Oubitando OÜ

Reg. No. 14767515

Laki str 4, Tallinn, Republic of Estonia 10621

Internal control system documents for ensuring the compliance with the control requirements of the European Union AML/CFT (AML Policy) and international Sanctions and Reporting procedure

Contents

Chapter 1. General Provisions

1. Terms Used in the AML Policy

1.1. The following terms and abbreviations are used in the AML Policy:

1.1.1. AMLD-4 – Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (*AMLD 4*).

1.1.2. AMLD-5 – Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (*AMLD-5*).

1.1.3. Money Laundering and Terrorist Financing Prevention Act of Estonia – AML law 1.1.4. AML – Anti-money laundering.

1.1.5. AML/CFT – Anti-money laundering/countering the financing of terrorism.

1.1.6. High-risk Third Countries – countries included in the European Union List of High-risk Third Countries determined according to Article 9, Clause 2 of AMLD-4 indicating the high-risk third countries without effective regulatory enactments for the fight against ML and TF or which have refused to cooperate with the international organisations in the prevention of ML and TF.

1.1.7. Contact Person – the person referred to in Clause 4.1 of this AML Policy, responsible for compliance with the requirements of this AML Policy.

1.1.8. Employee – person, who is employed by The Company and who has been assigned duty to perform the actions referred to in this AML Policy under the order issued by the Board of The Company or job description.

1.1.9. AML Policy – this AML Policy and Annexes thereto.

1.1.10. The Company – Oubitando OÜ.

1.1.11. Politically exposed person (PEP)- as said in article 9^1 of AML law.

1.1.12. FIU – National Financial Intelligence Unit (FIU), determined in accordance with Article 4, Clause 2 of AMLD4 as the relevant supervisory and control authority, which controls and supervises compliance with the requirements for prevention of ML and TF and/or the requirements for prevention of infringement of Sanctions in the Country of Registration or in the Country of Economic Activity.

1.1.13. Customer – natural person or legal entity, including a legal arrangement, which purchases goods or services from The Company within the framework of economic activity thereof.

1.1.14. Country of Registration – Member State of the European Union, where The Company is registered.

1.1.15. UBO – ultimate beneficial owner determined according to § 9^1 of AML law;

1.1.16. PEP – politically exposed person determined according to § 9^1 of AML law;

1.1.17. Country of Economic Activity – country beyond the Country of Registration where The Company is engaged in economic activity by using the permanent representation registered in that country, branch, or registration form of other kind.

1.1.18. Sanctions – international and national sanctions.

1.1.19. Goods of Strategic Significance – military and dual-use items determined according to the Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items; 1.1.20. TF – terrorist financing.

1.1.21. Virtual currency – value determined in digital form, which is digitally transferable, storable or tradeable, and which natural persons or legal entities assume as means of payment, but which are not legal means of payment in any of the country or means of payment under the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC;

1.1.22. Custodian wallet service – service, within the framework of which keys are generated for the Customers, or encryption keys of Customers are stored, and which may be freely used to keep, store, and transfer virtual currencies.

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

1.1.24. The remaining terms used in this AML Policy correspond to the definitions determined inAMLD-4 and AMLD-5.

2. Applicable Regulatory Enactments

2.1. The AML Policy is based on:

2.1.1. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

2.1.2. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EK and 2013/36/ES. 2.1.3. Money Laundering and Terrorist Financing Prevention Act of the Republic of Estonia;

2.1.4. International Sanctions Act of the Republic of Estonia.

2.2. The following has been considered during the development of the AML Policy:

2.2.1. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/TI and amending Council Decision 2005/671/TI.

2.2.2. FATF (Financial Action Task Force) International Standards for the Prevention of Money Laundering, as well as Prevention of Financing of Terrorism and Proliferation of Weapons of Mass Destruction as amended in February 2018 (FATF International Standards on Combating Money Laundering and the Financing of the Terrorism & Proliferation);

2.2.3. FATF (Financial Action Task Force) guidelines on politically exposed persons 2013 (FATF Guidance Politically exposed persons (recommendations 12 and 22).

2.2.4. FATF (Financial Action Task Force) guidelines on ascertaining of true beneficial owners 2014 (FATF Guidance Transparency and Beneficial ownership).

2.2.5. FATF (Financial Action Task Force) guidelines risk-based approach principles and procedures 2007 (FATF Guidance One the Risk-based Approach to Combating Money Laundering and Terrorist Financing).

2.2.6. The Commission's report to the European Parliament and the Council of 26 June 2017 on the Assessment of Money Laundering and Terrorism Financing Risks affecting internal market and applying to cross-border actions.

2.3. In case, if The Company is engaged in commercial activity outside the European Union, The Company shall apply requirements of this AML Policy and the requirements laid down by the European Union, as well as the

requirements in AML/CTF laid down by the Country of Registration, except for the case, if the regulatory enactments of the Country of Economic Activity provide for stricter requirements in AML/CTF. If the regulatory enactments of the Country of Economic Activity preclude from application of the requirements of this AML Policy, European Union, and the Country of Registration in AML/CTF in the case laid down in this Clause, The Company shall:

2.3.1. Refrain from establishment of new business relations in that country.

2.3.2. Terminate the existing business relations in that country.

2.3.3. Partly or fully discontinue provision of services.

2.3.4. Liquidate the businesses commenced in that country.

2.3.5. Apply other measures provided for in the regulatory technical standards adopted by the European Commission based on Article 45, Clause 7 of the Directive (EU)2015/849 of the European Parliament and of the Council.

3. The Company's services description and risk assessment

3.1. The company, Oubitando OÜ, with the trade name of Oubitando, with a Reg. No. 14767515, legal address:

Laki str 4, Tallinn, Republic of Estonia 10621.

Oubitado is entitled to provide services for exchanging, circulating, transferring, and storing cryptocurrency to their customers in local offices and worldwide using digital channels for transferring information, currency, and virtual currency. Oubitando is fully regulated and licensed by the Financial Intelligent Unit of Estonia, having the licenses under FVT000028. These licenses are granted by the Financial Intelligence Unit (FIU) that is part of the Estonian Police and Border Guard Board.

Licensed providers of a virtual currency service will have to apply the same AML measures as financial institutions (financial institutions are licensed by the Estonian FSA, Financial Supervisory Authority). That includes: - internal anti-money laundering rules of procedure customized to fit the business model at hand; - Appointing a Compliance officer.

- Undertaking KYC of all their customers; and
- Monitoring the business relationships with the customers.

Oubitando OÜ has started out only as an exchange service (selling crypto directly to customers) and the virtual wallet (store the crypto in the platform), but additional services were added along the way. Oubitando OÜ will provide in the future the following services:

- Crypto Card
- Liquidity provider

3.1.1. Exchange service: The main service Oubitando OÜ offers is an exchange service for buying and selling cryptocurrencies. Oubitando OÜ is an exchange platform, where the clients will buy/sell/exchange the crypto against fiat, or vice versa.

3.1.2. Wallet Service: Oubitando OÜ is a software wallet that can help the user to store, buy, and sell bitcoins or any altcoin. There is also a feature where you can request money, either in Fiat or Crypto. The

wallet also offers a vault where the bitcoins or any altcoin are stored. It is also convenient because you can easily add funds to your wallet.

This wallet ensures that all funds are stored offline. Drives and backups are placed in deposit boxes and vaults for safe keeping. The crypto can directly go the vault and is secured with a password. There is also a choice of creating a group vault but only up to five users. In Oubitando OÜ, we will provide HD wallet. This has more than plenty of advantages. You can have access to your funds with a password instead of a private key, which will be keep it just to make sure you don't lose the funds. You will be able to have multiple addresses inside of the wallet, with the same password.

3.1.3. Crypto-card services: this is a service which Oubitando OÜ will provide in a future. Oubitando OÜ's prepaid card is linked to your Bitcoin account or any other altcoin. The card balance is your available funds. The most popular crypto used for this card, is bitcoin. Having the card will allow to have the following advantage for the clients:

- Best way to save time and money. No need to add beneficiaries, fill in details, wait for hours.
- There are no commissions or maintenance costs on cards. Receive it, fill it, and keep using it.
- Cards will be accepted everywhere, so Make purchases online as well as in physical stores. - The processing speed is very high, So, use you card and make the payment instantly - Our card can be used anywhere in the world, so feel free to carry it on your trip and enjoy the services.
- With our payment method, avoid the headache of transferring your crypto from one wallet to another.
- We have developed a powerful platform so control all your expenses from one app or platform.

