FATF call for action countries <http://www.fatf-gafi.org/countries/#high-risk>

## LISA 5. AQDIGITAL OÜ HUVIDE KONFLIKTI ENNETAMISE TEATIS

Kinnitatud 25.11.2022

### 1. Huvide konflikti määratlus

- 1.1. Huvide konflikt on vastuolu isiku erahuvide ja ametikohustuste vahel või ametialaste huvide vahel, kui isikul on mitu ametikohta, mis võib mõjutada volituste kohusetundlikku täitmist ning objektiivsust ja erapooletust otsuste tegemisel. Huvide konflikt võib olla tegelik või võimalik.
- 1.2. Tegelik huvide konflikt on huvide konflikt, mis mõjutab otsuste tegemise objektiivsust või erapooletust või teatud tegevuste sooritamist või sooritamata jätmist.
- 1.3. Võimalik huvide konflikt tähendab, et ametikohustusi täitval isikul on isiklik või ametialane huvi, mis võib tulevikus teatud tingimustes mõjutada otsuste tegemise objektiivsust või erapooletust või teatud tegevuste sooritamist või sooritamata jätmist.
- 1.4. Eeldatakse, et juhatuse liikmel, järelevalveametnikul või töötajal on suhe, mis võib põhjustada huvide konflikti, kui olukord hõlmab:
  - 1) ärisuhteid (nt võlgniku, võlausaldaja, partneriga):
    - mis tahes üksusega, mis omab äritegevust ettevõttega;
    - mis tahes üksusega, mis konkureerib ettevõttega ja millel on vastupidised huvid;
    - teiste juhatuse liikmete, järelevalveametnikega või töötajatega;
    - mis tahes äriühingu klientidega;
  - 2) peresuhteid:
    - mis tahes üksuses, mis omab äritegevust ettevõttega;
    - mis tahes üksuses, mis konkureerib ettevõttega ja millel on vastupidised huvid;
    - teiste juhatuse liikmete, järelevalveametnikega või töötajatega;
    - mis tahes äriühingu klientidega;
  - 3) kingituste vastuvõtmist või tegemist ametikohustuste täitmise tõttu või selle käigus.

### 2. Huvide konflikti ennetamise meetmed

- 2.1. Tegelike ja võimalike huvide konfliktide õigeaegseks tuvastamiseks ning õigeaegse ennetamise ja tõhusa lahendamise tagamiseks soovatakse igal juhatuse liikmel, järelevalveametnikul ja töötajal teha regulaarselt enesehindamisi ning tegelike ja võimalike huvide konfliktide tuvastamisel tuleb esitada asjakohane deklaratsioon tegeliku või võimaliku huvide konflikti olemasolu (puudumise) kohta (lisa 5.1). Järelevalveametnik ja töötaja peab deklaratsiooni esitama juhatuse liikmele. Juhatuse liige peab deklaratsiooni esitama teisele juhatuse liikmele või tegema ühepoolse avalduse.
- 2.2. Enesehindamine on kohustuslik järgmistel juhtudel:
  - muutused volituste/kohustuste ulatuses;
  - uued asjaolud, mis võivad mõjutada otsuste objektiivsust või erapooletust.
- 2.3. Järelevalveametnik ega töötajad ei tohi osaleda tegevuses, mis võib põhjustada konflikti ettevõtte huvidega või mida võib pidada selliseks konfliktiks. Samuti ei tohi järelevalveametnik ega töötajad olla otseselt või kaudselt pereliikme või muu nende nimel tegutseva isiku kaudu olla sellise tegevusega seotud.
- 2.4. Kui on vaja kasutada füüsilise või juriidilise isiku teenuseid, tuleb tagada, et selle füüsilise või juriidilise isiku ja ettevõtte vahel ei ole huvide konflikti.
- 2.5. Võimalike ja tegelike huvide konfliktide ennetamiseks ja tuvastamiseks, mis võivad ettevõtte äritegevust piisavalt mõjutada, jälgib ettevõtte võimalikke ja tegelikke huvide konflikte juhatuse liikmete ja järelevalveametniku iga-aastaste deklaratsioonide kaudu:
  - 1) juhatuse liikmete poolt – jälgitakse selliste asjaolude olemasolu, mis võivad põhjustada võimalikku/tegelikku huvide konflikti; jälgitakse juriidilistes isikutes omandiõigust, mis ületab 20%;
  - 2) järelevalveametniku poolt – jälgitakse asjaolusid, mis võivad põhjustada võimalikku/tegelikku huvide konflikti.
- 2.6. Iga juhatuse liige, järelevalveametnik ja töötaja peab siinse huvide konflikti ennetamise teatise läbi lugema ja seda mõistma.

