WAWLLET

WAWLLET GENERAL TERMS AND CONDITIONS

Last changed: 14th of March 2019

READ THESE TERMS AND CONDITIONS ("TERMS") CAREFULLY BEFORE USING THE SERVICES DESCRIBED HEREIN. BY UTILIZING THE WEBSITE LOCATED AT www.wawllet.com ("WEBSITE") AND PRODUCTS OFFERED THEREIN, YOU ACKNOWLEDGE THAT YOU HAVE READ THESE TERMS AND CONDITIONS AND THAT YOU AGREE TO BE BOUND BY THEM. IF YOU DO NOT AGREE TO ALL OF THE TERMS STATED HEREIN, YOU ARE NOT AN AUTHORIZED USER OF THESE SERVICES AND YOU SHOULD NOT USE THIS WEBSITE OR ITS PRODUCTS. YOU MAY BE REFERRED TO YOU OR THE ENTITY YOU REPRESENT. YOU ACKNOWLEDGE THAT YOU HAVE READ THE WAWLLET ANTI-MONEY LAUNDERING POLICY AND THAT YOU AGREE TO BE BOUND BY IT. WAWLLET LIMITED (“WAWLLET”) RESERVES THE RIGHT TO CHANGE, MODIFY, ADD, OR REMOVE PORTIONS OF THESE TERMS AT ANY TIME FOR ANY REASON. WE SUGGEST THAT YOU REVIEW THESE TERMS PERIODICALLY FOR CHANGES. SUCH CHANGES SHALL BE EFFECTIVE IMMEDIATELY UPON POSTING. YOU ACKNOWLEDGE THAT BY ACCESSING OUR WEBSITE OR OUR PRODUCTS/SERVICES AFTER WE HAVE POSTED CHANGES TO THESE TERMS, YOU ARE AGREEING TO THE MODIFIED TERMS. THIS DOCUMENT OR ANY OTHER DOCUMENT PRODUCED AND SIGNED BY WAWLLET DOES NOT CONSTITUTE AN OFFER OR SOLICITATION TO SELL SHARES OR SECURITIES IN WAWLLET OR THE WEBSITE OR THE PRODUCTS OFFERED THERETO. NONE OF THE INFORMATION OR ANALYSES PRESENTED ARE INTENDED TO FORM THE BASIS FOR ANY INVESTMENT DECISION, AND NO SPECIFIC RECOMMENDATIONS ARE INTENDED, AND WAWLLET SERVICES AND THE WEBSITE ARE NOT, DO NOT OFFER, AND SHALL NOT BE CONSTRUED AS INVESTMENT OR FINANCIAL PRODUCTS, BUT AS A SOFTWARE APPLICATION. ACCORDINGLY, THIS DOCUMENT DOES NOT CONSTITUTE INVESTMENT ADVICE OR COUNSEL OR SOLICITATION FOR INVESTMENT IN ANY SECURITY AND SHALL NOT BE CONSTRUED IN THAT WAY. THIS DOCUMENT DOES NOT CONSTITUTE OR FORM PART OF, AND SHOULD NOT BE CONSTRUED AS, ANY OFFER FOR SALE OR SUBSCRIPTION OF, OR ANY INVITATION TO OFFER TO BUY OR SUBSCRIBE FOR, ANY SECURITIES, WAWLLET PRODUCTS INCLUDED. WAWLLET EXPRESSLY DISCLAIMS ANY AND ALL RESPONSIBILITY FOR ANY DIRECT OR CONSEQUENTIAL LOSS OR DAMAGE OF ANY KIND WHATSOEVER ARISING DIRECTLY OR INDIRECTLY FROM: (I) RELIANCE ON ANY INFORMATION CONTAINED IN THIS DOCUMENT, (II) ANY ERROR, OMISSION OR INACCURACY IN ANY SUCH INFORMATION, (III) ANY ACTION RESULTING THEREFROM, OR WAWLLET GENERAL TERMS AND CONDITIONS (IV) USAGE OR ACQUISITION OF PRODUCTS AVAILABLE THROUGH THE WEBSITE.

1. TERMS

1.1 The following terms shall have for the purposes of these General Terms and Conditions the following meanings.

(a) “Digital Portfolio Experts” or “Experts” shall have the meaning, set out in 4.1.

(b) “Digital Portfolio” shall have the meaning set out in 2.1(b) and 2.3.

(c) “Digital Assets” are cryptocurrencies and tokens available in a particular public blockchain network that are accepted by the Platform, such as but not limited to Bitcoin, Ethereum, Monero, Dash, Binance Coin and WCOIN. WAWLLET may from time to time without argumentation and in full discretion add or

remove particular cryptocurrencies or tokens from this list without the need to change these Terms ("Digital Assets" are also referred to for marketing purposes as "Cryptocurrencies" as a commonly interchangeable term for Digital Assets).

(d) "European Economic Area" or "EEA" shall mean all EU countries as well as Iceland, Liechtenstein, and Norway.

(e) "Fee Schedule" shall have the meaning set out in 7.3.

(f) "WAWLLET IP" shall have the meaning set out in 14.4.

(g) "WAWLLET Wallet" means a software solution and a service integrated into the Platform that enables users to store Digital Assets. An WAWLLET Wallet is required for the acquisition of Digital Assets.

(h) "WAWLLET" means a group of companies:

i. WAWLLET ENTERPRISES HQ Limited, a company registered in Ireland, under the company number 636739, 8-9 Marino Mart, Fairview, Ground Floor, Clontarf D03 P590, Ireland, a company which is holding the IP rights and is responsible for managing the entire WAWLLET project, as well as developing the core app.

ii. WAWLLET ENTERPRISES OU, a company registered in Estonia, under the company number 14549617, Harju maakond, Kesklinna linnaosa, Roosikrantsi tn 2, Tallinn, 10119, a company which is operating the WAWLLET platform under the virtual wallet service license no. FRK000349, granted at 24.09.2018 and under the virtual exchange service license no. FVR000428, granted at 24.092018.

(j) "Platform" shall have the meaning set out in 2.1(b) and 2.2. (l) "Restricted Areas" shall have the meaning set out in 8.1.

(k) "Terms" means these General Terms and Conditions.

(l) A "Third-party Wallet" is a software solution enabling users to store their Digital Assets that is not hosted by WAWLLET or on the Platform.

(m) "End user" or "User" is a user of any WAWLLET product, including WAWLLET's Digital Assets Management Platform.

(n) "VAT" means the value added tax of a jurisdiction, if applicable.

(o) "Website" shall mean www.WAWLLET.com.

2. PRODUCTS AND SERVICES

2.1 General

(a) WAWLLET offers a number of products and services, which are published on the Website. WAWLLET products and services can be changed and altered from time to time, and these Terms shall apply to all of them, unless stated otherwise in these Terms, on the Website, or in the documentation

accompanying a particular product or service. These Terms apply also to WAWLLET products and services offered, launched, or made public after publication of these Terms.

(b) WAWLLET's main product is the "Digital Assets Management Platform" (the "Platform"). Within the Platform, several Digital Portfolios may be available as products, as well as various other products and services, all accessible through the Website.

2.2 Digital Assets Management platform

(a) The Digital Asset Management platform is a software platform consisting of a webpage interface, a software interface for communication between the Website, 3rd parties and blockchain networks, all developed by WAWLLET ENTERPROSES HQ LIMITED and operated and offered by WAWLLET ENTERPRISES OU through the Website. It enables creation, management, sharing with other users, and comparison of different Digital Portfolios, as well as the investing in Digital Portfolios and acquisition of different cryptocurrencies and tokens or other financial services offered in partnership with 3rd parties according to their terms and conditions.

(b) The Platform operates 24/7, subject to certain limitations, such as the limitation of cryptocurrencies and tokens held in hot wallets (meaning being liquid) and per-session trading limitations, as well as unforeseeable technical and network issues.

(c) The management of Digital Portfolios is advised by the Experts for each particular Digital Portfolio.

2.3 Digital Portfolio

(a) A Digital Portfolio is a cryptographic token solution developed by WAWLLET ENTERPRISES HQ LIMITED that operates on the public blockchain.

(b) A Digital Portfolio can be custom designed for a wide range of purposes. A Digital Portfolio can include a number of Digital Assets. Consequently, its main feature is that it saves time and transaction costs for those users who wish to obtain cryptographic tokens of different Digital Assets (public blockchains).

(c) For the purpose of these Terms, Digital Assets are cryptocurrencies and tokens existing in any blockchain that are available to the users.

(d) Users can invest in Digital Portfolios through the Platform. The Platform was designed to be simple and user friendly and does not require the WAWLLET GENERAL TERMS AND CONDITIONS advanced technical knowledge that would otherwise be required for direct acquisition of multiple Digital Assets.
(e) The sole purpose of the Platform and its solutions (namely Digital Portfolios) is to provide a platform on which external Experts advise WAWLLET on operation of Digital Portfolios. Whenever a respective Expert's status is revoked, WAWLLET will take all necessary measures to safeguard all end users' rights and interests, if there is a need for that.

2.4 Exchange

(a) WAWLLET enables it's users to buy or sell certain cryptocurrencies, tokens and Digital Portfolios on the WAWLLET Platform through the exchange service operated and provided by several 3rd parties.

(b) The exchange service is offered under the conditions, including but not limited to:

(i) Fiat funds can only be transferred in euros to or from the SEPA (Single Euro Payments Area) bank account held in the name of the user buying or selling Digital Assets or Digital Portfolio.

(ii) Available payment methods at any time are listed on the WAWLLET Website and may depend on various factors, including but not limited to, user's location, provided identification information, and limitations imposed by the payment processors involved.

(iii) The service is offered only to users verified to Tier 2, which have passed the KYC process.

(iv) WAWLLET reserves the right to perform additional checks and to require additional information and documents under applicable anti-money laundering regulations.

(v) WAWLLET or its 3rd parties do not guarantee the availability of any exchange rate quoted on the Website.

(vi) The user acknowledges that the buy price exchange rate may not be the same as the sell price exchange rate at any given time, and that WAWLLET or its 3rd parties may add a margin or spread to the quoted exchange rate.

2.5 A Digital Portfolio is not an investment product, and any action, notice, communication, message, decision, managerial act, or omission of the mentioned is not an investment advice and shall not be understood and interpreted as such. Any such content provided by WAWLLET or a third-party Expert either by integration in the Digital Portfolio source code or by publishing through any means of communication shall be regarded solely as a statement of facts or observation and in no case as investment advice. A Digital Portfolio is not a security. WAWLLET gives no guarantees as to the value of any of the Digital Portfolios and explicitly warns users that there is no reason to believe that Digital Portfolios will increase in value, and that they might decrease in value or lose their value entirely.

2.6 You agree and accept that you are acquiring Digital Portfolios for your own personal use as a technical means for acquiring tokens from different blockchains simultaneously and for your personal utility, and not for investment or financial purposes. You also agree that you do not consider Digital Portfolios a security and you understand that Digital Portfolios may lose all their value.

2.7 This document or any other document produced and signed by WAWLLET or any of third-party Experts, the Website, or Digital Portfolios do not constitute an offer or solicitation to sell and shall not be construed in this way, and may only be construed as an invitation to offer, in all cases, the purchase of Digital Portfolios as software solutions.

2.8 Digital Portfolios are not cryptocurrency, regardless of the legal meaning the word "cryptocurrency" has, unless and to the extent that the meaning of Digital Portfolios are described and defined by these Terms.

2.9 Particular Digital Portfolios managed by third-party Experts may be in some aspects provided to the users under terms different from these Terms. Should this be the case, any deviation from these Terms will be explicitly written in a visible spot at the point of investment in such Digital Portfolios.

3. PURCHASING AND SELLING OF DIGITAL PORTFOLIOS AND OTHER DIGITAL ASSETS

3.1 The Platform provides for the possibility of purchasing and selling of Digital Portfolios. This section 3 applies to:

(a) all purchases and sales of Digital Portfolios via the Website,

(b) any transaction in which you load Digital Portfolios or other Digital Assets into your WAWLLET Wallet from any Third-party Wallet or unload Digital Portfolios or other Digital Assets from your WAWLLET Wallet to a Third-party Wallet.

3.2 You agree to purchase and/or sell of Digital Portfolios by the terms set forth herein. Your transaction is final. We will not provide any refunds or the possibility to reverse an ordered transaction under any circumstances. Once your order has been executed, you may not change, withdraw, or cancel your authorization for WAWLLET to complete your transaction. We reserve the right to refuse any cancellation request associated with an order once you have submitted your order, even if it has not yet been executed.

3.3 When you acquire the Digital Portfolios you agree with the published strategy, applicable terms, and fees of each Digital Portfolio you choose. You also agree and accept that each particular strategy, applicable terms, and fees of the Digital Portfolio may be changed by WAWLLET at any time without any prior notice, whether or not based on advice by each particular Digital Portfolio Expert.