3.1.4. Liquidity services: this is a service which Oubitando OÜ will provide in a future. Oubitando OÜ will provide bitcoin or other altcoins where the business will be able to provide the services of buy/selling crypto through our platform. This will a nice advantage as not all the companies can provide these services. They will make use of our licences. Oubitando OÜ is replacing the middleman in the crypto market. Providers purchase large number of cryptocurrencies from companies that issue them.

3.2. For identification, assessment, and analysis of risks of money laundering and terrorist financing related to their activities, the Company prepares a risk assessment, taking account of at least the following risk categories:

3.2.1. risks relating to customers.

3.2.2. risks relating to countries, geographic areas, or jurisdictions.

3.2.3. risks relating to products, services, or transactions.

3.2.4. risk relating to communication, mediation or products, services, transactions, or delivery channels between the obliged entity and customers.

3.3. The steps taken to identify, assess and analyse risks must be proportionate to the nature, size, and level of complexity of the economic and professional activities of the Company.

3.4. As a result of the risk assessment, the Company entity establishes:

3.4.1. Fields of a lower and higher risk of money laundering and terrorist financing.

3.4.2. The risk appetite, including the volume and scope of products and services provided during business activities.

3.4.3. The risk management model, including simplified and enhanced due diligence measures, to mitigate identified risks.

3.5. The Company's risk assessment and risk appetite are an integral part of the present AML Policy.

4. Contact Person (*Compliance officer*)

4.1. Board of The Company shall appoint one or several employees as the persons responsible for the compliance with the requirements of ML and TF, Sanction risk management, and who are entitled to adopt decisions and directly responsible for the meeting of requirements for prevention of ML and TF and infringement of Sanctions and for the information exchange with FIU.

4.2. Contact Person shall be:

4.2.1. Board Member of The Company – legal entity, or

4.2.2. other person, who has been determined as the Contact Person for the compliance with the requirements of this AML Policy by the Order issued by The Company.

4.3. Only a person with the necessary education, professional suitability, ability, personal qualities, experience, and impeccable reputation, which is required for the performance of the duties of the Contact Person may be appointed as Contact Person. The Company shall notify of changes in the composition of the Contact Persons according to the provisions of the regulatory enactments of the Country of Registration.

4.4. Contact Person shall:

4.4.1. Have a good knowledge of the risks related to ML and TF and the regulatory enactments governing this area.

4.4.2. Have a good knowledge of the risks related to infringement of the Sanctions and the regulatory enactments governing this area.

4.4.3. Organise collection and analysis of information applying to unusual transactions or transactions and circumstances suspected of ML or TF, detected while The Company performs its activity.

4.4.4. Report suspicions of ML or TF to FIU.

4.4.5. Provide reports on possible infringements of Sanctions.

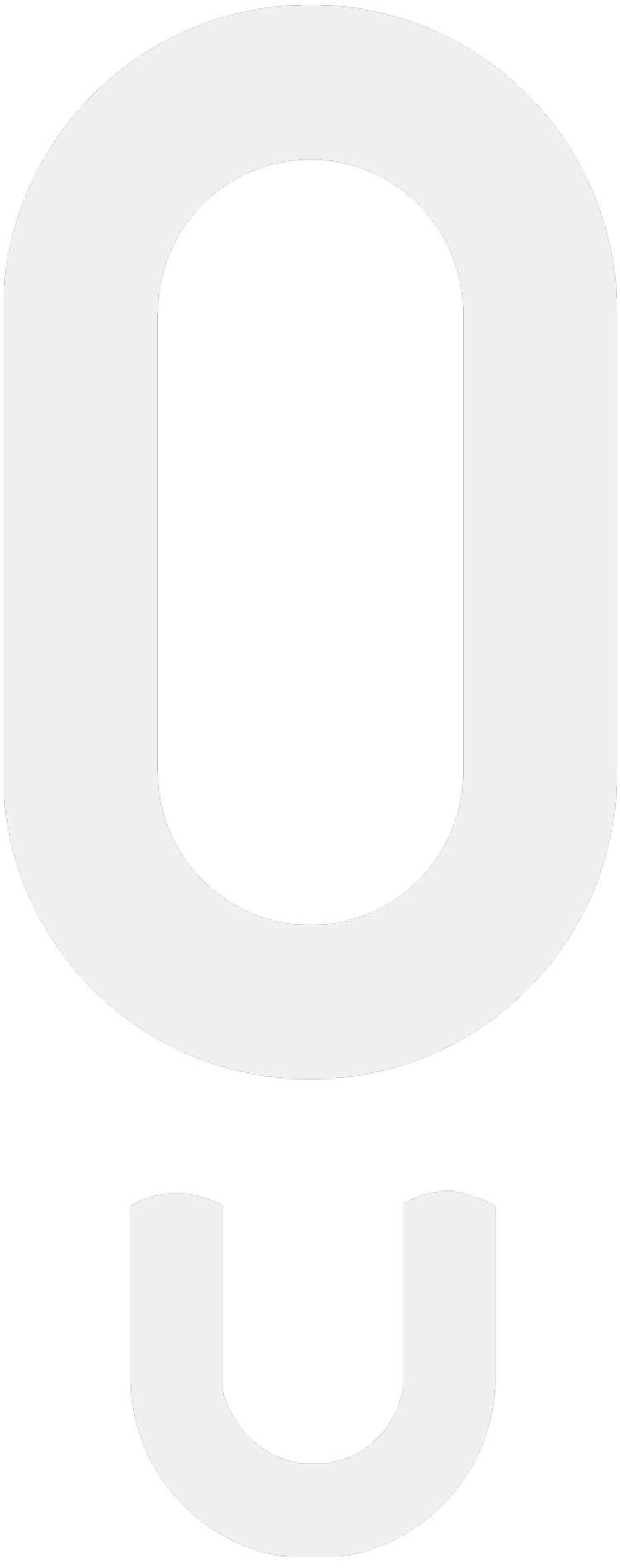
4.4.6. Periodically submit written reports on compliance with the requirements arising from the regulatory enactments of the Country of Registration.

4.4.7. Organise Employee training.

4.4.8. Provide fulfilment of other tasks related to scope of this AML Policy and requirements of the regulatory enactments of the Country of Registration.

4.5. The Contact Person, as well as the Board Member of The Company monitoring the area of prevention of ML and TF shall commence performance of his/her duties immediately after the adoption of the decision by the Board of The Company.

4.6. The Contact Person may delegate performance of certain tasks or duties for ensuring compliance with the requirements of this AML Policy to the Employees of The Company.



Chapter 2. Customer Due Diligence

5. General Provisions for Customer Due Diligence (CDD)

5.1. Customer due diligence and trust verification is a set of measures based on risk assessment, within the framework of which the Contact Person or Employee with the help of the company's third-party verification partners, SUMSUB, shall:

5.1.1. Determine information on the Customer's UBO.

5.1.2. Determine information on the Customer's UBO and relation of the persons related to the Customer to PEP.

5.1.3. Obtain information on the purpose and expected nature of the business relationship.

5.1.4. Obtain information on the Customer's economic or personal activity by determining at least the Customer's branch of activity, region (for legal entities and legal arrangements) or the Customer's occupation, employer, profession (for natural persons).

5.1.5. Provide monitoring of business relationship after commencement of business relationship.

5.1.6. Provide storage and regular update of the documents, data and information obtained during the Customer due diligence.

5.2. Customer due diligence and trust verification measures shall include the following:

5.2.1. Verification of the Customer's identity based on the documents, data or information obtained from the Customer and through the verification thereof using reliable and independent source, including means of electronic identification, relevant trust services, if available, according to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, or any other reliable, remote, or electronic identification processes governed, recognised, approved, or adopted by the Member States of the European Union.

5.2.2. Identification of the Customer's UBO and implementation of reasonable measures to verify identity of the referred person in such a way as The Company is confident that he/she knows, who UBO is, including about legal entities and legal arrangements, by applying reasonable measures to understand the structure of the Customer's property rights and control, including the structure of the Customer's top management.

5.2.3. Assessment and, if necessary, obtaining of information on the purpose and expected nature of the Customer's business relationship.

5.2.4. Constant monitoring of the Customer's business relationship, including monitoring of such verification, which attests that the transactions concluded during the aforementioned relationships are executed in accordance with the information on the Customer, transaction and risk profile, which is at the disposal of The Company, including, if necessary, on origin of the funds, as well as provision of regular update of the relevant documents, data or information.