### 3. Huvide konfliktide haldamine

3.1. Juhatus liige on kohustatud olukorda tõhusalt lahendama. Selleks peab ta:

- 1) haldama teavet konfidentsiaalselt ja erapooletult;
  - 2) hindama teatatud olukorda õiglaselt ja määrama, kas selline olukord on huvide konflikt (tegelik või võimalik);
  - 3) juhul, kui teatatud olukorda ei peeta huvide konfliktiks, selgitama ja põhjendama, miks sellisele järeldusele jõuti;
  - 4) juhul, kui jõutakse järeldusele, et tegemist on huvide konfliktiga, selgitama ja põhjendama järeldust ning koostama koos deklareeriva isikuga tegevuskava konflikti lahendamiseks. Tegevuskava võib:
    - tagada, et juhatuse liige, järelevalveametnik või töötaja ei ole seotud mis tahes küsimustega, mida on seostatud avalikustatud huvide konfliktiga;
    - rakendada leevendavaid meetmeid.
- Kui huvide konflikti ei ole võimalik muul viisil leevendada või lahendada:
- määrake juhatuse liikme, järelevalveametniku või töötaja ülesandeks mõni teine ülesanne selles valdkonnas;
  - tehke ettepanek töötaja üleviimiseks teise valdkonda;
  - leidke asendaja juhatuse liikmele või järelevalveametnikule;
  - palgake juurde juhatuse liige, järelevalveametnik või töötaja;
- rakendage muid mõistlikke meetmeid olukorra käsitlemiseks;
- koostage tegevuskava ja edastage see isikule, kes on huvide konfliktis;
- kui huvide konflikt on seotud ettevõtte kliendiga ja ettevõtte huvide konflikti lahendamise meetmed ei ole piisavad, et kõrvaldada kliendi huvide kahjustamise risk, avalikustab ettevõtte kliendile selle huvide konflikti ja meetmed, mida võidakse rakendada nende riskide vähendamiseks. Teatis esitatakse kliendile kirjalikult.

## ANNEX 5. AQDIGITAL OÜ CONFLICT OF INTEREST PREVENTION NOTICE

Approved 25.11.2022

### 1. Conflict of Interest Definition

- 1.1. A conflict of interests means conflict between a person's personal interests and professional duties or between different professional interests if a person holds several positions, which may affect conscientious performance of powers, objectivity and impartiality in decision-making. Conflict of interest can be real or potential.
- 1.2. A real conflict of interest means a conflict of interest, which affects the objectivity or impartiality of decision-making, or the performance or non-performance of certain actions.
- 1.3. A potential conflict of interest means the presence of a private or professional interest in a person endowed with professional duties, which may, under certain circumstances, in the future affect the objectivity or impartiality of decision-making or the performance or non-performance of certain actions.
- 1.4. It will be presumed that a Member of the board, Compliance officer, Staff has a relationship that can generate a conflict of interest when the situation involves:
  - 1) Commercial relationships (e.g.: debtor, creditor, partner):
    - with any entity that holds business activities with the Company.
    - with any entity that competes with and has opposite interests to those of the Company.
    - with other Members of the board, Compliance officers or members of Staff.
    - with any of the Company's customers.
  - 2) Family members:
    - in any entity that holds business activities with the Company.
    - in any entity that competes with and has opposite interests to those of the Company.
    - with other Members of the board, Compliance officers or members of the Staff.
    - with any of the Company's customers.
  - 3) Receiving or giving gifts as a reason of or in the course of the performance of his/her professional duties.

### 2. Measures to Prevent Conflict of Interests

- 2.1. For the timely identification of real and potential conflicts of interest and in order to ensure timely prevention and effective resolution of conflicts of interest, periodic self-assessment is recommended for each Member of the board, Compliance officer, Staff member, and in the case of detection of real and potential conflicts, it is required to submit an appropriate declaration about the presence (absence) of a real or potential conflict of interests (Annex 5.1). Compliance officer and Staff member must submit such declaration to Member of the board. Member of the board must submit declaration to another Member of the board or make a unilateral statement.
- 2.2. Self-assessment is mandatory in the event of:
  - changes in the scope of powers/duties;
  - new circumstances that may affect the objectivity or impartiality of decisions or actions.
- 2.3. Compliance officer, Staff members must not engage in activities which may lead to a conflict with the interests of the Company or may be considered as such a conflict. Also, Compliance officer, Staff must not be involved in such activities directly or indirectly, through a family member or other person acting on their behalf.
- 2.4. When there is a need to use the services of a natural person or legal entity, it should be ensured that there is no conflict of interest between this natural person or legal entity and the Company.
- 2.5. In order to prevent and identify potential and real conflicts of interest which may sufficiently affect Company business, the Company monitors potential and real conflicts of interest among Member of the board and Compliance officer through annual declarations:
  - 1) by Members of the board - regarding the existence of circumstances that may cause a potential/real conflict of interests; regarding ownership in legal persons which exceeds 20%.
  - 2) by Compliance officer - regarding the existence of circumstances that may cause a potential/real conflict of interests.
- 2.6. Every Member of the board, Compliance officer, Staff member must read and understand this Conflict of Interest Prevention Notice.

### 3. Managing Conflict of Interest

- 3.1. Member of the board is required to effectively address the situation. To do so, he/she must:
- 1) Manage the information in a confidential and unbiased manner.
  - 2) Evaluate the situation reported in a fair manner and determine if such situation is a conflict of interest (real or potential).
  - 3) If the situation reported is not considered a conflict of interest, explain it giving the reasons why that conclusion was reached.
  - 4) If the conclusion reached is that the case is a conflict of interest, explain it giving the reasons for that conclusion and outline an action plan with the declaring person to solve the conflict. The action plan may:
    - Ensure that Member of the board, Compliance officer or Staff member will not be involved in any matters related to the conflict of interest disclosed.
    - Implement mitigating controls.
    - If the conflict of interest cannot be otherwise mitigated or solved:
      - Assign Member of the board, Compliance officer or Staff member to another function within the area.
      - Propose the transfer of Staff member to another area.
      - Find a replacement for Member of the board, Compliance officer.
      - Hire additional Member of the board, Compliance officer, Staff member.
    - Implement other reasonable measures to approach the situation.
    - Set out an action plan and communicate it to the person who is in conflict of interest.
    - If conflict of interest is related to Company's customer and measures taken by the Company to manage conflicts of interest are not sufficient to ensure that the risk of harm to the customer's interests will be eliminated, the Company shall clearly disclose to the customer this conflict of interest and measures which may be taken to mitigate these risks. The notice shall be provided to the customer in writing.