3.4 After confirmation of transactions, Digital Portfolios are automatically transferred from or to your WAWLLET Wallet or, in limited cases, to a Third-party Wallet, should you indicate such in your profile settings.

3.5 WAWLLET does accept, hold, or exchange fiat money for Digital Assets under the conditions as stated in point 2.4. of these Terms. In case you are not eligible for exchange under the point 2.4. of these Terms, you may only fund your WAWLLET account with Digital Assets.

3.6 WAWLLET may, at any time and in its sole discretion, refuse any attempted purchase or sale of Digital Portfolios via the Platform, impose limits on per-session or per-day purchases and sales via the Platform, and impose any other conditions or restrictions upon your use of the Platform and Website without prior notice.

3.7 In order to acquire Digital Portfolios via the Platform, users will first need to deposit fiat money or cryptocurrencies into their WAWLLET Wallet. WAWLLET may from time to time add or remove the ability to deposit different Digital Assets into WAWLLET Wallets.

3.8 Provided that the balance of Digital Assets in your WAWLLET Wallet is net positive, you may convert any amount of Digital Assets in your WAWLLET Wallet to any listed cryptocurrency and withdraw your Digital Assets from your WAWLLET Wallet to a Third-party Wallet. If the Third-party Wallet rejects your Digital Assets or may otherwise be unavailable, you agree that you will not hold WAWLLET liable for any damages resulting from such rejected transactions.

3.9 WAWLLET does not purchase, sell, or exchange any Digital Assets on its own behalf.

3.10 When you submit an order for the purchase or sale of Digital Portfolios via the Platform, you authorize WAWLLET to execute a transaction in accordance with your order on a spot basis and to charge you any applicable fees.

3.11 You acknowledge and agree that:

(a) WAWLLET is not acting as your broker, intermediary, agent, or advisor or in any fiduciary capacity, and

(b) no communication or information provided to you by WAWLLET shall be considered or construed as advice or investment advice.

(c) you hold all the private keys and you are fully responsible of keeping them secured and operate them properly.

3.12 Particularly during periods of high volume, illiquidity, fast movement, or volatility in the marketplace for any Digital Asset or Digital Portfolio, the price of Digital Assets or Digital Portfolios may be different from the prevailing rate indicated on the Platform at the time your order is submitted. You understand that we are not liable for any such price fluctuations. In the event of a market disruption or force majeure event, WAWLLET may do one or more of the following:

(a) suspend access to the Platform;

(b) prevent you from completing any actions via the Platform.

4. STATUS OF DIGITAL PORTFOLIO EXPERTS

4.1 Digital Portfolios, available through the Platform, are NOT managed by WAWLLET. Third parties, not in any way related to WAWLLET ("Digital Portfolio Experts"), advise regarding the structure, time of rebalancing, and other characteristics of the Digital Portfolios. Experts are bound by the General Terms and Conditions for Digital Portfolio Experts prepared by WAWLLET.

4.2 Experts may provide certain content on the Platform, such as a brief description of the Digital Portfolio in regards to which they are advising WAWLLET and links to their webpages or to third-party webpages.

4.3 WAWLLET has discretionary powers to decide who can be awarded Digital Portfolio Expert status. WAWLLET follows its internal rules and policies and has no duty to explain its decisions regarding the appointment of Digital Portfolio Experts.

4.4 We do not control, endorse, or adopt any third-party content, including content generated and published by Experts. We shall have no responsibility for such content, including without limitation material that may be misleading, incomplete, erroneous, offensive, indecent, or otherwise objectionable. In addition, your business dealings and correspondence with Experts are solely between you and the Experts. We are not responsible or liable for any loss or damage of any sort incurred as the result of any such dealings, and you understand that your use of content generated by Experts, purchase or sale of respective Digital Portfolios, and any of your interactions with Experts are at your own risk.

4.5 Experts advise WAWLLET regarding the content and specification of a particular Digital Portfolio.

4.6 WAWLLET gives no guarantees or warranties, expressed or implied, regarding the advice or other actions or absence of advice or actions of Experts or the functioning of each particular Digital Portfolio.

Experts are independent third parties and are not related to WAWLLET or its affiliates. WAWLLET shall not be held liable for any damages arising out of the actions of Experts.

5. WAWLLET USER ACCOUNT

5.1 In order to use the Platform, you must create a user account at www.WAWLLET.com, by downloading the APP. When you create an WAWLLET account, you agree to:

a) these Terms;

b) create a strong password;

c) provide accurate and truthful information;

d) maintain and promptly update your information;

e) maintain the security of your account by protecting your password and restricting access to third parties; and

(f) take responsibility for all activities that occur under your account and accept all risks of any authorized or unauthorized access to your account, to the maximum extent permitted by law.

(g) WAWLLET does NOT hold any private key. You are fully responsible of keeping the private keys and the paper key/SEED safely. In case of losing or destroying your devise WAWLLET is not responsible for your Digital Assets, a recovery of your account couldn't be possible without paper Key/SEED.

5.2 A maximum of one user account per person is NOT allowed. If a user creates more than one account, WAWLLET reserves the right to freeze all accounts of that user and to carry out all necessary actions to merge the accounts into one account or to block the user from the platform in cases of obvious fraudulent activities and/or if the user shall make additional user accounts.

5.3 You must provide any information required when creating an account or when prompted by any screen displayed within the Platform or by a third party. You represent and warrant that any information you provide via the Platform or to a third party is accurate and complete.

5.4 WAWLLET may refuse access to WAWLLET services and the Website should it have doubts as to the accuracy, validity and completeness of information or validity, authenticity, and genuineness of the documents you provide.

5.5 WAWLLET undertakes to strictly apply privacy rules to your personal data, as set out in the WAWLLET Privacy Policy.

6. RISKS

6.1 You understand that Digital Assets, Digital Portfolios, the Platform, blockchain technology, the Ethereum protocol, ether, and other associated and related technologies are new and untested and

outside of WAWLLET's exclusive control. You understand that adverse changes in market forces or the technology, broadly construed, will excuse WAWLLET's performance under these Terms.

6.2 In addition to the above, you also acknowledge that you have been warned of the following risks associated with the Website, the Platform, Digital Portfolios, and other related products.

(a) Legal risks regarding securities regulations There is a risk that Digital Portfolios and other Digital Assets may be considered a security, now or in the future, in some jurisdictions. WAWLLET does not give warranties or guarantees that Digital Portfolios and Digital Assets are not securities in all jurisdictions. Each user of Digital Assets and Digital Portfolios shall bear his or her own legal or financial consequences of Digital Assets and Digital Portfolios being considered a security in their respective jurisdiction. Every user is bound to determine whether the purchase and sale of Digital Assets and Digital Portfolios is legal in his or her jurisdiction. By accepting these Terms, each user undertakes not to use Digital Assets and Digital Portfolios via the Platform should their use not be legal in the relevant jurisdiction. Purchasing cryptocurrencies and cryptographic tokens and exchanging them for other cryptocurrencies and cryptographic tokens will most likely continue to be scrutinized by various regulatory bodies around the world, which have so far had mixed reactions and regulatory impact. The legal ability of WAWLLET to provide Digital Assets and Digital Portfolios in some jurisdictions may be eliminated by future regulation or legal action. In the event that there is a high degree of certainty that Digital Assets and Digital Portfolios are not legal in a particular jurisdiction, WAWLLET will either a) cease operations in that jurisdiction, or b) adjust Digital Assets or Digital Portfolios in a way to comply with the regulation, should that be possible and viable. You understand and accept that each user shall bear the legal or financial consequences that may be incurred in their entirety from any action, inaction, notice, and/or communication related to the actions described herein. Every user understands and accepts that blockchain technology allows new forms of interaction and that it is possible that certain jurisdictions will apply existing regulations on or introduce new regulations addressing blockchain-technology-based applications that may be contrary to the current setup of the Platform and that may, inter alia, impede or limit the development and functionality of the Platform, resulting in substantial modifications of the Platform, including its termination and the loss of funds for the user.

(b) Risks associated with the Ethereum protocol Digital Portfolios are based on the Ethereum protocol. As such, any malfunction, unintended function, or unexpected functioning of the Ethereum protocol may consequently cause Digital Portfolios to malfunction or function in an unexpected or unintended manner. The user understands and accepts that it is possible that the value of ether (ETH), the native unit of account of the Ethereum protocol, will drop significantly in the future and that this may consequently cause Digital Portfolios to lose value. Ether, the native unit of account of the Ethereum protocol, may itself lose value in ways similar to Digital Portfolios, and also in other ways. More information about the Ethereum protocol is available at http://www.ethereum.org.

(c) Risks associated with users' credentials Any third party that gains access to a user's login credentials for the Website or the Platform, or who gains access to the user's private keys, may be able to dispose of the user's Digital Assets and Digital Portfolios. To minimize this risk, the user should guard against unauthorized access to their electronic devices using due diligence, especially the most technologically advanced security devices, up-to-date anti-malware software, and any other means necessary to protect their data connected to their login credentials as well as to the software they use to connect to and use the Website or the Platform. WAWLLET also provides advanced security techniques. Users' login

credentials are their own sole responsibility. WAWLLET shall not be held responsible for any unauthorized access to a user's devices or for any unauthorized access to a user's login credentials. Therefore, WAWLLET shall not be held responsible for any damage or loss resulting from such actions.

(d) Risk of unfavorable regulatory action in one or more jurisdictions Blockchain technologies have been the subject of scrutiny by various regulatory bodies around the world. The functioning of the Ethereum network and associated blockchain networks and Digital Assets and Digital Portfolios could be impacted by one or more regulatory inquiries or actions, including but not limited to restrictions on the use or possession of digital tokens such as Digital Portfolios that could or limit their existence, the permissibility of their use and possession, and their value.

(e) Risk of theft and hacking Hackers or other groups or organizations may attempt to interfere with your WAWLLET wallet or third-party wallet, the Platform, the Website, or the availability of Digital Portfolios and Digital Assets in any number of ways, including without limitation denial of service attacks, Sybil attacks, spoofing, smurfing, malware attacks, or consensus-based attacks.

(f) Risk of security weaknesses in the Platform and Digital Portfolio source code or any associated software and/or infrastructure. There is a risk that the Platform and Digital Portfolios may unintentionally include weaknesses or bugs in the source code interfering with the use of or causing the loss of Digital Portfolios and other Digital Assets.

(g) Risk of weaknesses or exploitable breakthroughs in the field of cryptography Advances in cryptography, or technical advances such as the development of quantum computers, could present risks to cryptocurrencies, the Ethereum platform, or the Platform and Digital Portfolios, which could result in the theft or loss of Digital Portfolios.

(h) Risk of mining attacks As with other decentralized cryptocurrencies, the Ethereum blockchain, which is used for Digital Portfolios, is susceptible to mining attacks, including but not limited to double-spend attacks, majority mining power attacks, "selfish-mining" attacks, and race condition attacks. Any successful attacks present a risk to the Digital Portfolios, the expected proper execution and sequencing of Digital Portfolios, and the expected proper execution and sequencing of Ethereum contract computations in general. Despite the efforts of WAWLLET and the Ethereum Foundation, the risk of known or novel mining attacks remains. Mining attacks, as described above, may also target other blockchain networks with which the Platform and Digital Portfolios interact, and consequently the Platform and Digital Portfolios may be impacted in that way to the extent described above.

(i) Risk of low or no liquidity Even though there are currently online service available that enable the exchange of cryptographic tokens, and some of them enable the exchange of cryptographic tokens for fiat money, there are no warranties and/or guarantees given that Digital Portfolios will be listed or made available for exchange for other cryptographic tokens, and no guarantees are given whatsoever concerning the capacity (volume) of such exchanges. It is explicitly cautioned that such exchange, if any, may be subject to poorly understood regulatory oversight, and WAWLLET does not give any warranties in regard to any exchange service providers. Users may be exposed to fraud and failure. WAWLLET and the Platform will be able to exchange Digital Assets for fiat currency under the condition as stated in point 2.4. of these Terms. Users may not at any given time be able to purchase or sell of their Digital Portfolios via the Platform due to lack of liquidity.

(j) Risk of loss of value As per the high volatility of the value of Digital Assets, their value might fluctuate unfavorably, which may consequently affect the value of the Digital Portfolios that are linked to those Digital Assets. There may also be other reasons, not related to the value of the Digital Assets to which Digital Portfolios are linked, that can cause unfavorable fluctuations of the value of Digital Portfolios.

(k) Risk of uninsured losses. Unlike bank accounts or accounts at some other financial institutions, funds held using the Platform, Digital Portfolios, or Ethereum network are entirely uninsured.