5.2.5. Ensures fraud mitigation by performing phone and email authentication for all customers using third party authentication partners

5.3 Perform ongoing due diligence for customers based on their risk levels. For Low ML risks customers, they are required to update their KYC details once every five years. Medium ML risk customers are required to update their KYC information once every three years while customers identified as High risk are required to update their KYC details with the company once yearly.

5.4. The Contact Person in addition to the third-party verification partner, SUMSUB, shall conduct the Customer due diligence and assessment of risks of ML, TF, and infringement of Sanctions according to Risk assessment of the Company. Sumsub screens all the information collected by the customers on an average of once daily against adverse media, PEP, and sanctions list

5.6. Considering the ML and TF risks laid down in Risk assessment, as well as the risks of infringement of Sanctions laid down in Clause 23.1 of the AML Policy, public information available on the internet regarding the Customer shall be assessed, including by verifying the information on the Customer's economic activity, Customer's UBO and top management, related companies, persons related to the Customer and such.

5.5. According to the type of economic or personal activity declared by the Customer and considering the risk assessment, The Company shall determine not only name of the type of Customer's 8
economic or personal activity (for example, trade, intermediation in trade transactions, but also more detailed information on the way the Customer organizes his/her economic or personal activity; actual location of economic activity, number of employees of the company; goods and services distribution channels; economic activity of the previous periods and such.

5.6. The Contact Person or Employee may request the Customer additional information at their own initiative to:

5.6.1. Conduct more comprehensive Customer's identification and verify the Customer's UBO and relation of the persons related to the Customer to PEP.

5.6.2. Be able to assess the ML and TF risk inherent to the Customer.

5.6.3. Be able to assess the risk of infringement of the Sanctions inherent to the Customer; 5.6.4. Provide efficient and comparable to the Customer's risk monitoring of the Customers And transactions executed thereby during the business relationship.

5.7. If necessary, the Contact Person or Employee shall provide explanation to the Customer regarding the requirements of the regulatory enactments about the Customer's due diligence, as well as issue to the Customer a written explanation on the necessity of the Customer due diligence.

Chapter 3. Customer Identification

6. General Provisions for the Customer Identification (Know Your Customer)

6.1. All customers must be duly identified and verified:

6.1.1. Before establishing the business relationship, or

6.1.2. Before an occasional transaction without establishing the business relationship.

6.2. Customer Identification before establishing the business relationship shall be conducted, if the Customer is being provided any of the services referred to in Article 2, Paragraph 1 of the AML Directive, or if The Company is able to foresee reasonably that the Customer is to be provided any of the services referred to in Article 2, Paragraph 1 of the AML Directive.

6.3. Customer Identification shall be conducted also before conducting of individual transaction without establishing the business relationship and executing an occasional transaction, if:

6.3.1. The amount of the transaction or the total sum of several seemingly linked transactions is EUR 15,000 or more or is in a foreign currency which according to the foreign exchange rate to be used in accounting at the beginning of the day of executing the transaction is equivalent to or exceeds EUR 15 000.

6.3.2. Transfer of funds is being performed, also including the credit transfer, direct debt transfer, money remittance, or transfer made with a payment card, electronic money instrument, mobile telephone, digital or another information technology device, and exceeds EUR 1000 according to Article 3, Clause 9 of Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

6.4. Additionally, to the provisions of Clause 6.2 and Clause 6.3 of the AML Policy, Customer Identification shall be conducted also in the following cases:

6.4.1. Payment for goods or services or intermediary services related to purchase of these goods or services is made cash or cash for this transaction is deposited in a credit institution to the seller's account in the amount of EUR 10,000 or more, or in a foreign currency which according to the foreign exchange rate to be used in accounting at the beginning of the day of executing the transaction is equivalent to or exceeds EUR 10,000 regardless of whether this transaction is executed as a single operation or several mutually related operations; Note. *When executing cash transactions, The Company shall comply with the limitations set for cash transactions in the Country of Registration or the Country of Economic Activity.* Note.

When executing cash transaction with a Customer, who asserts that he/she has imported the cash necessary for the execution of transaction from non-EU countries, evidence confirming declaration of this cash at the moment of crossing of the border of the European Union according to the provisions of Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community shall be necessary.

6.4.2. If there are suspicions of ML or TF regardless of exceptions, exemptions, or threshold amount in these transactions.

6.4.3. If there is doubt as to credibility or compliance of previously obtained Customer identification data.

6.5. Extraordinary Customer Identification shall be conducted also during the business relationship, before execution of occasional transaction, if:

6.5.1. The transaction conforms to at least one of the indications of unusual transactions laid down by The Company, or if there are suspicions of ML, TF or attempted ML, TF.

6.5.2. There are suspicions of possible infringement of Sanctions.

6.5.3. Change of data certifying identity of the Customer and/or representative thereof obtained before (for example, change of name, surname, company's name etc.).

6.5.4. Change of other data related to the Customer, the change of which may serve as grounds for the determination of higher degree of risk (Customer has obtained status of PEP, changes in the Customer's UBO, corporate structure, change of the Customer's jurisdiction etc.).

6.6. To identify and verify the customer, the Company uses SUM AND SUBSTANCE LTD. ("AML/KYC Partner"). The outsourced partner SUM AND SUBSTANCE LTD checks the customer against International Sanctions, PEPs, Watchlists, and Adverse Media, as well as Identity Document Verification, Face Match and Liveness Check, and Proof of Address Check.

6.7. SumSub is required to examine the validity of the identity document, ensure that the person matches the information on the document, and verify the individual's age when identifying a person. If there is any doubt regarding a person's identification, the appropriate employee is required to request additional information. The SumSub must refuse the customer registration if the document does not match the individual or is invalid.

6.8. SumSub validates the accuracy of customer data by relying on information obtained from a reliable and independent source. When a person is recognized and their identity is validated using electronic identification and trust services for electronic transactions, the person is identified, and their identity is verified using the document. 6.9. The relevant employee has access to the data at any time about any customer.

7. Identification of Natural Persons

7.1. The company's third-party verification partner, SUMSUB shall identify and verify the customer- natural person.

7.2. For conducting identification, a natural person shall be obliged to present an identity document issued in the country of his/her residence indicating at least the person's name, surname, personal identification number (if any), date of birth, number, and date of issue of the identity document, issuing country and authority and with attached photographic image of the person. Also, the customer shall conduct a liveness check to confirm his photograph matches that on his identity document.

7.3.3. To identify UBO and indicate relation thereof to PEP, management must give approval.

8. Identification of Legal Entities

8.1. Sumsub shall identify the Customer – legal entity – by requesting: 8.1.1. To present documents attesting incorporation or legal registration of the legal entity; 8.1.2. To present documents of establishment of the legal entity (Memorandum of Association, Articles of Association).

8.1.1. To provide information on the Customer's declared place of residence and the actual address.

8.1.2. To identify the persons, who are entitled to represent the legal entity based on the authorisation of the office, legal authorisation, or other type of authorisation, and obtain document attesting their rights to represent the legal entity.

8.1.3. To identify UBO and indicate relation thereof to PEP.

8.1.4. To provide information on the structure and management mechanism of the legal entity by also indicating owners and top management officials of the legal entity.

8.2. In addition to Sumsub's dentification of the legal entity, the Contact Person or Employee shall verify in the public registers conformity of the data provided by the Customer to the actual situation on the day, when decision on establishment of business relationship with the Customer is adopted and contract is signed, or occasional transaction is executed.

9. Identification of the Ultimate Beneficial Owner

9.1. Before commencement of business relationship and execution of occasional transaction, Sumsub shall identify the Customer's UBO by obtaining thereon at least the following information:

9.1.2. Name, surname, date of birth, citizenship, state of residence, number, and date of issue of identity document, issuing state and institution.

9.2. When obtaining the information laid down in Clause 12.1, it is determined also, whether the Customer or his/her UBO is a PEP or family member of such person, or a person closely related to PEP.

9.3. When obtaining the information on UBO of the Customer - legal entity or legal arrangement, structure of the shareholders of the relevant person, percentage of the Customer's capital shares or stock owned by the UBO and directly or indirectly controlled, including the ones of direct or indirect participation, in the total amount is also determined, as well as type of the Customer control to be implemented directly or indirectly, and the way of implementation of the Customer's UBO control over the Customer and benefiting from the Customer's economic activity.

9.4. Sumsub shall determine the UBO by identifying and verifying the UBO's identity and verifying this information.

9.5. The Contact Person or Employee shall clearly inform the Customer of his/her duty to immediately notify The Company of any changes in the composition of the UBO thereof.