(l) Risk of malfunction in the Ethereum network or any other blockchain It is possible that the Ethereum network, or any other network with which the Platform and Digital Portfolios interact, malfunctions in an unfavorable way, including but not limited to malfunctions that result in the loss of Digital Portfolios or of information concerning any other cryptographic tokens that are linked to the Digital Portfolios.

(m) Internet transmission risks You acknowledge that there are risks associated with using the Platform, Digital Assets, and Digital Portfolios including but not limited to the failure of hardware, software, or Internet connections. You acknowledge that WAWLLET shall not be responsible for any communication failures, disruptions, errors, distortions, or delays you may experience when using the Platform, however caused.

(n) Unanticipated risks Cryptocurrencies and blockchains are new and untested technology. In addition to the risks set forth here, there are risks that WAWLLET cannot foresee, and it is unreasonable to believe that such risks could have been foreseeable. Risks may further materialize as unanticipated.

6.3 With the acceptance of these Terms you acknowledge and confirm that:

● Digital Portfolios, Digital Assets, cryptocurrencies and products related thereto carry significant inherent risks that may not exist in or may differ from traditional asset classes, including financial instruments;

● past performance of Digital Portfolios, Digital Assets, cryptocurrencies and related products does not predict or guarantee future returns;

● assets invested into Digital Portfolios, Digital Assets, cryptocurrencies and related products on the WAWLLET platform do not represent a significant share of my total net worth;

● investment Digital Portfolios, Digital Assets, cryptocurrencies and related products may result in losses up to and including the total amount of my principal;

● assets invested into Digital Portfolios, Digital Assets, cryptocurrencies and related products on the WAWLLET platform do not represent a significant share of my total net worth;

● assets I deposit on the WAWLLET platform are my own and are not subject to the rights of third parties.

6.4 The Platform and Digital Portfolios are provided “as is.” We and our affiliates and licensors make no representations or warranties of any kind, whether express, implied, statutory, or otherwise, regarding the Platform and the Digital Portfolios, including any warranty that the Platform and Digital Portfolios will be uninterrupted, error-free or free of harmful components, secure, or not otherwise lost or damaged. Except to the extent prohibited by law, we and our affiliates and licensors disclaim all

warranties, including any implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement, or quiet enjoyment, and any warranties arising out of any course of dealing or usage of trade.

7. FEES

7.1 WAWLLET may charge a fee payable by the user to WAWLLET. There are two types of fees:

(a) a transaction fee, payable on the purchase and sale of each Digital Portfolio, that is normally defined as a percentage of the transaction (acquisition or disposal) value,

(b) a periodically management fee that is charged as a certain percentage of the overall Digital Portfolio value or a fixed value.

7.2 Both fees defined above are paid to WAWLLET in the form of the Digital Assets or fiat applicable to that particular transaction. Fees are normally integrated in the source code and executed automatically. WAWLLET may share part of the fees with 3rd parties.

7.3 The amount of fees and any additional conditions in connection with fees are stated on the Website in relation to each particular Digital Portfolio or other services offered on the platform (i.e. a fee for manual processing of incorrect transactions). WAWLLET may publish a Fee Schedule ("Fee Schedule") with general fees, which shall be published in a visible place on the Website or APP.

7.4 WAWLLET reserves the right to change the fees from time to time.

8. ELIGIBILITY

8.1 The Platform, the Website, and Digital Portfolios are not offered for use to natural and legal persons having their habitual residence or their seat of incorporation in the following countries:

i) the United States of America,

ii) Afghanistan, Algeria, United Arab Emirates, Bahrein, Bangladesh, Egypt, Indonesia, Iraq, Iran, Yemen, Jordanian, Qatar, Kuwait, Lebanon, Libya, Malaysia, Mali, Morocco, Mauritania, Nigeria, Oman, Pakistan, Palestine, Saudi Arabia, Somalia, Sri Lanka, Sudan, Syria, Tunisia, Turkey, Ethnic groups of Caucasus belonging to Russian Federation ("Restricted Areas"). WAWLLET may add other countries to the Restricted Areas list in the future without prior notice.

8.2 Natural and legal persons with their habitual residence or seat of incorporation in the Restricted Areas shall not use the Platform, the Website, or the Digital Portfolios. None of the activities of WAWLLET, the Platform, the Website, or the Digital Portfolios take place in the Restricted Areas.

8.3 WAWLLET reserves the right to decide at its discretion to adopt reasonable organizational and technical measures to assure that the Platform, the Website, and Digital Portfolios are not available to the persons described in paragraph 8.1. Due to the Platform, Digital Portfolios, and other products being offered on the Internet (meaning both the world wide web and the Ethereum blockchain), WAWLLET

and its users understand that there may be a certain “flow back” of WAWLLET products to natural and legal persons with their habitual residence or seat of incorporation located in the Restricted Areas. WAWLLET consequently explicitly prohibits the persons described in paragraph 8.1 from using the Platform, the Website, the Digital Portfolios, or any other WAWLLET product. WAWLLET shall not be held liable for any legal or monetary consequences arising from such use. Such persons using WAWLLET products and the Website despite the prohibition shall on first request indemnify and hold harmless WAWLLET from any legal or monetary consequences arising from their breach of the terms as described in this paragraph 8.3. Any person matching the criteria from paragraph 8.1 shall immediately stop using the Platform and leave the Website.

8.4 If you are registering to use the Platform on behalf of a legal entity, you represent and warrant that:
(a) such legal entity is duly organized and validly existing under the applicable laws of the jurisdiction of its organization; and

(b) you are duly authorized by such legal entity to act on its behalf.

(c) additional documentation may be required in such a case

8.5 You further represent and warrant that you:

(a) are of legal age to form a binding contract (at least 18 years old in most jurisdictions);

(b) have not previously been suspended or removed from using our Platform or any other services and products;

(c) have full power and authority to enter into this agreement under these Terms, and in doing so will not violate any other agreement to which you are a party;

(d) are not located in, under the control of, or a national or resident of any Restricted Areas;

(e) have not been placed on any of the sanctions lists published and maintained by the United Nations, European Union, any EU country, UK Treasury, or US Office of Foreign Assets Control (OFAC); and

(f) will not use the Platform, Digital Portfolios, Digital Assets, or any other WAWLLET products if any applicable laws in the jurisdiction of your habitual residence or incorporations prohibit you from doing so in accordance with these Terms.

9. FINANCIAL REGULATION AND COOPERATION WITH LEGAL AUTHORITIES AND AUTHORIZED FINANCIAL INSTITUTIONS AND REGULATORS

9.1 The Platform and the Digital Portfolios are regulated by the Estonian law.

9.2 This document or any other document produced and signed by WAWLLET, as well as the Website, the Platform, and any of their content, does not constitute an offer or solicitation to sell shares or securities.

9.3 None of the information or analyses presented are intended to form the basis for any investment decision, and no specific recommendations are intended. WAWLLET services and the Website and the

Platform are not, do not offer, and shall not be construed as investment or financial products, but as a software application.

9.4 WAWLLET undertakes to cooperate with any governmental legal authority or regulator or supervisory authority of any country, and also with all authorized financial institutions.

10. LIABILITY

10.1 WAWLLET and its affiliates and their respective officers, employees, or agents will in regard to the Website, the Platform, the Digital Portfolios, and any other related products or services not be liable to you or anyone else for any damages of any kind, including but not limited to direct, consequential, incidental, special, or indirect damages (including but not limited to lost profits, trading losses, or damages that result from the use or loss of use of this Website and its products, even if WAWLLET has been advised of the possibility of such damages or losses, including, without limitation, from the use or attempted use of the Website, the Platform, the Digital Portfolios, and/or any of WAWLLET's other products or another linked website.

10.2 Further, neither we nor any of our affiliates or licensors will be responsible for any compensation, reimbursement, or damages arising in connection with:

(a) your inability to use the Website, the Platform, or the Digital Portfolios, including without limitation as a result of any termination or suspension of the Ethereum network or these Terms, including as a result of power outages, maintenance, defects, system failures, or other interruptions;

(b) the cost of procurement of substitute goods or services;

(c) any investments, expenditures, or commitments by you in connection with these Terms or your use of or access to the Website, the Platform, or the Digital Portfolios; or

(d) any unauthorized access to, alteration of, or deletion, destruction, damage, loss, or failure to store any data, including records, private keys, and other credentials, associated with the Website, the Platform, or the Digital Portfolios.

10.3 In any case, our and our affiliates' and licensors' aggregate liability under these Terms will be limited to 50,00 EUR per user.

10.4 You waive your right to demand the return of any Digital Asset or cryptographic tokens you exchange with us for the purpose of purchasing Digital Portfolios, including, without limitation, a demand for specific performance.

10.5 You will defend, indemnify, and hold harmless us, our affiliates and licensors, and each of their respective employees, officers, directors, and representatives from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorney fees) arising out of or relating to any third-party claim concerning these Terms or your use of the Website, the Platform, or the Digital Portfolios contrary to these Terms. If we or our affiliates are obligated to respond to a third-party subpoena or other compulsory legal order or process described above, you will also reimburse us for reasonable attorney fees, as well as our employees' and contractors' time and materials spent

responding to the third-party subpoena or other compulsory legal order or process at reasonable hourly rates.

10.6 The information, software, products, and services included in or available through the Website may include inaccuracies or typographical errors. Changes are periodically added to the information herein. WAWLLET and/or its suppliers may make improvements and/or changes in the Website at any time. WAWLLET makes no representations about the suitability, reliability, availability, timeliness, and accuracy of the Website, the Platform, the Digital Portfolios, information, software, products, services, and related graphics contained on the Website for any purpose. To the maximum extent permitted by applicable law, the Website, the Platform, the Digital Portfolios, all such information, software, products, services, and related graphics are provided "as is" without warranty or condition of any kind. WAWLLET hereby disclaims all warranties and conditions with regard to the Website, the Platform, the Digital Portfolios, information, software, products, services, and related graphics, including all implied warranties or conditions of merchantability, fitness for a particular purpose, title, and non-infringement.

11. SECURITY

11.1 You will implement reasonable and appropriate measures designed to secure access to

(i) any device associated with the email address associated with your account,

(ii) private keys required to access any relevant blockchain address, and

(iii) your username, password and any other login or identifying credentials.

11.2 In case you suspect a security breach in any of the above mentioned cases, you will inform us immediately so we can take all required and possible measures to secure your account, the Platform, and systems as whole.

11.3 In the event that you are no longer in possession of any device associated with your account or are not able to provide your login or identifying credentials, we may, in our sole discretion, and only if we are able, grant access to your account to any party providing additional credentials to us. We explicitly reserve the right to determine the additional credentials required, which may include, without limitation, a sworn, notarized statement of identity.

12. PRIVACY

12.1 WAWLLET processes personal data of users in accordance with WAWLLET Privacy Policy, which is an integral part of these Terms. WAWLLET Privacy Policy provides to the user all necessary information regarding the processing of personal data, including the rights of users regarding the processing of their personal data.

13. TAXES

13.1 All your factual and potential tax obligations are your concern, and WAWLLET is not in any case and under no conditions bound to compensate for your tax obligation or give you any advice related to tax issues, including but not limited to what kind of filing or reporting is required of you by the competent tax authority, which taxes and to what extent you are obliged to pay, which tax exemptions you are eligible to, etc.

13.2 All fees and charges payable by you are exclusive of any taxes, and if certain taxes are applicable, they shall be added on top of the payable amounts. Upon our request, you will provide us any information we reasonably request to determine whether we are obligated to collect VAT from you, including your VAT identification number. If any deduction or withholding is required by law, you will notify us and will pay us any additional amounts necessary to ensure that the net amount that we receive, after any deduction and withholding, is equal to the amount we would have received if no deduction or withholding had been required. Additionally, you will provide us with documentation showing that the withheld and deducted amounts have been paid to the relevant taxing authority.

14. INTELLECTUAL PROPERTY

14.1 All rights, title, and interest in all of WAWLLET IP, including inventions, discoveries, processes, marks, methods, compositions, formulae, techniques, information, and data, whether or not patentable, copyrightable, or protectable in trademark, and any trademarks, copyrights, or patents based thereon, shall remain with WAWLLET ENTERPRISES HQ LIMITED. You may not use any of our intellectual property for any reason, except with our express, prior, written consent.

14.2 In particular, WAWLLET ENTERPRISES HQ LIMITED shall retain all intellectual property rights, mostly, but not limited to, copyright over the source code forming the Platform and Digital Portfolios. These Terms shall not be understood or interpreted in a way that would mean assignment of intellectual property rights, unless explicitly defined as such in these Terms.

14.3 You are being granted a non-exclusive, non-transferable, revocable license to access and use the Website, the Platform, and the Digital Portfolios strictly in accordance with these Terms. As a condition of your use of the Website, the Platform, and the Digital Portfolios you warrant to WAWLLET that you will not use the Website, the Platform, or the Digital Portfolios for any purpose that is unlawful or prohibited by these Terms. You may not use the Digital Portfolios or any other Digital Assets in any manner that could damage, disable, overburden, or impair the Website or the Platform or interfere with any other party's use and enjoyment of the Website, the Platform, Digital Portfolios, or any other products offered. You may not obtain or attempt to obtain any materials or information through any means not intentionally made available or provided for through the Website, the Platform, or Digital Portfolios or other services provided. Limitation of the transferability of licence shall not be understood in a way that the users are not allowed to transfer Digital Portfolios and their Digital Assets to third parties.

14.4 All content included on the Website or the Platform, including Digital Portfolios and associated products and services, such as, but not limited to, text, graphics, logos, images, source code, as well as the compilation thereof, and any software used on the Website and the Platform (hereinafter: “WAWLLET IP”) is the property of WAWLLET ENTERPRISES HQ LIMITED and protected by copyright,

trademark, and other laws that protect intellectual property and proprietary rights. You agree to observe and abide by all copyright and other proprietary notices, legends, or other restrictions contained in any such content and will not make any changes thereto.

14.5 You will not modify, publish, transmit, reverse engineer, participate in the transfer or sale, create derivative works, or in any way exploit any of the WAWLLET IP, in whole or in part, found on the Website, the Platform, or within Digital Portfolios or associated products and services. WAWLLET IP is not for resale. Your use of the WAWLLET IP does not entitle you to make any unauthorized use of any WAWLLET IP, and in particular you will not delete or alter any proprietary rights or attribution notices in any WAWLLET IP. You will use WAWLLET IP solely for your personal use, and will make no other use of WAWLLET IP without the express written permission of WAWLLET and the copyright owner (WAWLLET ENTERPRISES HQ LIMITED). You agree that you do not acquire any ownership rights in any WAWLLET IP. We do not grant you any licenses, express or implied, to the intellectual property of WAWLLET ENTERPRISES HQ LIMITED except as expressly authorized by these Terms.

15. ACCESS TO THE PLATFORM

15.1 The Platform and the Website are provided without warranty of any kind, either express or implied. We do not represent that the Website and the Platform will be available 100% of the time to meet your needs. In case of interruptions we take all reasonable actions to provide you with access to the Platform as soon as possible, but there are no guarantees that access will not be interrupted, or that there will be no delays, failures, errors, omissions, or loss of transmitted information.

15.2 We may suspend use of the Website and the Platform for maintenance.

15.3 WAWLLET reserves the right, in its sole discretion, to terminate your access to the Website, the Platform, and its related services or any portion thereof at any time, without notice, in particular due to legal grounds originating in anti-money laundering and know your client regulation and procedures, or any other relevant applicable regulation.

16. TRANSACTION RECOVERY

16.1 You are responsible to regularly monitor the deposit and withdrawal rules and procedures. With the change of the Platform from time to time, including but not limited to changes applied to the interface, instructions or procedures, you are obligated to read and follow the instructions related to making any kind of transactions very carefully every time you are conducting a deposit or withdrawal and to precisely follow each step of the process.

16.2 Your first deposit or withdrawal amount should be marginal so you can check that the transacted funds are received at the intended address. Only when you are convinced that the deposit or withdrawal you initiated follows the correct process, should you increase the transacted amount. You are fully responsible for any mistakes, errors or defects which may arise in the course of a transaction and lead to partial or complete loss of your funds. WAWLLET shall not be held liable for any damages resulting from any actions previously mentioned.

16.3 WAWLLET shall in no case be liable for any loss, including but not limited to transfers between addresses, transactions, deposits, or withdrawals, resulting from your improper actions or activities, or erroneous transactions, deposits or withdrawals, resulting in your funds being lost. WAWLLET shall not compensate you for any losses resulting from such actions or activities.

16.4 WAWLLET strongly advises against making any direct transactions between your WAWLLET account and any other account or collection address that may, among others, include exchange, service, third party, or (de)centralized infrastructure. If you decide to transfer funds to a designated collection address or deposit funds to any other exchange, service, third party or (de)centralized infrastructure directly from WAWLLET, make sure that such transaction includes no risks for the loss of funds and that you receive correct and detailed instructions from the other party prior to making any transaction. WAWLLET will not investigate ownership or enter into reimbursements in any cases of such false transactions.

16.5 WAWLLET provides investigation into lost funds as a payable service. Upon request, if a deposit or a withdrawal returns incomplete, erroneous or defect and you experience loss of funds or anticipate they may not be recovered, WAWLLET may, based on your explicit request, under best efforts, undertake to seek to return funds to you or to revoke any transaction that lead or may lead to loss of funds.

16.6 WAWLLET will charge an investigation fee for any such investigation. The fee shall amount to 10% of the value of lost funds, but in no case less than 0.1 BTC (or the equivalent amount of ETH valued in USD). We will investigate transactions that occurred not more than thirty (30) days prior to the date of the request for the recovery of funds. Due to the specifics and case-by-case nature, WAWLLET does not, in any way, guarantee success and shall not be liable if the investigation is ineffective and unsuccessful.

16.7 Due to the specifics that may be involved in each individual case, WAWLLET cannot provide exact timing for such investigations, but will strive to provide feedback within reasonable time.

17. NOTICES

17.1 We may provide any notice to you under these Terms by:

(i) posting a notice on the Website; or

(ii) sending an email to the email address associated with your account. Notices we provide by posting on the Website will be effective upon posting, and notices we provide by email will be effective when we send the email. It is your responsibility to keep your email address current. You will be deemed to have received any email sent to the email address associated with your account when we send the email, whether or not you actually receive or read the email.

17.2 To give us notice under these Terms, you must contact us by email at contact@wawllet.com or through the contact for provided by WAWLLET APP. We may update this email address for notices to us by posting a notice on our Website or Platform. Notices to us will be effective one business day after they are sent.

17.3 All communications and notices to be made or given pursuant to these Terms must be in the English language.

18. MISCELLANEOUS

18.1 We do not permit individuals under the age of 18 to register with our Website and use our products. If we become aware that a child under the age of 18 has provided us with personal data, we will delete such information from our files immediately and block him or her from accessing our Website and products.

18.2 We and our affiliates will not be liable for any delay or failure to perform any obligation under these Terms where the delay or failure results from any cause beyond our reasonable control, including acts of God; labour disputes or other industrial disturbances; electrical, telecommunications, hardware, software, or other utility failures; earthquakes, storms, or other elements of nature; blockages, embargoes, riots, acts or orders of government, acts of terrorism or war; changes in blockchain technology (broadly construed); changes in the Ethereum or any other blockchain protocols; or any other force outside of our control.

18.3 We and you are independent contractors, and neither party, nor any of their respective affiliates, is an agent of the other for any purpose or has the authority to bind the other. Both parties reserve the right

(a) to develop or have developed for them products, services, concepts, systems, or techniques that are similar to or compete with the products, services, concepts, systems, or techniques developed or contemplated by the other party, and

(b) to assist third-party developers or systems integrators who may offer products or services that compete with the other party's products or services.

18.4 These Terms do not create any third-party beneficiary rights in any individual or entity.

18.5 You will not assign these Terms, or delegate or sublicense any of your rights under these Terms, without our prior written consent. Any assignment or transfer contrary to these Terms will be void. Subject to the foregoing, these Terms will be binding upon, and inure to the benefit of, the parties and their respective successors and assigns.

18.6 Notwithstanding clause 18.5 above, WAWLLET may at any time assign or transfer all or any of its rights under or pursuant to these Terms to any other entity that is a subsidiary or affiliate of WAWLLET or to another entity, so long as such assignment or transfer does not result in the User being subject to any additional financial or legal obligations other than those stipulated by these Terms at the time of such assignment or transfer. For the avoidance of doubt, any assignment of transfer under these Terms shall not affect clause 14.4, and WAWLLET IP shall permanently remain with WAWLLET.

RULES OF PROCEDURE
FOR PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING
AND
COMPLIANCE WITH INTERNATIONAL SANCTIONS

Established by the decision of the management board of WAWLLET ENTERPRISES OÜ (registry code 14549617) (hereinafter **Provider of service**) on 05.09.2018.

1. General provisions 21
2. Definitions 21
3. Description of activities of the Provider of service 23
4. Compliance Officer 23
5. Application of due diligence measures 23
6. Normal due diligence measures 24
7. Identification of a person 25
8. Simplified due diligence measures 29
9. Enhanced due diligence measures 29
10. Risk assessment 30
11. Registration and storage of data 33
12. Reporting 40
13. Implementation of International Sanctions 42
14. Training 43
15. Internal audit and amendment of the Rules 43
Form 1 45
Exhibit 1 49

1. General provisions

1.1. These rules of procedure for prevention of money laundering and terrorist financing, and compliance with international sanctions (hereinafter **Rules**) lay down requirements for screening the Clients (as defined in section 2.7) in order to prevent entering into deals involving suspected Money Laundering and Terrorist Financing, and to ensure identification and reporting of such.

1.2. The obligation to observe the Rules rests with Management Board members and employees of the Provider of service, including temporary staff, agents of the Provider of service who initiate or establish Business Relationship (as defined in section 2.6) (hereinafter all together called the **Representative**). Every Representative must confirm awareness of the Rules with the signature.

1.3. The Rules are primarily based on the regulations of Money Laundering and Terrorist Financing Prevention Act (hereinafter **the Act**) and International Sanctions Act (hereinafter **ISA**).

2. Definitions

2.1. Money Laundering – is a set of activities with the property derived from criminal activity or property obtained instead of such property with the purpose to:

i. conceal or disguise the true nature, source, location, disposition, movement, right of ownership or other rights related to such property;
ii. convert, transfer, acquire, possess or use such property for the purpose of concealing or disguising the illicit origin of property or of assisting a person who is involved in criminal activity to evade the legal consequences of his or her action;
iii. participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to subsections 2.1.i and 2.1.ii.

2.2. Terrorist Financing – acts of financing of terrorism as defined in § 237^3 of the Penal Code of Estonia.

2.3. International Sanctions – list of non-military measures decided by the European Union, the United Nations, another international organisation or the government of the Republic of Estonia and aimed to maintain or restore peace, prevent conflicts and restore international security, support and reinforce democracy, follow the rule of law, human rights and international law and achieve other objectives of the common foreign and security policy of the European Union.

2.4. Compliance Officer or CO – representative appointed by the Management Board responsible for the effectiveness of the Rules, conducting compliance over the adherence to the Rules and serving as contact person of the FIU.

2.5. FIU - Financial Intelligence Unit of the Police and Border Guard Board of Estonia.

2.6. Business Relationship – a relationship of the Provider of service established in its economic and professional activities with the Client.

2.7. Client – a natural or legal person, who uses services of the Provider of service.

2.8. Beneficial Owner – is a natural person, who:

i. Taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed taking advantage of his 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.
ii. Ultimately owns or controls a legal person 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 which is under the control of a natural person holds or multiple companies which are under the control of the same 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.

iii. Holds the position of a senior managing official, if, after all possible means of identification have been exhausted, the person specified in clause ii cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner.

iv. In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations': settlor or person who has handed over property to the asset pool, trustee or manager or possessor of the property, person ensuring and controlling the preservation of property, where such person has been appointed, or the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.

2.9. Politically Exposed Person or PEP - is 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.

2.9.1. The provisions set out above also include positions in the European Union and in other international organizations.

2.9.2. A family member of a person performing prominent public functions is the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.

2.9.3. A close associate of a person performing prominent public functions is a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

2.10. Local Politically Exposed Person or local PEP – a natural person, provided in section 2.9, who performs or has performed prominent public functions in Estonia, a contracting state of the European Economic Area or in an institution of European Union.

2.11. Provider of service – WAWLLET ENTERPRISES OÜ, registry code 14549617, address Roosikrantsi 2-617K, Tallinn 10119, Estonia.

2.12. Management Board or MB – management board of the Provider of service. Member of the MB, as appointed by relevant MB decision, is responsible for implementation of the Rules.

2.13. Equivalent Third Country – means a country not a Member State of European Economic Area but applying an equivalent regime to the European Union corresponding (AML) framework (see also Exhibit 1).

2.14. Virtual currency - a value represented in the digital form, which is digitally transferable, preservable or tradable and which persons accept as a payment instrument, but that is not the legal

tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same directive.

3. Description of activities of the Provider of service

3.1. The Provider of service is the provider of a virtual currency wallet service in the framework of which the Provider of service generates Clients' encrypted keys, which can be used for the purpose of keeping, storing and/or transferring virtual currencies.