10. Identification of the Politically Exposed Persons (PEP)

10.1. Before commencement of business relationship or execution of occasional transaction,-Sumsub shall ascertain, whether the Customer or his/her UBO, or persons related to the Customer, are PEP, family member of such a person, or a person closely related to PEP

10.2. In case, if the Customer or UBO thereof is a PEP or family member of such a person, or a person closely related to PEP, The Company shall perform additional measures to determine origin of funds and welfare characterizing the material situation of the Customer and his/her UBO.

10.3. By verifying the accuracy of the information provided by the Customer, The Company shall perform additional verification and:

10.3.1. Obtain information on correspondence of the Customer and/or Customer's UBO to the status of PEP from public lists of PEP.

10.3.2. Obtain information on correspondence of the Customer and/or Customer's UBO to the status of PEP or PEP family member from Declarations of Public Officials.

10.3.3. Pay attention also to the information on correspondence of the Customer and/or Customer's UBO to the status of a family member of PEP or a person closely related to PEP available in mass media and public domain.

10.4. The Contact Person or Employee shall clearly inform the Customer that, if, at the moment of commencement of business relationship, the Customer's UBO is not a PEP or a family member of such a person, or a person closely related to PEP, the Customer shall be obliged to inform The Company immediately, if the UBO obtains the status of PEP, status of a family member of PEP or status of a person closely related to PEP after commencement of business relationship.

11. Identification of the Purposes and Expected Nature of the Business Relationship

11.1. At the moment of commencement of the business relationship, in case, if, based on the ML and TF risk assessment, medium or high ML and TF risk has been established, the Contact Person or Employee shall obtain and document the following information:

11.1.1. On the purpose and expected nature of the business relationship, including the plan services to be provided to the Customer.

11.1.2. On the planned number and volume of transactions.

11.1.3. On the Customer's economic or personal activity, within the framework of which the Customer would use services provided by The Company.

11.2. If the Customer corresponds to the status of PEP, a family member of PEP or a person closely related to PEP, the Contact Person or Employee shall obtain and document information on origin of funds and welfare characterising the material situation of the Customer.

Chapter 4. Simplified and Enhanced Customer Due Diligence

12. Simplified Customer Due Diligence

12.1. In cases of low ML and TF risk, as well as if measures to ascertain, assess and understand the ML and TF risks of its own actions and inherent to the Customer have been implemented, The Company shall be entitled to conduct Customer due diligence by performing the Customer identification actions referred to in Clause – 11 of the AML Policy and the Customer due diligence measures referred to in Clause 12–15 of the AML Policy to the extent corresponding to the character of business relation or occasional transaction and level of the ML and TF risks.

12.2. In case of low ML and TF risk, which does not contradict to the risk assessment, including the national ML and TF risk assessment report, and if measures to ascertain, assess and understand the ML and TF risks of its own actions and inherent to the Customer have been implemented, The Company shall be entitled to conduct simplified Customer due diligence in the cases, if the Customer is:

12.2.1. A Member State of the European Union or the European Economic Area, derived public person, direct administration institution or indirect administration institution of these states, or a capital company controlled by these states or local governments, characterised by low ML and TF risk.

12.2.2. A merchant, the shares of which have been included in a regulated market or several Member States of the European Union or the European Economic Area.

12.2.3. A credit institution or financial institution, which acts in its own name, or a credit institution or financial institution, which is in a contractual or third country of the European Economic Area, which is subject to the requirements equal to AMLD-4 and AMLD-5, and to the state supervision at the place of residence.

12.3. Additionally, to the cases laid down in Clause 15.2 of the AML Policy, The Company is entitled to conduct simplified Customer due diligence in cases, when the Customer's state or territory of residence correspond to any of the following risk reducing conditions:

12.3.1. Member State of the European Economic Area.

12.3.2. Third country with effective AML/CTF systems.

12.3.3. Third country, where according to the report of Transparency International corruption level is low (corruption rating up to 50).

12.3.4. Third country, where according to credible sources, for example, mutual assessment, reports or published post-verification reports, AML/CTF requirements correspond to the updated FATF recommendations and provided that the requirements are efficiently implemented.

13. Enhanced Customer Due Diligence (ECDD)

13.1. Enhanced Customer due diligence shall mean actions for additional Customer due diligence based on the risk assessment to:

13.1.1. Verify that the person indicated as UBO is the actual UBO of the company.

13.1.2. Provide enhanced monitoring over the Customer's transactions.

13.1.3 Verify the customers Source of Fund (SOF) and Source of Wealth (SOW)

13.2. The Contact Person or Employee shall conduct enhanced due diligence in the following cases:

13.2.1. Upon commencement of business relationship with the Customer, who has not participated in the identification procedure in person, except for the case, when:

13.2.1.1. The Company has provided proper measures reducing ML and TF risks, including the development of policies and procedures, and Employee training regarding conducting of non-face-to-face identification.

13.2.1.2. The Customer Identification by using the technological solutions including video identification or secure electronic signature or other technological solutions is conducted in accordance with the procedures laid down in Clause 8 of the AML Policy.

13.2.2. Upon commencement of business relationship with the Customer – PEP, family member of such a person or a person closely related to PEP.

13.2.3. Upon commencement and maintenance of business relationship or execution of occasional transaction with the Customer, whose UBO is a PEP, family member of such a person or a person closely related to PEP.

13.2.4. Upon commencement and maintenance of business relationship or execution of occasional transaction with the Customer, any of the conditions increasing the Customer's ML and TF risk laid down in Clause 23–26 of the AML Policy is identified.

13.2.5. Upon the Customer's risk assessment, medium (increased) or high overall Customer's ML and TF risk is identified.

13.2.6. Upon the Customer's risk assessment, medium (increased) or high overall Customer's risk of infringement of the Sanctions is identified.

13.2.7. The Customer engages in transactions involving persons from High-risk third countries or the place of execution of transactions is in the territory of High-risk third countries.

13.2.8. According to Clause 23.3 of the AML Policy, a group of mutually related Customers has been identified, and any of the Customers of the group is subject to enhanced due diligence, due to which enhanced due diligence is applied also to other Customers of the group of mutually related Customers.

13.2.9. In other cases, upon commencement and maintenance of business relations or execution of occasional transaction with the Customer, if there is medium (increased) or high ML and TF risk and/or medium (increased) or high risk of infringement of the Sanctions.

13.3. In the case referred to in Clause 17.2 of this AML Policy, the Contact Person or Employee shall:

13.3.1. Obtain additional documents or information confirming the Customer's identity.

13.3.2. Request the Customer to submit document confirming that the specified UBO is the Customer's actual UBO.

13.3.3. Summarise additional information on the purpose and type of business relationship, transaction, or activity, as well as verify the submitted information on the basis of additional documents, data or information obtained from reliable and independent source.

13.3.4. Summarise additional information and documents to identify the source and origin of the funds used within the framework of the transactions.

13.3.5. Obtain confirmation of a credit institution or financial institution registered in other Member State of the European Union that the Customer has business relationship with this credit institution or financial institution.

13.3.6. Provide making of the first payment within the framework of the business relationship by using such an account, which has been opened in the Customer's name in a credit institution, which has been registered in the Member States of the European Union or the European Economic Area, subject to the requirements for the prevention of ML and TF arising from the European Union law.

13.3.7. Request Customer's personal presence during the first transaction.

13.3.8. If the Customer is a natural person – resident: obtain information confirming the Customer's identity from the original of the document or the document signed by the Customer using secure electronic signature.

13.4. The Contact Person or Employee shall conduct enhanced Customer due diligence by filling in the form "Customer Due Diligence Form" attached in Annex No. 5 to this AML Policy.

Chapter 5. Recognition and Acceptance of the Results of the Customer Identification and Due Diligence

14. Procedures for the Recognition and Acceptance of the Results of the Customer Identification and Due Diligence

14.1. The Company may partially or completely comply with the results of the Customer identification and due diligence laid down in Clause 5–15 of the AML Policy on the basis of data and documents summarised by other persons, registered and performing their activity in the Member States of the European Union or third countries, which set requirements equal to the requirements of AMLD-4 and AMLD-5 in the area of prevention of ML and TF, if all the following criteria are met:

14.1.1. The Contact Person shall summarise information received from Sumsub on who the Customer is, which establishes business relationship or executes occasional transaction, representative and UBO thereof, as well as the purpose and nature of the business relationship.

14.1.2. The Company has ensured that, if necessary, it may immediately obtain all data and documents, which it relied on by using data summarised by SUMSUB on the results of the Customer identification and due diligence.