3.2. The Provider of service is a subject to authorisation by the FIU.

4. Compliance Officer

4.1. The MB shall appoint a CO whose principal tasks are to:

4.1.1. monitor the compliance of the Rules with the relevant laws and compliance of the activity of the Representatives with the procedures established by the Rules;

4.1.2. compile and keep updated the data regarding countries with low tax risk, high and low risk of Money Laundering and Terrorist Financing and economical activities with great exposure to Money Laundering and Terrorist Financing;

4.1.3. carry out training, instruct and update the Representatives on matters pertaining to procedures for prevention of Money Laundering and Terrorist Financing;

4.1.4. report to the MB once a year (or more frequently, if necessary) on compliance with the Rules, and on circumstances with a suspicion of Money Laundering or Terrorist Financing;

4.1.5. collect, process and analyse the data received from the Representatives or Clients concerning suspicious and unusual activities;

4.1.6. collaborate with and report to the FIU on events of suspected Money Laundering or Terrorist Financing, and respond to enquiries of the FIU;

4.1.7. make proposals on remedying any deficiencies identified in the course of checks.

4.2. The CO must meet all the requirements, prescribed by the Act, and appointment of the CO shall be co-ordinated with the FIU. If, as a result of a background check carried out by the FIU, it becomes evident that the CO's credibility is under suspicion due to their previous acts or omissions, the Provider of service may extraordinarily terminate the CO's employment contract due to the loss of credibility.

4.3. Tasks of the CO can be performed by a department, therefore provisions of section 4.2 will apply accordingly.

5. Application of due diligence measures

5.1. The Provider of service shall determine and take due diligence (hereinafter **DD**) measures using results of conducted risk assessment (see Section 10), and provisions of national risk assessment, published on the web-page of the Ministry of Finance of Estonia.

5.2. The Representatives shall pay special attention to circumstances that refer to Money Laundering or Terrorist Financing.

5.3. Depending on the level of the risk of the Client and depending on the fact whether the Business Relationship is an existing one or it is about to be established, the Provider of service shall apply either normal DD measures (see Section 6), simplified DD measures (see Section 8) or enhanced DD measures (see Section 9). The Provider of service shall also apply continuous DD measures to ensure ongoing monitoring of Business Relationships (see Sections 5.7-5.10).

5.4. DD measures shall include the following procedures:

i. Identifying the Client and verifying its identity using reliable, independent sources, documents or data, including e-identifying;

ii. Identifying and verifying of the representative of the Client and the right of representation;
iii. Identifying the Client's Beneficial Owner;
iv. Assessing and, as appropriate, obtaining information on the purpose of the Business Relationship;
v. Conducting ongoing DD on the Client's business to ensure the Provider of service's knowledge of the Client and its source of funds is correct;
vi. Obtaining information whether the Client is a PEP or PEP's family member or PEP's close associate.

5.5. The Provider of service shall establish the source of wealth of the Client, where appropriate.

5.6. To comply with the DD obligation, the Representatives shall have the right and obligation to:
i. request appropriate identity documents to identify the Client and its representatives;
ii. request documents and information regarding the activities of the Client and legal origin of funds;
iii. request information about Beneficial Owners of a legal person;
iv. screen the risk profile of the Client, select the appropriate DD measures, assess the risk whether the Client is or may become involved in Money Laundering or Terrorist Financing;
v. re-identify the Client or the representative of the Client, if there are any doubts regarding the correctness of the information received in the course of initial identification;

5.7. The objective of the continuously applied DD measures is to ensure on-going monitoring of Clients. Conducting ongoing monitoring of the Business Relationship includes:
i. Keeping up-to-date the documents, data or information, obtained during taking DD measures;
ii. Paying particular attention Client's conduction, leading to criminal activity or Money Laundering or Terrorist Financing;
iii. Paying particular attention to the Business Relationship, if the Client is from or the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries (see Exhibit 1).

5.8. Annual review of a Client being a legal entity is carried out regularly once a year. Updated data shall be recorded in the Provider of service's Client database.

5.9. The Representative updates the data of a Client, who is either a legal person or a natural person, i.e. takes appropriate DD measures every time when:
i. the Client addresses the Provider of service with the request to amend a long-term contract during the term of its validity;
ii. upon identification and verification of the information there is reason to suspect that the documents or data gathered earlier are insufficient, have changed or are incorrect. In this case, the Representative may conduct a face-to-face meeting with the Client;
iii. the Provider of service has learned through third persons or the media that the activities or data of the Client have changed significantly.

5.10. The Representative shall evaluate the substance and the purpose of the Client's activities, in order to establish the possible links with Money Laundering or Terrorist Financing. The evaluation should result in an understanding about the purpose of the Business Relationship for the Client, the nature of the Client's business, the risk levels of the Client and, if necessary, the sources of funds.

6. Normal due diligence measures

6.1. The Provider of service shall conduct normal DD in the following cases:

i. Upon establishing a new Business Relationship;
ii. In the event of insufficiency or suspected incorrectness of the documents or information gathered previously in the course of carrying out DD measures;
iii. Upon suspicion of Money Laundering or Terrorist Financing.

6.2. **In the course of conducting normal DD measures, the Representative shall apply the measures of DD as provided for in section 5.4.**

6.3. No new Business Relationship can be formed, if the Client, in spite of the respective request, has failed to present documents and appropriate information required to conduct DD, or if based on the presented documents, the Representative suspects Money Laundering or Terrorist Financing.

6.4. If in spite of the respective request an existing Client has failed to present during the contract period documents and appropriate information required to conduct DD, such behaviour constitutes material breach of contract that shall be reported by the Representative to the CO, and in such case the contract(s) concluded with the Client shall be cancelled and the Business Relationship shall be terminated as soon as feasible[1].

6.5. The Provider of service shall not enter into Business Relationships with anonymous Clients.

7. Identification of a person

7.1. Upon implementing DD measures the following person shall be identified:

i. Client – a natural or legal person;
ii. Representative of the Client – an individual who is authorized to act on behalf of the Client;
iii. Beneficial Owner of the Client;
iv. PEP – if the PEP is the Client or a person connected with the Client (see Section 2.9).

7.2. **Upon establishing the relationship with the Client the Provider of service shall identify and verify the Client while being present at the same place as the Client or by using information technology means.**

7.3. For identification of a Client and verification of the identity of a Client by using information technology means, the Provider of service shall use:

7.3.1. a document issued by the Republic of Estonia for the purpose of digital identification;

7.3.2. another electronic identification system within the meaning of the Regulation (EU) No 910/2014 of the European Parliament and of the Council[2]. If the Client is a foreign national, the identity document issued by the competent authority of the foreign country is also used simultaneously.

7.4. In case of identification of a Client and verification of the identity of a Client by using information technology means the Provider of service shall additionally obtain data from a reliable and independent source, e.g. identity documents databases.

7.5. <u>Identification of a Client being a natural person and a representative of a Client who is a legal person</u>

7.5.1. Upon establishing a Business Relationship, identification takes place, above all, during a face-to-face meeting or by using information technology means.

7.5.2. The Rules must be considered when dealing with the documents that can be used to identify the Client or its representative and the requirements established for them (see

[1] The termination of the long-term contract or contract without the term must foresee the Provider of service's right to terminate the contract extraordinarily without observing the period of pre-notice in case the Client does not provide requested identification or verification documents (in due time)

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1510127223064&uri=CELEX:32014R0910

Section 7.10). If it is not possible to obtain original documents for identification of a Client, request documents certified or authenticated by a notary public or authenticated officially for verification of the identity of the natural person, or use data obtained from other reliable and independent sources (including electronical identification) on condition that information is obtained from at least two different sources.

7.5.3. Verification must be made whether or not such person is a PEP (see Section 7.9).

7.5.4. A new Client and, if necessary, an existing Client shall confirm the correctness of the submitted information and data by signing the Client data registration sheet (see Form 1).

7.6. Identification of a Client being a legal person

7.6.1. To identify a Client who is a legal person, the Representative shall take the following actions:

i. Check the information concerning a legal person by accessing the relevant electronic databases (e-commercial register/ e-äriregister and European Business Register);

ii. If it is not possible to obtain an original extract from the register or the respective data, request documents (extract from the relevant registry, certificate of registration or equivalent document) certified or authenticated by a notary public or authenticated officially for verification of the identity of the legal person, or use data obtained from other reliable and independent sources (including electronical identification) on condition that information is obtained from at least two different sources;

iii. Ask the representative of a foreign legal person to present an identity documents and a document evidencing of his/her power of attorney, which has been notarised or authenticated pursuant to an equal procedure and legalised or authenticated by a certificate substituting for legalisation (apostille), unless otherwise prescribed by an international agreement;

iv. On the basis of the information received from the representative of the foreign legal person, control whether or not the legal person could be linked with a PEP (see Section 7.9);

v. If the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries (see Exhibit 1), report this to the CO, who shall decide the additional measures to be applied to identifying and background checking of the person.

7.6.2. The document presented for identification of a legal person shall set out at least the following:

i. business name, registry code (number), date of registration, seat and address;

ii. names and authorisations of members of the Management Board or the head of branch or the other relevant body.

7.6.3. A legal representative of a new Client (subsequently as required) shall confirm the correctness of the submitted information and data by signing the Client data registration sheet (see Form 1).

7.7. Consequences of insufficient identification of a Client

7.7.1. Should the Representative establish that the identification of a Client is insufficient the Representative shall:

i. Promptly apply the enhanced DD measures pursuant to the Rules;

ii. Notify the CO of the failure to implement normal DD in a timely manner;

iii. Assess the risk profile of the Client and notify CO and/or MB for the purposes of the provisions in Section 12.3.

7.8. Identification of the Beneficial Owner of the Client

7.8.1. Registration and assessment of the Beneficial Owner(s) of a legal person is mandatory.

7.8.2. There is no need to identify the Beneficial Owners of a Client/company whose securities have been accepted for trading on a regulated securities market.

7.8.3. In order to establish the Beneficial Owner, the Representative shall take the following actions:

i. Gather information about the ownership and control structure of the Client on the basis of information provided in pre-contractual negotiations or obtained from another reliable and independent source;

ii. In situations, where no single person holds the interest or ascertained level of control to the extent of no less than 25 per cent (see Section 2.9), apply the principle of proportionality to establishing the circle of beneficiaries, which means asking information about persons, who control the operations of the legal person, or otherwise exercise dominant influence over the same;

iii. If the documents used to identify a legal person, or other submitted documents do not clearly identify the Beneficial Owners, record the respective information (i.e. whether the legal person is a part of a group, and the identifiable ownership and management structure of the group) on the basis of the statements made by the representative of the legal person, or a written document under the hand of the representative;

iv. To verify the presented information, make enquiries to the respective registers, and request an annual report or another appropriate document to be presented.

v. If no natural person is identifiable who ultimately owns or exerts control over a Client and all other means of identification are exhausted, the senior managing official(s) might be considered to be the Beneficial Owner(s).

vi. Pay attention to companies established in low tax rate regions (see Exhibit 1).

7.8.4. While establishing the Beneficial Owner, it is possible to rely on information received in a format reproducible in writing from a credit institution registered in the Estonian commercial register or from the branch of a foreign credit institution, or from a credit institution that has been registered or whose place of business is in a contracting state of the European Economic Area or an Equivalent Third Country (see Exhibit 1).

7.9. Identification of Politically Exposed Person

7.9.1. The Representative shall implement the following measures to establish whether or not a person is a PEP:

i. asking the Client to provide necessary information;

ii. making an enquiry or checking the data on websites of the respective supervisory authorities or institutions of the country of location of the Client.

7.9.2. The matter of whether to establish a Business Relationships with a PEP, or a person associated with him or her, and the DD measures applied to such person shall be decided by the MB.

7.9.3. If a Business Relationship has been established with a Client, and the Client or its Beneficial Owner subsequently turns out to be or becomes a PEP, CO and MB shall be notified of that.

7.9.4. In order to establish a Business Relationship with a PEP or a company connected with that person, it is necessary to:

i. take enhanced DD measures (see Section 9);

ii. establish the source of wealth of this person;

iii. monitor the Business Relationship on a continual basis.

7.9.5. DD measures, mentioned in Section 7.9.4 might be not applicable regarding local PEPs, if there are no relevant circumstances, leading to the higher risks.

7.9.6. Respective remark must be made in the Provider of service's database of Clients on documents of such person in the form of notation "Politically Exposed Person".

7.10. Documents that can be used for identification

7.10.1. In case of Clients being natural persons and the representatives of Clients, the following documents can be used for identification[3]:

i. Personal ID card (whether ID card, e-resident card or residence permit card);
ii. Passport or diplomatic passport;
iii. Travel document issued in a foreign country;
iv. Driving licence (if it has name, facial image, signature and personal code or date of birth of holder on it).

7.10.2. The Representative shall make a copy of the page of identity document which contains personal data and photo.

7.10.3. In addition to an identity document, the representative of a Client shall submit a document in the required format certifying the right of representation.

7.10.4. Legal person and its passive legal capacity shall be identified and verified on the basis of the following documents:

i. in case of legal persons registered in Estonia and branches of foreign companies registered in Estonia, the identification shall be conducted on the basis of an extract of a registry card of commercial register;
ii. foreign legal persons shall be identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equal document, which has been issued by competent authority or body not earlier that six months before submission thereof.

7.10.5. If not original documents are used for identification, the Representative shall control and verify data by using at least two reliable and independent sources.

7.11. If the Client is a natural person, the following data shall be recorded:

i. Name of the Client;
ii. Personal identification code (in case of absence the date and place of birth and place of residence);
iii. Information regarding identification and verification of the right of representation. If the right of representation does not arise from law, name of the document used for establishing and verification of the right of representation, the date of issue and the name or name of the issuing party.

7.12. If the Client is a legal person, the following data shall be recorded:

i. Name of the Client;
ii. Registry code (or registration number and registration date) of the Client;
iii. Names and authorisations of members of the Management Board or the head of branch or the other relevant body;
iv. Telecommunications numbers.

[3] About documents to be used for identification: https://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/isikusamasuse-tuvastamine.dot
Authenticity of personal ID documents can be checked here: http://www.consilium.europa.eu/prado/ET/prado-start-page.html (14.02.2017) or here: https://www.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/

8. Simplified due diligence measures

8.1. Simplified DD measures may be taken, if the Client is:

i. A company listed on a regulated market that is subject to disclosure requirements consistent with European Union law;
ii. a legal person governed by public law founded in Estonia;
iii. a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area;
iv. an authority of the European Union;
v. a credit institution or a financial institution, acting on behalf of itself, located in a contracting state of the European Economic Area or in a third country (see Exhibit 1), which in the country of location is subject to equal requirements and the performance of which is subject to state supervision.

8.2. Upon identifying and screening of such Clients, the following circumstances, if present concurrently, shall be considered criteria pointing to low level of risk:

i. the Client can be identified on the basis of publicly available information;
ii. the ownership and control structure of the Client is transparent and constant;
iii. the operations of the Client and their accounting or payment policies are transparent;
iv. Client reports to and is controlled by an authority of executive power of Estonia or a contracting state of the European Economic Area, another agency performing public duties, or an authority of the European Union.

9. Enhanced due diligence measures

9.1. Enhanced DD measures must be taken in cases where the risk level of the Client is higher.

9.2. The Representative shall establish the Client's risk profile and determine the risk category in accordance with the Rules (see Section 10). The risk category may be altered during the course of the Business Relationship, taking into consideration the changes in data gathered.

9.3. The Representative, who upon entering into a Business Relationship with a new Client, detects that there is at least one of the following high-risk characteristics present in respect of a Client, shall consult with and report to the CO, and shall take the DD measures set out in the Rules.

9.4. The Representative shall apply enhanced DD measures in the following situations:

9.4.1. when suspicion arises regarding truthfulness of the provided data and/or of authenticity of the identification documents regarding the Client or its Beneficial Owners;
9.4.2. the Client is a PEP (excluding local PEPs, if there are no relevant circumstances, leading to the higher risks);
9.4.3. the Client is from or the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries (see Exhibit 1);
9.4.4. in case of companies that have nominee shareholders or shares in bearer form;
9.4.5. in a situation with higher risk of Money Laundering and terrorists financing as described in Sections 9.1 and 9.3.

9.5. Enhanced DD measures shall include at least one the following measures in addition to normal DD measures as established in Section 5.4:

9.5.1. Identification and verification of a Client on the basis of additional documents, data or information, which originates from a reliable and independent source;
9.5.2. Identification and verification of a Client while being present at the same place;
9.5.3. Asking the identification or verification documents to be notarised or officially authenticated;

9.5.4. Obtaining additional information on the purpose and nature of the Business Relationship and verification from a reliable and independent source;

9.5.5. Reassessment of a risk profile of a Client not later than 6 months after establishment of Business Relationship.

9.6. After taking enhanced DD measures, the MB shall decide whether to establish or continue the Business Relationship with the Client in respect of whom the enhanced DD measures were taken.

9.7. If a Client who, by the date of entry into a contract, has not performed any prominent public functions for at least a year, and such person is deemed to pose no further risk specific to PEP, this Client is not considered as the PEP, therefore application of enhanced DD measures is not required.

9.8. The Representative may not apply enhanced DD measures stipulated in section 9.5 to local PEP, if there are no other circumstances leading to the higher risk.

10. Risk assessment

10.1. The Representative will establish a risk profile of a Client based on information gathered under the Rules.

10.2. The Provider of service applies the following risk categories:

i. Normal risk (the risk level is normal, there are no high risk characteristics present);

ii. High risk, which is subcategorized as High risk I and High risk II.

10.3. For every Client, who does not fall into the "normal risk" category, the Representative shall record the Client's risk category in the Provider of service's database of Clients and on the documents as "High risk I" or "High risk II". Only the CO shall have the right to change the risk category recorded for a Client.

10.4. <u>Assessment of risk profile of natural persons</u>

10.4.1. When establishing the risk category of a Client being a natural person, the country of residence of the Client, the region where the Client operates, and status of PEP shall be taken into account.

10.4.2. If there are several characteristics of the category "High risk I" present, or if, in addition to the characteristics of "High risk I", at least one of the "High risk II" characteristics is present, the Client shall be determined to be falling into the category "High risk II".

10.4.3. Characteristics of high risk in the case of a natural person, and the appropriate DD measures:

High risk category I	**DD measures**
The actual place of residence or employment or business of a Client is in a country, which is included in the list of risk countries (see Exhibit 1), or the Client is an official citizen/resident of such country.	Ask the Client to provide additional information about the purpose of establishing the Business Relationship and his/her economic activities. Ask the Client to provide additional information about its links with the said foreign state.
The Client is a person associated with a PEP.	The decision is taken by the MB.
The Client is a local PEP.	Conduct an internet search about the Client. Ask additional information and documents, which prove the legal origin of Client's assets. If there are no other circumstances leading to the higher risk and the MB

	approves, it is not required to apply enhanced DD measures stipulated in section 10.7.

	High risk category II	DD measures
	The Client is a PEP or a person associated with him or her.	Conduct an internet search about the Client. Ask additional information and documents, which prove the legal origin of Client's assets.
	There is information that the Client is suspected to be or to have been linked with a financial offence or other suspicious activities.	Check information about International Sanctions (see also Section 15)[4] or ask guidance from the CO. Ask additional information and documents, which prove the legal origin of the Client's assets.
	The Client is a non-resident individual, whose place of residence or activities is in a country, which is listed in the list of risk countries (see Exhibit 1).	Ask the Client to provide additional documents to identify the Client and, if possible, check the Client's data vis-à-vis the previously presented documents and information. Verify and compare the data submitted by the Client against the additional documents, data or information, which originates from a reliable and independent source.

10.5. Assessment of risk profile of legal persons

10.5.1. When establishing the risk category of a legal person, assessment shall be based on the country of location of the legal person, its area of activity, the transparency of ownership structure and the management.

10.5.2. If there are several characteristics of the category "High risk I", or if, in addition to the characteristics of "High risk I", at least one of the "High risk II" characteristics is present, the Client shall be determined to be falling into the category "High risk II".

10.5.3. Characteristics of high risk in the case of a legal person, and the appropriate DD measures

	High risk category I	DD measures
	The Client is a legal person registered in the European Economic Area or in Switzerland, whose area of activity is associated with enhanced money-laundering risk (see Exhibit 1).	Ask the Client to provide additional documents to identify it and, if possible, check the Client's data vis-à-vis the previously presented documents and information. Verify and compare the data submitted by the Client against the additional documents or information, which originates from a reliable and independent source.
	The Client is situated in a country, which is listed in the list of risk countries (see Exhibit 1).	Ask the Client to provide additional information about its links with the said foreign state. Ask for additional information about the purpose of

[4] For search regarding financial sanctions imposed against a person please refer to: https://www.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/

	establishing the Business Relationship.
The legal person is a non-profit association, trust, civil law partnership or another contractual legal arrangement, whose activities and liability are insufficiently regulated by law, and the legality of financing of which is not easy to screen.	Check the authenticity of the presented documents and verify the accuracy of the data. Ask for help from the CO. Ask the Client to provide information about relationships with other credit or financing institutions, and the opinion of the respective credit or financing institution. Ask additional information and documents, which prove the legal origin of the Client's assets.
The representative or the Beneficial Owner of a legal person is a local PEP or his or her family member.	Ask the Client to provide additional information about the need and purpose of establishing the Business Relationship. Ask the Client to provide information about relationships with other credit or financing institutions, and the opinion of the respective credit or financing institution about the Client. Conduct an internet search about the Client, being a legal person, and its Beneficial Owner. Ask additional information and documents, which prove the legal origin of the Client's assets. If there are no other circumstances leading to the higher risk and the MB approves, it is not required to apply enhanced DD measures stipulated in section 10.7.

High risk category II	**DD measures**
The representative or the Beneficial Owner of a legal person is a PEP or his or her family member.	Ask the Client to provide additional information about the need and purpose of establishing the Business Relationship. Ask the Client to provide information about relationships with other credit or financing institutions, and the opinion of the respective credit or financing institution about the Client. Conduct an internet search about the Client, being a legal person, and its Beneficial Owner. Ask additional information and documents, which prove the legal origin of the Client's assets.
There is information that the person is suspected to be or to have been linked with a financial offence or other suspicious activities.	Check information about International Sanctions (see also Section 15)[5] or ask guidance from the CO. Ask additional information and documents, which prove the legal origin of the Client's assets.
A legal person registered outside	Ask the Client to provide additional information about

[5] See footnote 3

	the European Economic Area, whose field of business is associated with a high risk of Money Laundering (see Exhibit 1). A legal person registered outside the European Economic Area, who is operating outside the country of its registered location. A legal person is operating or is registered in a low tax rate country (see Exhibit 1) or the place of residence, place of registration of the legal person, its owners or Beneficial Owners, or the territory of business of the legal person is situated in a country listed in the list of risk countries (see Exhibit 1).	its links with the said foreign state. Ask for additional information about the purpose of establishing the Business Relationship. Verify and compare the data submitted by Client against the additional documents, data or information, which originates from a reliable and independent source (if obtaining such information is possible). Ask additional information and documents, which prove the legal origin of the Client's assets.

10.6. The above listed DD measures can be combined, as appropriate, in respect to other listed or non-listed risks.

10.7. <u>Identification and management of risks of technology and services</u>

10.7.1. Identified RISK Categories:

10.7.1.1. Service Provider Risks

a. Imperfect implementation

b. Improper operations

10.7.1.2. User Related Risks

a. Erasing by Error

b. Forget PIN

c. Loss of the device

10.7.1.3. Risks generated by Third Parties activities

a. Hacking

b. Denial-of-service

c. Spoofing

10.7.2. Risk management

10.7.2.1. Service Provider Risks

10.7.2.1.1. Imperfect implementation. Active monitoring processes and procedures compliance and mitigation through:

10.7.2.1.2. Offline Database

10.7.2.1.3. Log of acceptance test

10.7.2.1.4. Improper operations

10.7.2.1.5. Concerning access Databases. Mitigation through tighter access control

10.7.2.1.6. Concerning Tests. Mitigation through performing tests on different instances

10.7.2.1.7. Concerning upgrades. Mitigation through contingency plans (mostly revert to original status)

10.7.2.2. USER Related Risks

10.7.2.2.1. Erasing by Error. Mitigation through RECOVER procedure.

10.7.2.2.2. Forget PIN. Mitigation through RECOVERY procedure

10.7.2.2.3. Loss of the device. Mitigation through RECOVER procedure

10.7.2.3. Risks generated by Third Parties activities on servers

10.7.2.3.1. Hacking. Mitigation Through:

a. Active monitoring

b. Firewalls

c. Encrypted back-up

d. Offline Databases

10.7.2.3.2. Denial-of-service. Mitigation through:

a. Identify normal conditions for network traffic by defining “traffic patterns”, which is necessary for threat detection and alerting

b. Identifying incoming traffic to separate human traffic from human-like bots and hijacked web browsers.

c. Filtering through anti-DDoS technology like connection tracking, IP reputation lists, deep packet inspection, blacklisting/whitelisting, rate limiting

10.7.2.3.3. Spoofing. Mitigation through one or more of the following methods:

a. Packet filtering

b. Use spoofing detection software:

c. Use cryptographic network protocols like Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS)

10.8. The Provider of service uses safe technological solution for providing services and implements physical and personal measures to keep safety.