14.1.3. The Company has established that SUMSUB, the information obtained by whom it relies on, shall be obliged to meet and actually comply with the requirements, which are equal to the requirements laid down by AMLD-4 and AMLD-5, including the requirements with regard to the implementation of measures of the Customer due diligence, identification of PEP and data storage, is subject to the state monitoring with regard to the meeting of compliance requirements in the area of AML/CTF;

14.1.4. The Company has implemented sufficient measures to ensure compliance with the criteria laid down in Clause 16.1.3 of the AML Policy.

14.2. For the purposes of external services of the Customer identification and due diligence, The Company may conclude a written contract with the person referred to in Clause 16.1 of the AML Policy, if the contract concluded by and between the parties provide that:

14.2.1. External services of the Customer identification and due diligence do not obstruct the activities of The Company or performance of tasks and duties laid down in this AML Policy.

14.2.2. When providing external services, third person performs all duties of The Company it should perform in the process of the process of Customer identification and due diligence.

14.2.3. External services do not obstruct supervision of the structures of The Company;

14.2.4. The Company may provide supervision over the person, who provides external services, including by conducting on-site inspections or other supervisory measures.

14.2.5. External service provider has the necessary knowledge, skills, and abilities to comply with the requirements laid down in this AML Policy.

14.2.6. The Company shall be entitled to verify compliance with the requirements laid down in this AML Policy without limits.

14.2.7. Documents and data obtained during execution of the requirements of this AML Policy and

regulatory enactments are stored, and copies of the documents applying to the identification of the Customer and its UBO or other relevant documents shall be immediately transferred at the request of The Company.

14.3. For the purposes of compliance with the requirements of this AML Policy in case of recognition and acceptance of the results of the Customer identification and due diligence, the Contact Person or the Employee shall:

14.3.1. Request from the persons referred to in Clause 16.1 of this AML Policy information obtained because of the Customer identification and due diligence.

14.3.2. Request information obtained because of the Customer identification and due diligence documents, based on which the Customer identification and due diligence has been conducted from the persons referred to in Clause 18.1 of this AML Policy.

14.4. If the Customer does not provide consent to the transfer of the information and documents laid down in Clause 16.3 of this AML Policy, the Contact Person or the Employee may not recognise and accept the results of the Customer identification and due diligence of the persons referred to in Clause 16.1 of this AML Policy.

14.5. Recognition and acceptance of the results of the Customer identification and due diligence shall not release The Company from compliance with other requirements of this AML Policy

15. Prohibition on making transactions and establishing business relationships

15.1. The Customer due diligence shall be discontinued, and business relationship shall not be started, as well as occasional transaction shall not be executed, if:

15.1.1. Relation of the Customer, Customer's owners, Customer's UBO, representatives and top management (Board Members, Members of the Council, as well as other persons, which may affect the Customer's activity) to the High-risk third countries, which have been included in the European Union List of High-risk Third Countries VPN´s determined according to Article 9 of AMLD-4 indicating the high-risk third countries without effective regulatory enactments for the fight against ML and TF or which have refused to cooperate with the international organisations in the area of prevention of ML and TF, is established, our interface is NOT offered to persons or entities who reside in, are citizens of, are incorporated in, or have a registered office in the United States of America or any Prohibited Localities, as defined below (any such person or entity, a "Restricted Person"). We do not make exceptions. If you are a restricted person, then do not attempt to access or use the Interface. Use of a virtual private network (e.g., a VPN) or other means by Restricted Persons to access or use the Interface is prohibited.

15.1.2. The Customer is a legal entity, which is issuing or is entitled to issue bearer shares or bearer securities of other kind.

15.1.3. During the Customer due diligence, conditions, which overall show high Customer's risk, which is not typical for Customers of such type, are established, and The Company does not want to maintain business relationship or execute occasional transaction with the Customer due to this high risk;

15.1.4. Listing of the Customer, Customer's owners, Customer's UBO, representatives and top management (Board Members, Members of the Council, as well as other persons, which may affect the Customer's activity) or key cooperation partners in the Sanctions lists is established, including - in the Sanctions lists of the US Office of Foreign Assets (OFAC).

15.1.5. During the Customer due diligence before the execution of occasional transaction, information is obtained that the Customer requests to execute a transaction, which would result in infringement of sectoral sanctions.

15.1.6. The Customer does not voluntarily provide the whole information necessary to The Company for comprehensive conducting of the Customer due diligence.

15.2. Upon the Customer's notification of refusal to commence business relationship or execute occasional transaction, The Company shall not be obliged to explain in detail the justification of the adopted decision to the Customer.

Chapter 6. Monitoring of Transactions

16. Monitoring of Business Relationship

16.1. The Company shall provide permanent monitoring of the Customers and the transactions executed thereby including careful investigation of the transactions executed by the Customer to verify that the transactions executed by the Customer correspond to the economic or personal activity declared by the Customer (taking into account also the types and amounts of income declared by the Customer, the Customer's overall level of welfare and proportionality thereof to the executed transactions), and the level of ML and TF risk initially determined for the Customer, as well as risk of infringement of the Sanctions.

16.2. If, prior to the commencement of or during business relationship it shall be found that the Customer is a shell arrangement, the Contact Person or the Employee shall receive the consent of the top management of The Company prior to the commencement or continuation of business relationship, unless the Contact Person simultaneously holds position of the Board Member of The Company.

16.3. After the commencement of business relationship, the Contact Person or the Employee shall perform the following actions on the basis of assessment of ML and TF risks:

16.3.1. Updating of the information on the Customer's economic or personal activity according to Clause 28.6 of the AML Policy;

16.3.2. Permanent monitoring of transactions to verify, if the transactions are not to be considered as unusual or suspicious.

16.4. During the monitoring of business relationship, the Contact Person or the Employee shall pay special attention, in so far as reasonably possible, considering the context and purpose of the transactions, to all transactions of such a kind:

16.4.1. Transactions corresponding to at least one of the following conditions:

16.4.1.1. Complex transactions;

16.4.1.2. Unusually large transactions;

16.4.1.3. Unusually kind of transactions;

16.4.1.4. Lack of obvious economic or legal purpose;

16.4.2. Transactions among several mutually related persons, including transactions among the companies of the group of Customers;

16.4.3. Transactions involving persons from High-risk Third Countries;

16.4.4. Transactions involving persons from the countries or territories, on whom the Sanctions have been imposed by the international organisations or the Country of the Economic Activity.

16.5. The Contact Person shall determine updating of the information on the Customer's economic and personal activity according to the assessment of ML and TF risk, as well as according to the assessment of infringement of the Sanctions.

16.6. According to the degree of ML and TF risk and the degree of risk of infringement of the Sanctions, the Contact Person or the Employee shall perform the actions laid down in Clause 28.3 of the AML Policy:

16.6.1. At least once in 3 (three) months if the Customer corresponds to high ML and TF risk and high risk of infringement of the Sanctions.

16.6.2. At least once in 6 (six) months if the Customer corresponds to medium ML and TF risk and medium risk of infringement of the Sanctions.

16.6.3. At least annually, if the Customer corresponds to low ML and TF risk and low risk of infringement of the Sanctions.

16.7. The Contact Person or the Employee shall determine the Customer's duty to report timely on any changes in the information provided by the Customer, as well as warn of consequences of failure to submit the required information.

16.8. When establishing any of the indications laid down in Clause 28.4.1 of the AML Policy, the Contact Person or the Employee shall request the Customer to submit all the documents, which can prove and justify the nature and purpose of the executed transactions both from the legal and economic viewpoint, as well as eliminate all the reasonable doubt regarding the possible suspiciousness of these transactions.

16.9. To understand the nature of the Customer's economic or personal activity, the Customer may be required to submit documents supporting the transaction or statements of the bank accounts covering the previous period of activity, thus enabling assessment of the Customer's previous transactions, business partners, volume of transactions and compare with the information declared by the Customer to get a complete picture of the Customer's economic activity and volume thereof. The Customer may be required to provide information also on the actual location of the economic activity, where the Customer offers or receives products and services (for example, office address, warehouse address, where the goods offered by the Customer are stored and such), material technical means available for the performance of economic activity, copies of documents attesting the personnel skills etc.

16.10. In any case, when the Contact Person or the Employee establishes that the legal and economic nature of the Customer's transactions is not clearly understandable, the Customer is required to provide explanation on the overall economic activity thereof and the legal and economic nature of the relevant transaction. Information request shall be sent to the Customer's legal address and e-mail address. The Customer shall be provided a reasonable time limit for the submission of this information according to the volume of the required information, but such time limit shall not exceed 45 (forty-five) days.

17. Business Relationship with Politically Exposed Persons (PEP)

17.1. Upon commencement of business relationship with the Customer, during the implementation of measures based on risk assessment, The Company shall verify, if the Customer or the UBO thereof is PEP or a family member of PEP, or a person closely related to PEP.

17.2. If, prior to the commencement of or during the business relationship, it is established that the Customer or the UBO thereof is PEP, or a family member of such person, or a person closely related to PEP, the Contact Person or the Employee shall implement the following measures:

17.2.1. Receive consent of the top management of The Company prior to the commencement or continuation of the business relationship, unless the Contact Person simultaneously holds position of the Board Member of The Company;

17.2.2. Implement and document measures based on risk assessment to determine origin of funds and welfare characterising material situation of the Customer and the UBO thereof. 18.3. According to Clause 29.4.1 of the AML Policy, during the assessment of the risk inherent to the business relationship with PEP, a family member of PEP or a person closely related to PEP, the person of the top management of The Company shall consider at least the following risk factors:

17.3. Whether the person has business interests related to the person's public functions.

17.3.1. Whether the person is involved in the processes of public procurements and has significant impact on the adoption of the crucial decisions.

17.3.2. Whether the person comes from a country, where the FATF or the European Union has identified significant strategic deficiencies in the system for the prevention of ML and TF; 18.3.4. Whether the person comes from a country, which is known as a country with high level of organised crime and/or corruption.

17.3.3. Whether the person implements public functions in sector, which is subject to high risk of corruption (for example, oil and gas extraction, extraction of gold and other minerals, construction, sector of arms and defence, gambling etc.);

17.3.4. Whether the person performs public functions, within the framework of which he/she may affect establishment of system for prevention of ML and TF, as well as anti- corruption system (for example, head of the government, the minister responsible forthe relevant area etc.).

17.4. During the maintenance of business relationship with PEP or a family member of such person, or a person closely related to PEP, The Company shall permanently monitor the transactions executed by the Customer. 17.5. The Company shall pay attention also to the information on action of PEP and possible involvement thereof in illegal activities available in mass media and public domain.

17.6. Considering the fact that the Customer or the UBO thereof may acquire the status of PEP also after the commencement of business relationship, The Company shall periodically verify correspondence of the Customer or the UBO thereof to the status of PEP or a family member of PEP, or a person closely related to PEP according to the degree of risk assigned to the Customer and the monitoring regularity laid down in Clause 28.6 of the AML Policy. Permanent monitoring shall be provided in relation to the Customers from countries with high corruption risk (according to the report of Transparency International, corruption level is high or especially high with the corruption rating from 80).

17.7. On the basis of the risk assessment, The Company shall discontinue application of the enhanced Customer due diligence in relation to the correspondence thereof to the status of PEP, a family member of PEP, or a person closely related to PEP, if:

17.7.1. PEP dies.

17.7.2. PEP no longer holds significant public office for at least 12 months and the business relationship thereof no longer cause increased ML risk.

17.8. In order to assess, whether the business relationship of PEP cause increased ML risk after leaving the office, at least the following risk factors shall be taken into account:

17.8.1. Duration of the level of influence the person may still retain and the influence the person implemented during the exercise of a significant public office.

17.8.2. Whether previous activity of the person is somehow related to the person's activity he/she performs after leaving the significant public office.

18. Monitoring of the Sanctions

18.1. The Company shall perform verification of monitoring of the Sanctions risk regarding the Customer, the Customer's owners, the Customer's UBO, the Customer's representatives and the Customer's top management (Board Members, Members of the Council, as well as other persons, which may affect the Customer's activity). Furthermore, if possible, The Company shall also verify the possible inclusion of the Customer's key cooperation partner in the Sanctions lists.

18.2. When establishing coincidence of the names or titles of the persons referred to in Clause 20.1 of this AML Policy with the information of subjects referred to in the Sanctions lists, The Company shall verify accuracy of this information and perform comparison of data based on the information at the disposal of The Company on the Customer and the related persons thereof. If necessary, The Company shall request from the Customer additional information to ascertain, whether the Customer or any of the related persons thereof is a subject of the Sanctions.

Note. *In cases, when The Company has implemented commensurate and appropriate measures for the assessment of coincidence of correspondence of Sanctions, but information, which would allow to adopt decision on accuracy of coincidence is not available, the Contact Person or the Employee may apply to the FIU with a request to ascertain correspondence of the Customer or the persons related thereto to the status of the subjects of the Sanctions by indicating the information, which is at the disposal of The Company*.

18.3. When identifying any of the persons referred to in Clause 20.1 of the AML Policy as a subject of the sanctions (true coincidence) in the sanctions lists of the United Nations or the European Union, or any other international organisation and/or the Country of Registration and/or the Country of Economic Activity, The Company shall not establish business relationship and refrain also from executing occasional transaction with the Customer concerned, as well as with the legal entities and legal arrangements, which are owned or controlled by these persons, or related in any way to these persons.

18.4. The Company shall reserve rights not to establish business relationship or not to execute transactions related to natural persons or legal entities, including legal arrangements referred to in the Sanctions lists prepared by the US Office of Foreign Assets (OFAC), as well as legal entities and legal arrangements, which are owned or controlled by these persons, or related in any way to these persons.

18.5. For the purposes of identification of possible infringements of the sectoral Sanctions (Sanctions imposed not against particular persons or companies, but with regard to certain territories, goods and services), The Company shall implement appropriate measures for the Customer due diligence and obtain from the Customer additional information on the goods imported or exported by the Customer, regions and countries, to which the goods are being exported, by ascertaining the end user of the goods, obtaining additional information on the Customer's cooperation partners, what kind of transportation and route for the delivery of the goods to the final destination and such.

18.6. If the Customer has been determined low overall risk of infringement of the Sanctions, the Contact Person or the Employee shall separately verify, if the transaction would not result in infringement of the Sanctions in the cases, where the transaction is executed under untypical circumstances or by involving persons, whose country of residence or other circumstances may show on involvement thereof in infringement of the Sanctions, of the transaction is related to the Goods of Strategic Significance.

18.7. If the Customer has been determined medium (increased) or high overall risk of infringement of the Sanctions, the Contact Person or the Employee shall verify that the transaction would not result in infringement of the Sanctions, prior to execution of each transaction. Including the Contact Person or the Employee shall verify that the transaction would not result in indirect bypass of the Sanctions by indirectly using the services provided by The Company for the infringement of the Sanctions.

18.8. In case, if the Customer receives from The Company any services for the actions with the Goods of Strategic Significance, including acquisition of these goods or further transactions therewith, the Contact Person or the Employee shall verify that the Customer prevents transfer of these goods to such persons, who are included in the Sanctions lists.

Chapter 7. Conduct in Case of Suspicion of Money Laundering and Terrorist Financing Action when Detecting Unusual and Suspicious Transaction 19. Detecting Unusual and Suspicious Transaction

19.1. According to this AML Policy, prior to the execution of each transaction, the Contact Person or the Employee shall verify correspondence of the transaction to the indications of unusual and suspicious transaction determined by The Company.

19.2. Transaction corresponding to at least one indication of high ML and TF risk or raising to the Contact Person, or the Employee suspicions related to ML or TF, or attempts of such actions, or other criminal offence related thereto due to any other reason is to be considered as a suspicious transaction.

19.3. The Employee shall report to the Contact Person immediately on any unusual or suspicious actions or transactions referred to in this AML Policy and established during provision of services to the Customer concerned, as well as on transactions involving the Customer, who is suspected of committing terrorist acts or complicity therein and has been included in the list of the persons notified by the FIU.

20. Reporting to the FIU

20.1. The Contact Person shall report to the FIU immediately, but not later than the next business day, on:

20.1.1. Where a business relationship is not established, a transaction or operation is not made or a service is not provided, and the application thereof is considered also in the event of the following reasons:

20.1.1.1. The Company is unable to apply the due diligence measures required under AML law;

20.1.1.2. the Company suspects money laundering or terrorist financing;

20.1.2. Every suspicious transaction established, consulted, planned, applied, initiated, postponed, committed or approved as a result of the analysis;

20.1.3. If, during the Customer's data verification, it has been established that the Customer or 23 persons related thereto have been included in the terrorist lists and suspected of committing terrorist acts or complicity therein;

20.1.4. If the Customer has executed cash transactions for the total amount exceeding the limits for cash transactions determined in the Country of Registration or the Country of Economic Activity (considering, the time limits and other limits laid down in the regulator enactments) regardless of whether there is one or several transactions and regardless of whether its has been completed within a single or several operations.