10.8.1. The following technological solutions provide a comfortable safety level:

10.8.1.1. Physical safety of background servers: VPS, data centres or controlled access technical rooms

10.8.1.2. Separate test instances (no tests on production machines)

10.8.1.3. Server Internet connection security: at least two different [path and logic] ISP

10.8.1.4. Encrypted and salted Wallet back-up

10.8.1.5. Single Point of Failure avoidance

10.8.1.6. Regular backups

10.8.1.7. Firewalls

10.8.1.8. User Recovery option/User Wallet server copy information stored offline

10.8.1.9. Last version works only (USERs must have last version/revision)

10.8.1.10. Multiple, layered USER authentication factors

10.8.1.11. PIN [personal, 6 digits]

10.8.1.12. SEED [mnemonic Phrase]

10.8.1.13. 2nd Factor Authentication, such:

a. Telephone

b. e-mail
c. Fingerprint
d. Eyeball iris
e. Draw pattern

10.8.1.14. 3rd Factor Authentication, like:
a. Telephone
b. e-mail
c. Fingerprint
d. Eyeball iris
e. Draw pattern

10.9. The Provider of service uses special technical solutions to keep provided service in safe and keeps history of transactions.

10.9.1. Offered service being personal wallet, Service Provider is maintaining/keeping copies of Users transactions (meaning either Send or Receive). Service Provider deploys, as part of the technical solution, one or more Nodes for each blockchain of the wallet supported cryptocurrencies (for each and any cryptocurrency supported by wallet at least one blockchain node is deployed).

10.9.2. User Application maintains on User Device [e.g. mobile phone] lists of last 50 transactions.

10.9.3. Security of transactions involving User wallet and cryptocurrency respective blockchain and/or smart contract only [thus limited to Send and Receive] is provided by blockchain technology itself and by our developed technology:

10.9.3.1. The (operations) records on a blockchain are (by default) secured through cryptography. USERs have their own private keys that are assigned to the transactions they make and act as a personal digital signature. Being not contained in a central location, blockchains (public ones) do not have a single point of failure and cannot be changed from a single computer. It would require massive amounts of computing power to access at least a 51% majority of a certain blockchain and to alter them all at the same time.

10.9.3.2. Service Provider deployed blockchain nodes maintain transactions history and therefore a list of past transactions could be identified for a given public address

10.9.4. As from third parties performing unauthorized transactions from users' wallets perspective, these falls under user's responsibility to avoid dissemination of their private keys, since transactions (Send or Receive) require private keys to be validated by blockchain, and Service Provider has no control on these private keys [neither knowing, accessing or handling unencrypted]

10.10. Authorisation process, securing user accounts. In case of a loss or theft of private cryptographic keys or user credentials by the Clients, the Provider of service has activities to mitigate the risk.

10.10.1. Any User could access his/her wallet through an authorization process, in which several procedures could be employed [at least two are mandatory for users]:

10.10.1.1. Back-up [for Restore purposes only]

10.10.1.2. PIN [personal, 6 digits]

10.10.1.3. SEED [mnemonic Phrase]
10.10.1.4. 2nd Factor Authentication, like:
a. Telephone
b. e-mail
c. Fingerprint
d. Eyeball iris
e. Draw pattern
10.10.1.5. 3rd Factor Authentication, like:
a. Telephone
b. e-mail
c. Fingerprint
d. Eyeball iris
e. Draw pattern

10.10.2. In case of loss or theft, a user will be able to Recover his/her wallet through recovery procedure.
10.10.2.1. This procedure has the following steps [prior user had to install the wallet application on a new device]:
10.10.2.1.1. user requires recovery [of a lost or stolen wallet]
10.10.2.1.2. Service Provider requires the seed [the mnemonic phrase] (in full or partial)
10.10.2.1.3. user is informed that proceeding to recovery makes the usage of former wallet obsolete
10.10.2.1.4. user introduces seed
10.10.2.1.5. user confirms proceeding to recovery
10.10.2.1.6. The seed is required as the only way to decrypt the stored back-up wallet.
10.10.2.1.7. In case user lost the seed there will be no foreseeable means to restore. Service provider is not holding and un-encrypted users' private keys or user seeds.

10.10.3. In case of hacking of the technological solution, the Provider of Services uses following solutions:
10.10.3.1. As the general topology is [Loose] Server – [Strong] Client, Service Provider has the focus on Server and Database part. This implies:
10.10.3.2. Physical databases security [including [wallets] back-ups] (web server and databases will not share the same machines [either physical or virtual]
10.10.3.3. Offline databases server (secured VPN/PN between web-server and Databases)
10.10.3.4. Firewall (on application server layer)
10.10.3.5. Database Encryption
10.10.3.6. Web Server and Database Firewalls
10.10.3.7. Periodical system tape back-up with vault storage
10.10.3.8. Tightly database access
10.10.3.8.1. Strong password (alphanumeric and symbols)
10.10.3.8.2. Password hashes stored encrypted and salted
10.10.3.8.3. Access denied after three (3) unsuccessful attempts
10.10.3.8.4. Access accounts deleted when:

a. Staff is leaving
b. Staff receives other roles
c. Cold/warm copies of current web server [current working version] ready for reinstallation

10.11. Limits set for holding different type of virtual currencies

10.11.1. There is no limit pre-set, apart from the theoretical upper value due to field limit [about 12 digits].

10.11.2. Each USER has for each cryptocurrency an upper limited defined by the cryptocurrency under his/her control.

10.11.3. Note: Several limits are to be applied for EXCHANGE operations, which are out-of-scope for purposes of this document [wallet only]

10.12. Describe how safety is secured in the Provider of service.

10.12.1. Service Provider considers that information security is efficient when:

10.12.1.1. physical security and adequate maintenance of information and technological infrastructure are provided,

10.12.1.2. operational (technical, logical) measures aimed at preventing violations related to the use and operation of systems are being implemented,

10.12.1.3. all information sources are identified, and the ways of their permissible use are prescribed,

10.12.1.4. employees are qualified, aware, vetted and under control,

10.12.1.5. analyses of information risks and business continuity plans are being implemented,

10.12.1.6. it is legitimate and contributes to the fulfilment of organizational strategies,

10.12.1.7. it is compliant with relevant legislation and an explicit information security policy is adopted,

10.12.1.8. security management is present and competent for adopting the right decisions,

10.12.1.9. third-party processes and relationships are formally regulated and abide by the ethical operation principle,

10.12.1.10. organizations adapt to changes in their external environment and follow security trends.

10.12.2. Management commitment to information security

10.12.2.1. Board of Executive Directors is ultimately accountable for corporate governance as a whole. The management and control of information security risks is an integral part of corporate governance. The executive responsibilities for most governance matters is delegated to the Chief Operating Officer (hereinafter COO).

10.12.2.2. The COO gives overall strategic direction by approving and mandating the information security principles and axioms but delegate operational responsibilities for physical and information security to the Security Committee chaired by the COO.

10.12.2.3. CEO and Executive Directors depend heavily on the COO to coordinate activities throughout Service Provider's organization, ensuring that suitable policies are in place to support Service Provider's security processes and procedures. CEO and other Executive Directors also rely on feedback from the Chief Technology Officer, Chief Legal Counsel, Auditors, and other functions to ensure that the procedures, processes and policies are being enforced in practice.

10.12.2.4. The CEO and other Executive Directors demonstrate their commitment to information security by:

a. A statement of support from the CEO;

b. Reviewing and re-approving the processes and procedures every year or whenever is necessary;

c. Approving a specific budgetary element set aside for information security;

Receiving and acting appropriately on management reports concerning information security performance metrics, security incidents, investment requests etc.

10.12.3. Information security coordination. Information security activities is coordinated throughout Service Provider's organization to ensure operating compliance with processes, procedures and policies.

10.12.3.1. The Security Committee, appointed by CEO is responsible for:

10.12.3.1.1. Management for both physical and logical aspects of security;

10.12.3.1.2. Coordinating entire security framework, including the information security controls at all locations;

10.12.3.1.3. Commissioning or preparing information security policy statements, ensuring their compliance with the processes and procedures approved by Executive Directors;

10.12.3.1.4. Periodically reviewing the security policy, processes and procedures, recommending improvements wherever necessary;

10.12.3.1.5. Identifying significant trends and changes to Service Provider's information security risks and proposing to improve information security;

10.12.3.1.6. Reviewing serious security incidents and, where appropriate, recommending strategic improvements to address any underlying root causes;

10.12.3.1.7. Periodically reporting on the status of the security controls infrastructure.

10.12.3.2. All Service Provider's workers will be held to:

10.12.3.2.1. Day-to-day compliance with procedures and processes;

10.12.3.2.2. Upon hire, as a condition of employment, each worker undertakes to comply with Service Provider's information security policies. Any worker failing to comply with the security policies could be subject to disciplinary action, potentially including termination of employment or contract and/or prosecution.

10.13. As a rule, the Provider of service systematically analyses whether adoption of additional security measures is required. The Service Provider employs the following mechanisms to review and if case amend or adopt processes, procedures and methods:

10.13.1. Preventive – settled by Security Committee

10.13.2. Annually review of procedures, processes, methods

10.13.3. Based on efficiency of current procedures and processes

10.13.4. Based on evolution of technology

10.13.5. Monthly analysis on controls, reports, conformity checks

10.13.6. Includes analysis of risks identified as Minor or Informative

10.13.7. Corrective – settled by COO

10.13.8. On each incident [external, either USERs or third parties' actions origins]

10.13.9. On each conformity infringement [internal origins]

10.13.10. On risks identified by Technology Department or any other staff and evaluated as Major or Critical

10.13.11. Service Provider maintains records of Security Committee meeting reports, COO corrective issues settlement decisions, incidents and conformity infringements.

11. Registration and storage of data

11.1. The Representative shall ensure that Client data are registered in the Provider of service's Client database within the required scope.

11.2. Registration of data of a Client who is natural person

11.2.1. The following obtained data shall be recorded in the Provider of service's information system:

i. Name, personal ID code or, in the absence of the latter, date of birth and the address of the person's permanent place of residence and other places of residence;

ii. the name and number of the document used for identification and verification of the identity of the person, its date of issue and the name of the issuing authority;

iii. occupation, profession or area of activity – establish the area of activity (occupation) and the status of the person (trader, employee, student, pensioner);

iv. If the Client is a natural person, the Representative shall record information about whether the person is performing or has performed prominent public functions, or is a close associate or family member of the person performing prominent public functions;

v. Citizenship and the country of tax residency;

vi. the origin of assets.

11.2.2. In case of a representative, the following info shall be recorded:

i. same as provided for in pints i-ii of Section 11.2.1;

ii. the name of the document used for establishing and verification of the right of representation, the date of issue and the name or name of the issuing party.

11.2.3. If the Business Relationship is established by the Client or the representative with the use of the ID card or other e-identification system, the data of the document used for identification is saved automatically in the digital signature. If identification takes place at a face-to-face meeting with the Client, the data of the document used for identification is recorded on the copy of the identification document.

11.3. Registration of data of a Client who is a legal person

11.3.1. The following information on the Client being a legal person shall be recorded:

i. Name, legal form, registry code, address, date of registration and activity locations;

ii. information concerning means of communication and contact person(s);

iii. names of the members of the management board or an equivalent governing body, and their powers to represent the Client, and whether any of them is a PEP;

iv. information about the Beneficial Owners;

v. Field(s) of activity (i.e. the NACE codes);

vi. name and number of the document used for identification and verification of the identity, its date of issue and the name of the issuing authority;

vii. country of tax residency of the legal person (VAT number);

viii. date of registration of the legal person in the Provider of service's database;

ix. purpose of the Business Relationship;

x. origin of assets (normal business operations/other);

11.3.2. The following information about the Beneficial Owner shall be recorded:

i. Name, personal ID code or, in the absence of the latter, date of birth and place of residence;
ii. type of control over the enterprise (e.g. shareholder);
iii. is the person a PEP;
iv. information about the representative as set forth under 11.2.2.

11.3.3. If the Business Relationship is established by the representative of the Client with the use of the ID card or other e-identification system, the data of the document used for identification is saved automatically in the digital signature. If identification takes place at a face-to-face meeting with the representative of the Client, the data of the document used for identification is recorded on the copy of the identification document.

11.3.4. Information from the B-card, i.e. the legal representatives of the Client being a legal person stated on the B-card, shall be recorded on the Client data registration sheet or the contract concluded with the Client.

11.4. The Representative shall record all the data regarding

11.4.1. Provider of service's decision to refuse establishment Business Relationship. The Representative shall record all the data, if, as a result of taking DD measures, a person refuses to establish the Business Relationship.

11.4.2. Impossibility to take DD measures due to information technology means;

11.4.3. Termination of the business relationship, as a result of impossibility to take DD measures;

11.5. Storage of Data

11.5.1. The respective data is stored in a written format and/or in a format reproducible in writing and, if required, it shall be accessible by all appropriate staff of the Provider of service (MB, Representatives, marketing, CO etc).