20.2. Furthermore, the Contact Person shall provide all the possible information on the Customer's transactions at the request of the FIU officials.

20.3. Reports laid down in this Clause of the AML Policy shall be submitted to the competent institution of the country, which, in accordance with Article 4, Clause 2 of the Directive AMLD 4 has been determined as the FIU the Country of Economic Activity of The Company having regard to the procedures laid down in the regulatory enactments of the Country of Economic Activity.

20.4. Guidelines on the characteristics of suspicious transactions: https://www.fiu.ee/en/guidelines fiu/guidelines#guidelines-on-the-ch

20.5. Guidelines for submitting a report to the Financial Intelligence Unit can be found here: https://www.fiu.ee/en/guidelines-fiu/guidelines#guidelines-for-submi

21. Refraining from Executing a Transaction

21.1. The Company shall adopt a decision on refraining from executing a transaction, if the transaction is related to ML or TF, or if there are justified suspicions that it might be related to ML or TF, or if there are justified suspicions that funds have been directly or indirectly acquired from criminal activity or related to attempted TF or this criminal offence.

21.2. If The Company is not able to refrain from executing a suspicious or unusual transaction or refraining from executing such a transaction may provide information helping the persons involved in ML or TF to avoid liability, The Company shall be entitled to execute the transaction reporting accordingly to the FIU after completion thereof.

21.3. Upon refraining from executing a transaction, The Company shall not perform any further activities with the funds involved in the transaction up to the moment when the Subject has received the FIU order to continue or terminate refraining from executing a transaction.

21.4. Upon receipt of the FIU order on discontinuation of the transaction, The Company shall discontinue the transaction and report in writing the Customer, as well as send thereto a copy of the FIU order containing explanation of the procedures for contesting of the order.

21.5. If the Customer has provided a justified information on lawfulness of cash of other funds to The Company, this information shall be sent to the FIU immediately.

21.6. The Company shall terminate refraining from the transaction, if the Subject has not received the FIU order to discontinue the transaction within the set time limit or has received a written notice that further refraining of The Company from executing the transaction is unjustified and is to be terminated.

22. Action when Detecting Infringement of the Sanctions

22.1. According to the provisions of Clauses 19.2–19.2 of this AML Policy, the Contact Person or the Employee may verify also prior to executing the transaction, whether the transaction would not result in infringement of the Sanctions. Verification shall be conducted in accordance with the procedure laid down in Clauses 19.1–19.2 of the AML Policy.

22.2. Having established that the Customer or persons related thereto have been included in the Sanctions lists, the Employee shall report it to the Contact Person immediately. 21.3. When identifying any of the persons referred to in Clause 19.1 of the AML Policy as subject of the Sanctions (true coincidence), The Company shall apply limits laid down by the sanctions and, according to the sanctions risk policy laid down by The Company, refrain from executing also other transactions with this Customer.

22.4. The Company shall adopt decision on refraining from executing a transaction also in case, if the Customer or persons related thereto have not been included in the Sanctions lists, but there are justified suspicions that the transaction might be related to infringement of the Sanctions.

23.5. When identifying unusual and suspicious transaction, the Contact Person shall report to the FIU according to the provisions of Clause 32 of the AML Policy every case involving the following: 23.5.1. The Company refrains from executing the transaction with the Customer on the basis of justified suspicions regarding infringement of the Sanctions;

23.5.2. Business relationship with the Customer has been terminated based on inclusion of the Customer in the international or national Sanctions lists.

23.6. The Company shall strictly comply with and perform the duties imposed by the competent institutions for the control of enforcement of the Sanctions and perform any further actions with the financial funds, property, and items or rights of other kind subject to sanctions in accordance with the AML Policy of the competent authorities only.

Chapter 8. Termination of Business Relationship 23. Termination of Business Relationship

23.1. If the Contact Person or the Employee is unable to implement the Customer due diligence measures laid down in Clause 5–15 of the AML Policy, the service provider shall be prohibited from commencement and continuation of the business relationship (which is to be terminated) and executing occasional transaction with the Customer concerned. The Contact Person shall document and assess each such case and, in case of suspicions regarding ML or TF, report to the FIU.

23.2. If the Contact Person or the Employee does not receive from the Customer true information and documents required for meeting the requirements of Clause 5–15 of the AML Policy within 45 (forty five) days counting from the 1st (first) day of request in the volume, which enables conducting of verification on the merits, the business relationship with the Customer shall be terminated, and the Customer shall be required to perform the obligations early within 30 (thirty) days.

23.3. The Customer shall be informed on termination of the business relationship by sending a notice to the Customer's legal address and e-mail address.

23.4. On the occurrence of the circumstances laid down in Clause 24.1 of the AML Policy, the Contact Person shall decide on termination of the business relationship not only with the Customer concerned, but also with other Customers, which share the UBOs with the Customer, and on request of early performance of the obligations of such Customers.

24. Termination of Business Relationship in Case of the Sanctions

24.1. In any case, when detecting inclusion of the Customer in the Sanctions list, the business relationship with the Customer shall be terminated immediately, and the business relationship shall not be established and occasional transactions shall not be conducted with the Customer up to the moment, when the Sanctions against the Customer are terminated.

24.2. In case of justified suspicions, when there is a justified possibility that the Customer would use the services provided by The Company for infringement of the Sanctions, the business relationship with the Customer shall be terminated immediately, and the business relationship shall not be established and occasional transactions shall not be conducted with the Customer up to the moment, when all
justified suspicions regarding the possible Customer's relation to infringement of the Sanctions are removed.

Chapter 9. Document Storage and Destruction

25. Storage of Acquired Documents, Data and Information

25.1. The Contact Person or the Employee shall document the Customer identification and due diligence measures and pres+ent these documents or submit copies thereof at the request of the FIU.

25.2. The Contact Person and the Employees shall be entitled to electronically process and store the data on the Customers, representatives and UBOs thereof acquired because of the Customer identification and due diligence.

When storing these documents electronically, option of immediate printing or sending thereof electronically to the FIU should be provided.

25.3. The following documents shall be maintained and stored for at least 5 (five) years after the termination of the business relations or execution of occasional transaction:

25.3.1. Copies of documents attesting Customer identification data;

25.3.2. Information on the Customer;

25.3.3. The Customer's notices of UBO;

25.3.4. The Customer's notices of relation of UBO to PEP;

25.3.5. Correspondence with the Customer, including correspondence via electronic mail;

25.3.6. Forms filled in according to the requirements of this AML Policy; 26.3.7. Other documents, including electronic documents, which have been obtained during the Customer due diligence.

25.4. In order to provide transparency of the Customer data and updating of information, the Contact Person or the Employee shall provide registration of the information provided by the Customer in electronic form by filling in the Customer data journal.

25.5. When assessing necessity, proportionality, and justification of further storage, as well as for the purposes of prevention, disclosure or investigation of cases or ML or TF, the time limit referred to in Clause 25.3 may be prolonged at the AML Policy of the FIU or other national security or investigative institution, public prosecutor's office or court for the term not exceeding five years and timely notifying The Company thereof.

25.6. During the storage period of the documents, they shall be available to the Contact Person or the Employees only. The documents referred to in Clause 25.3 of the AML Policy shall be confidential, and during the work with these documents, requirements set for processing of sensitive data of natural persons shall be complied with. Copying of the documents laid down in Clause 26.3 of the AML Policy or forwarding thereof to third parties shall be inadmissible, except for the FIU and other national security or investigative institutions, public prosecutor's office, or court authorities for the performance of lawful duties thereof.

25.7. When performing any actions with the data of natural persons, the Contact Person and the Employees shall comply with the requirements of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

26. Destruction of Documents, Data, and Information

26.1. After the expiry of the time for the storage of documents and information laid down in Clause 26.3 of the AML Policy, Contact Person or the Employees shall organise destruction of the documents and information on persons laid down in Clause 26.3 of the AML Policy.

26.2. Destruction of the documents shall be provided by applying such methods, which provide full destruction of data and 100% confidentiality and by applying Level 3 (three) laid down in the international security standard DIN 32757 Shred Particle Security Levels (or equivalent) or higher.

26.3. An act on the destruction of the documents shall be drawn up describing the destroyed documents, number and type of destruction thereof.

Chapter 10. Providing Enforcement of the AML Policy 27. Providing Compliance with the Requirements of the AML Policy

27.1. The Contact Person and the Employees shall comply with the requirements of the regulatory enactments and this AML Policy.

27.2. The Contact Person and the Employees shall be entitled to request and receive from The Company the information and technical resources required for the performance of the actions laid down in the AML Policy.

27.3. The Company shall assess efficiency of the internal control system at least once in 18 (eighteen) months, including by reviewing and updating assessment of ML and TF risks, as well as assessment of the risk of infringement of the Sanctions related to the Customer, Country of Residence (Registration), Customer's economic or personal activity, used services and products and supply channels thereof, as well as the executed transactions and, if necessary, implement measures for the improvement of efficiency of the internal control system, including by reviewing and clarifying ML and TF prevention policies and procedures, as well as policies and procedures for the prevention of infringement of the Sanctions.

287.4. The Company shall perform reviewing and updating of ML, TF and Sanctions risks at least once in 3 (three) years.

27.5. The Contact Person shall conduct verification of efficiency of the AML Policy at least on annual basis. If this verification shall result in disclosure of deficiencies in the AML Policy, the Contact Person shall eliminate these deficiencies within reasonable period of time.

27.6. Regardless of the set regularity of risk assessment, The Company shall implement repeated risk assessment and measures for the improvement of the internal control system, if the internal control system has any deficiencies or introduction of the activity processes, management structure, provided services and products and supply channels thereof, Customer base or geographical regions of activity of The Company is planned, as well as prior to introduction of new technologies or services.

27.7. The Contact Person or the Employee, who performs the activities referred to in this AML Policy, shall be entitled to request from the Customers of The Company the true information and documents necessary for the due diligence thereof, including on the UBO, transactions executed by the Customers, economic and personal activity, financial situation, sources of cash or other funds of the Customers and the UBO, relation of the Customer and the UBO with PEP and other information, which may be justifiably considered as necessary for the compliance with the requirements of the Law and this AML Policy.

27.8. The Employees of The Company may timely warn the management/supervisory authority on suspicious transactions or the Customer's behaviour, including possible cases of corruption, fraud, malfeasance, or unethical behaviour anonymously (*whistle-blower system*) by sending an anonymous e-mail letter to the Board Member of The Company, who is responsible for the supervision of the area of prevention of ML and TF in accordance with Clause 5.2.1 of the AML Policy.

28. Employee Training

28.1. The Company shall ensure that the Contact Person and the Employees have good command of the risks related to ML and TF, risk related to infringement of the Sanctions, regulatory enactments, and requirements thereof in prevention of ML and TF, requirements of the regulatory enactments in prevention of infringement of the Sanctions and prevent involvement of The Company in ML and TF or attempt of such actions, as well as in infringement of the Sanctions.

28.2. The Company shall ensure regular training of the Contact Person and the Employees in prevention of ML and TF, as well as in infringement of the Sanctions, so they were able to identify transactions of the Customer's actions, whose direct or indirect purposes are related to ML and TF or infringement of the Sanctions, as well as so they knew how to react, if The Company is involved in the aforementioned actions or attempt thereof.

28.3. The Company shall ensure that the Contact Person and the Employees are knowledgeable and competent, have a good knowledge of the requirements of the regulatory enactments and the internal regulatory enactments of The Company and the duties imposed thereon to be able to implement measures of Customer identification, due diligence and monitoring in good quality.

28.4. Training in prevention of ML and TF, as well as in the area of prevention of infringement of the Sanctions shall be provided for all Employees, whose direct professional duties include Customer service and executing transactions with the Customers.

28.5. The Contact Person shall provide Employee training according to the topics determined by The Company: for new employees, who would perform the actions referred to in this AML Policy – within 1 (one) month after recruitment, for current employees, who perform the actions referred to in this AML Policy – at least on annual basis.

28.6. Additionally, to the provisions of Clause 30.5 of the AML Policy, the Contact Person shall provide extraordinary Employee training in the following cases:

28.6.1. New external regulatory enactments in prevention of ML and TF or in the area of Sanctions control applicable to The Company have entered into effect.

28.6.2. Significant changes are in progress in this AML Policy or the Customer risk assessment criteria.

28.6.3. Significant changes have been introduced in the processes of the economic activity of The Company or action has been commenced in new service markets or Customer segments.

28.6.4. New services have been introduced, which cause changes in the exposition of ML and TF risks and/or risks of infringement of the Sanctions of The Company;

28.6.5. During the performance of professional duties, the Employee violates this AML Policy or external regulatory enactments in prevention of ML and TF or in Sanctions control due to insufficient knowledge.

27.7. The Contact Person shall ensure that the Employees confirm hearing of the training programme with their signatures after the training. The fact that the Employee has been trained in prevention of ML and TF, in the prevention of infringement of Sanctions, as well as in work with the internal control system shall be confirmed by the Employee's signature in the AML Policy registration journal. List with the signatures of the Employees

confirming hearing of the training programmes shall be stored at the legal address of The Company for at least 5 (five) years after the end of the relevant training.

29. Liability for Compliance with the Requirements of the AML Policy

29.1. Action taken by the Members of the Council, Board Members, Contact Persons and Employees of The Company within the framework of performance of activities compliant with the requirements of the law shall not be considered as a violation of the requirements of the standards regulating the professional activity or requirements of the monitoring and control authorities.

29.2. If the Contact Person has provided a statement or other information to the FIU according to the requirements of the Law and in good faith, regardless of whether the fact of ML, TF or attempts of such actions, or other criminal offences related thereto is or is not proven in the pre-trial criminal proceedings or court, as well as regardless of the provisions of the mutual contract between the Customer and The Company, provision of information to the FIU is not to be considered as disclosure of non-disclosable information, and, in this regard, The Company, its management (Members of the Council and Board), Contact Persons and Employees shall not be held legally liable, and civil liability shall also be excluded.

29.3. If the Contact Person or the Employee has refrained from executing a transaction in good faith according to Article 35 of AMLD-4, or terminated the business relationship or required early performance of obligations, The Company, its management (Members of the Council and Board), Contact Persons and Employees shall not be held legally liable due this refraining or delay of transaction, termination of the business relationship or requirement for early performance of obligations, and civil liability shall also be excluded.

29.4. If the Customer is deterred from involvement in criminal activities, including by consulting and dissuading the Customer from wrong action, it is not to be considered as disclosure of non-disclosable information, and, in this regard, The Company, its management (Members of the Council and Board), Contact Persons and Employees shall not be held legally liable, and civil liability shall also be excluded.

29.5. Persons shall be liable for the violations of the requirements of this AML Policy in accordance with the procedures laid down in the regulatory enactments of the Country of Registration and/or the Country of Economic Activity.

30. Confidentiality

30.1. The Company shall comply with strict confidentiality regarding all the information received from the Customer for the meeting of requirements of this AML Policy or obtained by indirect receipt of information on the transactions executed by the Customer.

30.2. Confidentiality requirements shall be ignored in the situations laid down in the Law only, by providing reports to the control and monitoring institutions laid down in the regulatory enactments.

30.3. Duty of The Company not to disclose professional secret shall be protected, unless:

30.3.1. The Company personally participates in ML or TF;

30.3.2. Purpose of the provided assistance is ML or TF;

30.3.3. The Company is informed that the service provided to the Customer is required to perform ML or TF.

Chapter 11. Final provisions 31. Providing Compliance with the Requirements of the AML Policy

31.1. The AML Policy shall enter effect at the moment of approval thereof by the Board of The Company.

31.2. The Contact Person shall implement all the required measures to provide full compliance with the requirements of this AML Policy within 1 (one) month from the moment of entry of the AML Policy into effect.

31.3. Matters, which are not stipulated in this AML Policy, shall be resolved in accordance with the applicable regulatory enactments of the Country of Registration and/or the Country of Economic Activity. If any clause of this AML Policy shall contradict the provisions of the regulatory enactments, provisions of the regulatory enactments shall be applied.

31.4. If such a regulatory enactment enters effect, which provides for, stipulates, or imposes different rights and duties of The Company or other persons referred to in this AML Policy, the AML Policy shall be subject to appropriate amendments in accordance with the provisions of this regulatory enactment.

31.5. The Contact Person shall update this AML Policy, as well as Annexes thereto as necessary by transferring appropriate amendments to the AML Policy to the Board of The Company for approval.

31.6. If any of the provisions of the Annexes to the AML Policy shall contradict the general provisions of the AML Policy, the provisions of the Annexes to the AML Policy shall prevail.

31.7. If any of the supplements to the AML Policy or Annexes thereof approved at later date are subject to diverging interpretation, the latest provisions shall prevail.