11.5.2. The originals or copies of the documents, which serve as the basis for identification a person, and of the documents serving as the basis for establishing a Business Relationship, shall be stored for at least five (5) years following the termination of the Business Relationship.

11.5.3. The data of the document prescribed for the digital identification of a Client, information on making an electronic query to the identity documents database, and the audio and video recording of the procedure of identifying the person and verifying the person's identity shall be stored at least five (5) years following the termination of the Business Relationship.

11.5.4. Also to be stored:

i. manner, time and place of submitting or updating of data and documents;
ii. name and position of Representative who has established the identity, checked or updated the data.

12. Reporting

12.1. Notification of the CO

12.1.1. Any circumstances identified in the Business Relationship are unusual or suspicious or there are characteristics which point to Money Laundering, Terrorist Financing, or an attempt of the same the Representative shall promptly notify the CO.

12.1.2. The CO shall analyse and forward the respective information to the MB.

12.2. Notification of FIU

12.2.1. Before reporting any transaction connected with suspected Money Laundering or Terrorist Financing to the FIU, the CO shall analyse the content of the information received, considering the Client's current area of activity and other known information.

12.2.2. The CO shall decide whether to forward the information to the FIU and the MB shall decide whether to terminate the Business Relationship.

12.2.3. The CO shall make a notation "AML" behind the name of the Client in the Provider of service's Client database or on the documents, and shall notify the FIU promptly, but not later than within 2 business days after discovering any activities or circumstances or arising of suspicion, using the respective web-form for notifying the FIU. Copies of the documents as set forth by guidelines of FIU or further requested by FIU shall be appended to the notice.

12.2.4. The FIU shall be notified of any suspicious and unusual transactions where, including such where the financial obligation exceeding 32 000 euros or an equivalent amount in another currency is performed in cash, regardless of whether the transaction is made in a single payment or several related payments.

12.2.5. The CO shall store in a format reproducible in writing any reports received from the Representatives about suspicious circumstances, as well as all information gathered to analyse such notices, as well as other linked documents and notices to be forwarded to the FIU, along with the time of forwarding the notice, and the information about the Representatives who forwarded the same.

12.2.6. The Client who is reported to the FIU as being suspicious, may not be informed of the same.

12.2.7. It is also prohibited to inform any third persons, including other Representatives, of the fact that information has been reported to the FIU, and the content of the reported information, except for the MB/CO.

12.3. Termination of the Business Relationship with a Client in the event of suspected Money Laundering and Terrorist Financing

12.3.1. Pursuant to law, the Provider of service is obliged to extraordinarily and unilaterally terminate the Business Relationship without observing the advance notification period, if:

i. The Client fails to present upon identification or upon updating the previously gathered data or the taking of DD measures, true, full and accurate information, or

ii. The Client or a person associated with the Client does not present data and documents evidencing of the lawfulness of the economic activities of the Client, or

iii. the Provider of service suspects for any other reasons that the Client or the person associated with the Client is involved in Money Laundering or Terrorist Financing, or

iv. the documents and data submitted by the Client do not dispel the Provider of service's suspicions about the Client's possible links with Money Laundering or Terrorist Financing.

12.3.2. The decision on terminating the Business Relationship shall be taken by the Management Board, considering also the proposal of the CO.

12.3.3. The Client shall be notified of the termination of Business Relationship in writing, provided that it is consistent with Section 12.2.7. Notation about the cancellation of the Business Relationship shall be made in the Provider of service's Client database or documentation, and a note "AML" shall be added to the Client's data, provided that it is consistent with Section 12.2.8.

12.4. Indemnification of the Representatives

12.4.1. The Provider of service and its Representatives shall not, upon performance of the obligations arising from the Rules, be liable for damage arising from failure to carry out any transactions (by the due date) if the damage was caused to the persons in connection with notification of the FIU of the suspicion of Money Laundering or Terrorist Financing in good faith, or for damage caused to a Client or in connection with the cancellation of a Business Relationship on the basis provided in Section 12.3.

12.4.2. Fulfilment of the notification obligation by the Representative acting in good faith, and reporting the appropriate information shall not be deemed breach of the confidentiality obligation imposed by the law or the contract, and no liability stemming from the legislation or the contract shall be imposed upon the person who has performed the notification obligation.

13. Implementation of International Sanctions

13.1. The Provider of service is required to implement International Sanctions in force.

13.2. Representatives shall draw special attention to all its Clients (present and new), to the activities of the Clients and to the facts which refer to the possibility that the Client is a subject to International Sanctions. Control and verification of possibly imposed International Sanctions shall be conducted by the Representatives as part of DD measures applied to the Clients in accordance with these Rules.

13.3. The Representatives who have doubts or who know that a Client is subject to International Sanctions, shall immediately notify the CO. In case of doubt, if the CO finds it appropriate, the Representative shall ask the Client to provide additional information that may help to identify whether he/she is subject to International Sanctions or not.

13.4. The CO shall be responsible for the implementation of International Sanctions.

13.4.1. The CO shall:

i. regularly follow the webpage of FIU (https://www.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/) and immediately take measures provided for in the act on the imposition or implementation of International Sanctions;

ii. upon entry into force of an act on the imposition or implementation of International Sanctions, the amendment, repeal or expiry thereof, immediately check whether any of the Clients is subject to International Sanctions with regard to whom the financial sanction is imposed, amended or terminated;

iii. if an act on the imposition or implementation of International Sanctions is repealed, expires or is amended in such a manner that the implementation of International Sanctions with regard to the subject of International Sanctions is terminated wholly or partially, terminate the implementation of the measure to the extent provided for in the act on the imposition or application of International Sanctions;

iv. keep an updated record of subjects of International Sanctions and submit this information to the Representatives in the form that allows to use this information in the course of their activity;

v. provide training to the Representatives that allows them to establish independently the subjects of International Sanctions;

vi. assist the Representatives if they have doubt or knowledge that a Client is a subject to International Sanctions;

vii. supervise the application of the Rules regarding the implementation of International Sanctions by the Representatives;

viii. review and keep updated the Rules regarding the implementation of International Sanctions
ix. notify FIU of Clients who are subject to International Sanctions or in part of whom the CO, the Representatives have doubts;
x. keep record of made checks, notifications submitted to FIU and applied measures in part of detected subjects to International Sanctions.

13.4.2. When making checks on Clients as to detect whether they are subject to International Sanctions, the following information shall be recorded and preserved for five years:
i. Time of inspection;
ii. Name of person who carried out inspection;
iii. Results of inspection;
iv. Measures taken.

13.4.3. If in the course of the check, it shall be detected that a Client or a person who used to be a Client is subject to International Sanctions, the CO shall notify the Representatives who dealt with this Client, the Management Board and FIU. The notification shall be submitted at least in the way that allows its reproduction in writing.

13.4.4. The Client who is subject to International Sanctions and about whom the notification is made, shall not be informed of the notification.

13.4.5. Application of special measures and sanctions on the Client who is detected to be subject to International Sanctions should be authorized by FIU.

13.4.6. When making checks of Clients, the possible distorting factors in personal information (i.e. way of written reproduction of name etc.) must be kept in mind.

14. Training

14.1. The Provider of service shall ensure that all Representatives who have contacts with Clients or matters involving Money Laundering are provided with regular training and information about the nature of the Money Laundering and Terrorist Financing risks, as well as any new trends within the field. The CO shall arrange regular training concerning prevention of Money Laundering and Terrorist Financing to explain the respective requirements and obligations.

14.2. Initial training is provided at the start of representative´s service. The Representatives who are communicating with the Clients directly may not start working before they have reviewed and committed to the adherence of these Rules or participated in the Money Laundering and Terrorist Financing prevention training.

14.3. Training is provided regularly, at least once a year, to all Representatives and other relevant designated staff of the Provider of service. Training may be provided also using electronic means (conference calls, continuous e-mail updates provided confirmation on receipt and acceptance is returned and similar means).

14.4. Training materials and information shall be stored for at least three years.

15. Internal audit and amendment of the Rules

15.1. Compliance with the Rules shall be inspected at least once a year by the CO, whose job duties are set out in Section 4.1.

15.2. The report on the results of the inspection concerning the compliance with the measures for prevention of Money Laundering and Terrorist Financing shall set out the following information:

i. time of the inspection;
ii. name and position of the person conducting the inspection;
iii. purpose and description of the inspection;

iv. analysis of the inspection results, or the conclusions drawn on the basis of the inspection.

15.3. If the inspection reveals any deficiencies in the Rules or their implementation, the report shall set out the measures to be applied to remedy the deficiencies, as well as the respective time schedule and the time of a follow-up inspection.

15.4. If a follow-up inspection is carried out, the results of the follow-up inspection shall be added to the inspection report, which shall state the list of measures to remedy any deficiencies discovered in the course of the follow-up inspection, and the time actually spent on remedying the same.

15.5. The inspection report shall be presented to the MB, who shall decide on taking measures to remedy any deficiencies discovered.

***

Form 1

Client Data

Updated:	Risk category

Client data sheet ('know your customer)

Name, address, etc.	Name	
	Personal code/Date of birth/Registry code	
	Address/Location	
	Citizenship (in case of natural person)	
	Occupation, area of activity	
	Name and date of issuance of document used for identification (in case of natural person and representative of legal person)	
	Name and number of the document used for identification and verification of the identity of a foreign legal person	
	Postal code and city	
	The country of tax residency	
	Area of activity (in case of legal person)	
	E-mail	Telephone
	Contact person and e-mail	Telephone
	Have the securities of the company been accepted for trading on a regulated securities market? (in case of legal person) NO YES, if Yes, then on which securities market?	

Beneficial Owner (in case of legal person)	Record the Beneficial Owners: *A Beneficial Owner is a natural person who:* *i. Taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed taking advantage of his 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.* *ii. Ultimately owns or controls a legal person 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 which is under the control of a natural person holds or multiple companies which are under the control of the same 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. *iii. Holds the position of a senior managing official, if, after all possible means of identification have been exhausted, the person specified in clause ii cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner.* *iv. In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations': settlor or person who has handed over property to the asset pool, trustee or manager or possessor of the property, person ensuring and controlling the preservation of property, where such person has been appointed, or the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.*		
	Does the company have Beneficial Owners: YES NO, if No, please explain:		
	Name	Personal ID code/ DOB	
	Place of residence	Citizenship	
		Shareholding (%)	
	Name	Personal ID code/ DOB	
	Place of residence	Citizenship	
		Shareholding (%)	
	Name	Personal ID code/ DOB	
	Place of residence	Citizenship	
		Shareholding (%)	

Members of the MB (in case of legal person)	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
	Name	Personal ID code/ DOB	

	Place of residence	Copy of the ID document appended YES	Valid till

Authorised persons (representatives)	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
		Power of attorney appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
		Power of attorney appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
		Power of attorney appended YES	Valid till

Purpose of the Business Relationship	Please specify

Identification of Politically Exposed Persons (to be filled if relevant)	Record on the Beneficial Owners, members of the MB or authorised representative a Politically Exposed Person. *A Politically Exposed Person is 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.* *• The provisions set out above also include positions in the European Union and in other international organizations.*

<table>
<tr><td></td><td colspan="3">• A family member of a person performing prominent public functions is the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.
• A close associate of a person performing prominent public functions is a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.
YES
NO
If Yes, please record the person’s name, position (occupation) and links with the politically exposed person.
<table>
<tr><td>Name</td><td>Position (occupation)</td><td>Link</td></tr>
<tr><td>Name</td><td>Position (occupation)</td><td>Link</td></tr>
</table>
</td></tr>
</table>

Exhibit 1

Exhibit 1a. Contracting states of the European Economic Area

Please refer to http://elik.nlib.ee/pohifakte-euroopa-liidust/liikmesriigid-euroopa-majanduspiirkonna-riigid/

Exhibit 1b. Countries who have established Anti-Money Laundering requirements equivalent to the European Union AML framework
Please refer to https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations_en

Exhibit 1c. List of risk countries (countries which according to FATF does not follow requirements of prevention of Money Laundering and Terrorism Financing)

Please refer to: http://www.fatf-gafi.org/countries/#high-risk

Exhibit 1c. List of risk countries (countries which according to the FIU are under big threat of terrorism)

Afghanistan, Algeria, United Arab Emirates, Bahrein, Bangladesh, Egypt, Indonesia, Iraq, Iran, Yemen, Jordanian, Qatar, Kuwait, Lebanon, Libya, Malaysia, Mali, Morocco, Mauritania, Nigeria, Oman, Pakistan, Palestine, Saudi Arabia, Somalia, Sri Lanka, Sudan, Syria, Tunisia, Turkey, Ethnic groups of Caucasus belonging to Russian Federation (chechens,lesgid, ossetians, ingushes etc.)

Exhibit 1d. List of countries that are NOT regarded as low tax rate countries

https://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest