# RULES OF PROCEDURE

# PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

# And

# INTERNATIONAL SANCTIONS

# FOR IMPLEMENTATION AND MONITORING OF REQUIREMENTS

Approved by the decision of the board

DATE 20.09.2023 no. **1**

**VIRTUAL CURRENCY WALLET, CURRENCY AND VIRTUAL CURRENCY EXCHANGE SERVICE PROVIDER:**

**Register code:** 14707826
**Legal address:** Harju maakond, Tallinn, Kesklinna linnaosa, Pärnu mnt 105, 11312
**Location:**

**The following shall be responsible for drawing up and supplementing the rules of procedure and the internal control rules:**

AML officer

**Contact person**: AML officer

# Contents

# I. DEFINITIONS

**Unusual transactions or activities** are economically unusual or illogical circumstances and activities or activities that are not viable and suggest possible links to money laundering or the concealment of illegal income.

**The EEA** (European Economic Area) is a common economic area comprising the Member States of the European Union and three (EFTA) countries: Norway, Iceland and Liechtenstein [1].
**Company** is Wellex Payment OÜ, reg, nr. 14707826 which provides a virtual currency service. No cash is used in the company's business relationship.

**The FATF** (*Financial Action Task Force*) is an intergovernmental body that sets standards, develops and promotes policies to combat money laundering and terrorist financing. **A medium-risk country** is a **country** other than a low- or high-risk country.

**The customer** is legal entity or a natural person at least 18 years old who uses, has used or has expressed a wish to use the company's services.

**A local person with a national background** is a person with a national background who exercises or has exercised an important public authority function in a Member State of the European Economic Area or in an institution of the European Union.

**The contact person** is a person appointed by the company's management board who is responsible for the company's prevention of money laundering and terrorist financing and compliance with the requirements of an international sanction.

**A high-risk country is:**

- country where reliable sources such as peer evaluations, detailed assessment reports or published follow-up reports pursuant does not set on money laundering and terrorism financing in place effective systems [2];
- a country where, according to reliable sources, the level of corruption or other criminal activity is significant [3];
- a country subject to sanctions, embargoes or similar measures, such as by the European Union or the United Nations [4];
- a country which finances or supports terrorism or in whose territory terrorist organizations designated by the European Union or the United Nations operate.

**The terms of use** is agreement entered into between the company and the customer when establishing a business relationship, using and providing services.

**The low-risk country** is:

- EEA Member State;

- a third country with effective anti-money laundering and anti-terrorist financing systems (other than a high-risk country) [5];
- a third country with low levels of corruption and other criminal activity according to reliable sources [6];
- a third country where, according to reliable sources, such as peer reviews, reports or published follow-up reports, anti-money laundering and anti-terrorist financing requirements are in place in line with the revised FATF Recommendations and are effectively implemented [7]

1 https://elik.nlib.ee/et/pohifakte
2 http://www.fatf-gafi.org/countries/#high-risk
3 https: //www.transparency.org/cpi
4 https://www.sanctionsmap.eu/#/main
5 http://www.fatf-gafi.org/countries/#high-risk
6 https: //www.transparency.org/cpi
7 http://www.fatf-gafi.org/countries/#FATF

**The personnel** is an employee of the company, a manager, a member of the management board.

**The portal** is the company's online environment at www.wellcoinex.com, through which customers can use the service, communicate with the company and perform other operations.

**The FIU (RAB),** ie the Money Laundering Data Bureau, is an independent structural unit of the Police and Border Guard Board, the main task of which is to prevent money laundering and terrorist financing in Estonia. The contact details of RAB are:
Postal address: Pronksi tn 12, Tallinn, 10117
General telephone: (+372) 696 0500
E-mail: info@fiu.ee

**Money laundering** is the laundering of assets derived from, or instead of, criminal activity:
Conversion or transfer for the purpose of concealing the illicit origin of property or of assisting a person who has engaged in criminal activity to evade the legal consequences of his or her actions;
the acquisition, possession or use of property known at the time of its acquisition to have been derived from criminal activity or from participation therein;
concealment of the true nature, origin, location, disposition, transfer or ownership of property or other rights in relation to property.
Money laundering also occurs where the criminal activity which resulted in the laundered assets was carried out in the territory of another country.

**Suspicion of money laundering** is a circumstance or knowledge that indicates that a transaction or activity is intended to commit money laundering or to conceal the proceeds of crime and that due diligence has not been undertaken to eliminate the suspicion.

**An international sanction** is a foreign policy measure aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, respect for human rights

and international law, or other objectives of the UN Charter or the EU's common foreign and security policy.

**An international financial sanction** is an international sanction that:
▪ obliges the freezing of the funds and economic resources of the subject of an international financial sanction ;
▪ the making available of funds and economic resources to the subject of a financial sanction is prohibited;
▪ the granting of loans and credits is prohibited under the conditions prescribed by the legislation implementing the international sanction;
▪ is prohibited under the conditions provided for in the legislation implementing the international sanction
opening and using a deposit, payment, securities or other account;
▪ securities transactions are prohibited under the conditions prescribed by the legislation implementing the international sanction;
▪ the conclusion of an insurance contract under the conditions prescribed by the legislation implementing the international sanction is prohibited;
▪ investment under the conditions provided for in the law implementing the international sanction shall be prohibited; or
▪ it is prohibited to enter into or continue a business relationship, provide advice or provide other financial services related to the activities listed above under the conditions prescribed by the legislation implementing the international sanction .

**The subject of** an international **financial** sanction shall be the one imposing the international sanction or country, territory, territorial unit, regime, an organization, association or grouping, natural or legal person, agency, partnership or any other entity that is subject to an international financial sanction.

**The Rules** are these **Rules** of Procedure.

**A *Politically Exposed Person* (PEP)** is a natural person who performs or has performed important functions of public authority, including:
▪ the head of state, head of government, minister and deputy or assistant minister;
▪ a Member of Parliament or a member of a similar legislative body;
▪ a member of the governing body of a political party;
▪ member of the Supreme Court and the Supreme Court;
▪ member of the Supervisory Board of the National Audit Office and the Central Bank;
▪ Ambassador, Chargé d'Affaires and a senior officer of the Defense Forces;
▪ a member of the management board and administrative or supervisory body of a state-owned company;
▪ the head of an international organization, a deputy head and a member of the governing body, or a person performing equivalent duties who is not a middle or lower-ranking official. A person shall not be considered to be a person with a public background if, at the date of the transaction, he has not exercised an essential function of public authority for at least one year, nor shall the family members and close associates of such a person be considered to be a person with a public background.

**A close associate** of a person **with a national background** is a natural person who is known to be:
▪ the beneficial owner or joint owner of a legal person or legal entity together with a person with a national background or a local person with a national background; or
▪ in a close business relationship with a person with a national background or a local person with a national background and is the sole beneficial owner of a legal person or entity that is known to be effectively established for the benefit of a person with a national background or a local national background.

**A family member of** a **person with a national background** is:
▪ his wife;
▪ a partner equivalent to a spouse according to the law of the person's country of residence or a person who has had a joint household with him or her for at least one year as of the date of concluding the transaction;
▪ his children and their spouses or partners within the meaning of the previous point;
▪ his parent.

**The risk assessment** is an additional document to these rules, in which the company identifies, analyzes and assesses the potential risks of money laundering and terrorist financing related to its economic activities, defines the risk categories and risk appetite and the corresponding risk management model.

**Unusual transactions involving high-risk countries** are unusual circumstances or activities in transactions where at least one party to the transaction is related to a high-risk country.

**A beneficial owner** is a natural person who, by exercising his or her influence, exercises control over a transaction, act or other person and in whose interest, for whose benefit or at the expense the transaction or act is performed. For a company, the criterion for the beneficial owner is ownership (direct) or control (indirect). In the case of direct ownership, a natural person owns at least 25% + 1 of the company. In the case of indirect ownership, the company (ies) owned by the natural person shall own at least 25% + 1 of the shares in the company.
If the final beneficiary cannot be identified, it shall be deemed to be a member of the senior management.

**Terrorism financing** is the allocation or collection of funds, within the meaning of the Penal Code, with a view to the planning or perpetration of terrorist acts or the financing of terrorist organisations, or with knowledge that such funds will be used for the aforementioned purposes.

**Suspicion of terrorist financing** is facts or knowledge that indicate that the transaction or activity is aimed at terrorist financing and that the suspicion cannot be ruled out by the application of due diligence measures.

**A business relationship** is a contract between the company and the customer, based on the relationship, under which the company provides to the customer in its economic and professional activities within the framework of the service. The beginning of a business relationship is considered

to have taken place if the customer has registered as a user of the service (ie provided the company with the data required for identification and agreed to the terms of use) and the company has confirmed the account (ie established the customer's identity).

# II. BASIS OF COMPILATION AND IMPLEMENTATION AND ANNEXES

## 1. Basis of preparation and their implementation

1.1. The company is obliged to establish procedural rules for money laundering and terrorist financing and international sanctions governing the activities of the company and its personnel , which ensure compliance with the relevant legislation and decisions of the governing bodies
1.2. The Management Board ensures the performance of the rules and their compliance with the actual processes by regularly reviewing them at least **once a year** and updating them so as to ensure the protection of the interests of clients and compliance with legislation
1.3. The rules and any amendments thereto shall be established by a decision of the Management Board and communicated to the staff by the Management Board or a person designated by it.
1.4. The established rules and their revisions are binding on both the company and all staff from the moment they are announced . Staff will be signed, which they confirmed the rules of inspection, such an understanding , and the performance acceptance
1.5 Proper compliance with the rules by staff is monitored by a person or management body who directly supervises the person. Violation of the rules is, among other things, the basis of the company's internal to initiate a disciplinary investigation.

## 2. Accessories

2.1. The rules consist of the documents referred to in the rules.
2.2. In addition, the rules as an integral addition to the company's Board of decisions clarifying be amended or supplemented by the rules set out procedures and risk assessment documents.

# III. MAINTENANCE MEASURES

## 1. General information

1.1. The purpose of the application of due diligence measures is to prevent the use of criminal assets and terrorist financing in the company's economic activities.
1.2. The company applies due diligence measures:
1.2.1. establishing a business relationship;
1.2.2. money laundering or terrorist financing and/or an unusual transaction, etc. in case of doubt, guided by the circumstances set out in Annex 1;

1.2.3. in case of suspicion of inadequacy or inaccuracy of documents or data previously collected in the course of identification and verification of submitted documents or updating of data.

1.3. The company and its staff are obliged to pay close attention to the client's activities and circumstances that indicate money laundering and/or terrorist financing or which is likely to be involved in money laundering and/or terrorist financing.

1.4. The Company applies due diligence measures to the extent appropriate and necessary based on the nature of the business and the level of risk of the customer . Due diligence measures are appropriate and necessary in scope than those using is able to determine the make - money laundering and terrorism suspicious and unusual transactions, as well as transactions which do not have a reasonable economic substance or which at least contribute to the achievement of those objectives. In identifying suspicious transactions, the company proceeds from, among other things. the characteristics specified in Annex 1 to these Rules.

1.5. The Management Board shall give its consent to the establishment or continuation of a business relationship with a person with a national background and a person with a local national background.

## 2. Due diligence measures applicable to the establishment and duration of the business relationship

2.1. The usual due diligence measures apply to a client with a low to medium risk profile and include the company /staff member:

2.1.1. establishes the identity of the customer on the basis of the data and documents specified in clauses IV 2) and 3);

2.1.2. verifies the information and documents provided by the customer for identification from reliable and independent sources;

2.1.3. identifies the identity and right of representation of the client's representative and verifies the information received from reliable and independent sources, incl. the scope and rights of the mandate to establish a business relationship;

2.1.4. identifies the actual beneficiary (ies);

2.1.5. identify, on the basis of information obtained from reliable and independent sources, whether the customer, the customer's legal representative (s) or the beneficial owner (s) is a PEP, a member of its family or a close associate and /or the subject of an international financial sanction;

2.1.6. continuously monitors the business relationship, including during operations carried out and their volume controlled by the customer's identity is detected used data and performs if necessary their modernization and risk profile of the re-evaluation **annually** ;

2.1.7. inform the contact person of situations where the transaction is suspicious, ie. there are indications of money laundering or terrorist financing in the content of the transaction or in the activities of the client.

2.2. Enhanced due diligence measures apply to a customer with a high risk profile and the company:

2.2.1. performs the identification of the client on the basis of the data and documents specified in clauses IV 2) and 3);

2.2.2. obtains additional information on the purpose, causes and nature of the business relationship and the transaction upon identification of a natural person;
2.2.3. asks the client , if necessary, if the relevant information is not available, for additional information on the origin and wealth of the persons involved, the beneficiaries and their funds ;
2.2.4. monitors continuously the business relationship, including the business relationship cycle executed transactions and verifies the client's identity identification of used data and performs , if necessary, their updating and the customer's risk profile, re-evaluation **every half a year.**
2.2.5. inform the contact person of situations where the transaction is suspicious, ie. there are indications of money laundering and terrorist financing in the content of the transaction or in the activities of the client;
2.2.6. asks management for consent to enter into a business relationship or transaction if the customer is a PEP, a family member or a close associate.

## 3. Risk appetite and risk assessment in the application of due diligence measures

The company determines the risk profiles of customers, evaluates and takes into account the establishment and duration of a business relationship, incl. possible money laundering and terrorist financing risks and implement the necessary measures to mitigate them as reflected in the company's risk assessment document.

## 4. The company shall not establish a business relationship.

4.1. persons whose identity cannot be established or whose right of representation cannot be verified;
4.2. a person who is not at least 18 years of age;
4.3. a natural person who wishes to use a representative;
4.4. with a person who is himself or whose legal representative or beneficial owner is the subject of the financial sanction;
4.5. a person for whom it is not possible to identify the beneficial owner except in the case of housing and building associations, public and listed companies;
4.6. a person in respect of whom there is a reasonable suspicion of money laundering and /or terrorist financing or an undercover agent;
4.7. a legal person whose business is related to the arms industry, the sale or brokering of weapons;
4.8. a person who does not provide additional information and /or documents within a reasonable time if the company so requests;
4.9. a person who does not confirm acceptance of the Terms of Use;
4.10. with the person if the bearer securities constitute his or her capital represented.

# IV. IDENTIFICATION

## 1. General information

1.1. The identity of all persons and their representatives entering into a business relationship with the company must be verified. Public identification of a person does not preclude the fulfillment of the obligation to identify.
1.2. The Company shall ensure that staff and contact persons have access at all times during working hours to correspondence, data, documents relating to the identification of customers and the implementation of other appropriate due diligence measures, as necessary to perform their duties.
1.3. In the case of outsourcing of identity verification activities, the Company shall ensure that the service provider is informed of the requirements set out in these Rules and in the relevant legislation, is trained and is able to properly comply with the requirements arising therefrom.
1.4. All possible means shall be used to verify identity.
1.5. The Company will provide the customer with more detailed information on the means, procedures, etc. of identification on its portal.
1.6. Identification is not required for the performance of activities with informative content, i.e. activities without legal consequences.
1.7. The data collected for the purposes of identification, as well as for the purposes of monitoring the business relationship, will be checked against available public or paid registers/databases, and internet search engines. If necessary, the company has the right to request additional information or documents from the customer.
1.8. When establishing a business relationship with a customer with a high risk profile, or if such a circumstance becomes apparent during the course of the business relationship, the contact person must be informed immediately.
1.9. If, during the course of the business relationship, it becomes apparent that the Customer can no longer have a business relationship with the Company on the grounds set out in clause 4 of Part III, the Company will immediately terminate the business relationship with that person and inform the Contact Person.
1.10. In the event that any documents provided by the Customer are in a foreign language, the Company shall have the right and the Customer shall have the obligation to provide a translation into English.
1.11. Failure by the Customer to provide the required documents or the provision of false information shall be considered fraudulent and shall result in the suspension of the Service or the termination of the Contract. contract without prior notice and to immediately inform the contact person.

## 2. Identification of the natural person

At the establishment of the business relationship or during the course of the business relationship, the identity of the natural person and the representative of the legal person shall be verified by means of information technology without being present in the same place as the person ITDS §2 par. 2 of the ITDS and complying with the requirements of Section 16 of the ITDS and the requirements of the chapter on the type of identity document concerned, in accordance with one of the procedures set out in Sections 2.1 to 2.2.8.

### 2.1. A low-risk natural person client

2.1.1. The Company will identify the customer as follows if:
2.1.1.1. the client is domiciled in a low-risk country;
2.1.1.2. the expected volume of transactions per year does not exceed 15,000 euros; and
2.1.1.3. there are no indications of medium or high risk in the risk assessment.
2.1.2. In order to establish identity, the customer submits the following information about himself /herself on the company portal:
2.1.2.1. first and last name;
2.1.2.2. the country in which he has his habitual residence;
2.1.2.3. e-mail address;
2.1.2.4. expected volume of transactions per year (in euros);
2.1.2.5. information on whether he is a PEP, a member of his family or a close associate.
2.1.3. In order to establish identity, the customer provides the following confirmations on the company's portal:
2.1.3.1. he is the beneficial owner of the transaction;
2.1.3.2. he agrees to the terms of use of the services;
2.1.3.3. he has provided the company with correct, accurate and truthful information and has not provided information in respect of which the company may have a legitimate interest.
2.1.4. In addition, the company sends a letter to the customer, through which the customer confirms the correctness of his e-mail address.
2.1.5. In order to establish identity, the customer shall provide the company with:
2.1.5.1. a color photograph showing the facial image of the customer and the photograph (page) side of the identity document used for identification;
2.1.5.2. color photo identity detection used in personal identification document, on which the names nationality, personal identification number or date of birth the document number, the issuer of the document and the date of issue and validity date. The above photo quality should be such that it allows the company to clearly read the data on the identity document, revealed by a person from a photograph to compare the same photo the apparent identity be proved to be from the document the apparent person's facial image and make sure that it is not photomontage or corrupted or falsified documents.
2.1.6. Upon receipt of the information and documents referred to in points 2.1.2 to 2.1.5, the company shall:
2.1.6.1. compares the photo on the document to the photo of the customer who identifies it uses to identify that:

2.1.6.1.1. the person is externally similar and age-appropriate to the appearance of the person depicted in the photograph of the document and to the information visible on the document;

2.1.6.1.2. it is not a photomontage, and that the identity document shown in the photograph document has not been tampered with or falsified, and verifies that the photograph was taken immediately before or during the customer identification process.

2.1.6.2. verify the validity of the document from an appropriate freely accessible and reliable database;

2.1.6.3. checks from freely accessible and reliable databases that the customer is not subject to international financial sanctions subject and /or national background, incl. local national background, person, its family member or close associate.

2.1.7. Customer 's identity shall be deemed to be established, if the client and the data obtained from the data is consistent and there is no basis for questioning to make sure that the customer is the person he claims himself to be , and does not occur in middle or high risk circumstances referring to.

2.1.8. If the entity has doubts about the identity of the customer or circumstances indicating a medium or high risk category, the provisions of clauses 2.2 and 2.2.8 of this Part or Part V shall apply.

2.1.9. To fulfill the requirements mentioned in section 2.1, the company may use a professional identification and sanctions screening service provider. Such a company in this case is the service Veriff.

## 2.2. Natural person client with medium risk profile

2.2.1. The Company will verify the identity of the customer in accordance with the procedure set out below, if: 2.2.1.1. the customer is permanently resident or located in a medium risk country; and/or 2.2.1.2. the expected volume of transactions per year is between EUR 15,000 and EUR 30,000; and 2.2.1.3. there are no indications of high risk as set out in the risk assessment.

2.2.2. In order to verify the identity of the Customer, the Customer will provide the following information about himself/herself on the Company Portal:

2.2.2.1. first name and surname;

2.2.2.2. the country in which he or she has his or her permanent residence or domicile;

2.2.2.3. e-mail address;

2.2.2.4. the expected volume of transactions per year (in EUR);

2.2.2.5. address of permanent residence (country, county/city, postcode, street, house, apartment);

2.2.2.6. information on whether he/she is a PEP, a member of his/her family or a close associate.

2.2.3. The customer will provide the following confirmations in the Company Portal to verify his/her identity:

2.2.3.1. he or she is the beneficial owner of the transaction;

2.2.3.2. he/she agrees to the Portal User Terms;

2.2.3.3.he has provided the Company with correct, accurate and truthful information and has not omitted any information in respect of which the Company might have a legitimate interest.

2.2.4. In addition, the Company will send a letter to the customer's e-mail address in which the customer undertakes to confirm the accuracy of his e-mail address as described.

2.2.5. For the purpose of identification, the Customer shall provide the Company with:

2.2.5.1. a colour photograph showing the customer's facial image and the (page) side of the identity document used for identification purposes;

2.2.5.2. a colour photograph of the identity document used for identification purposes, showing nationality, identity code or date of birth, the number of the document, the issuer of the document and the date of issue and validity of the document. The quality of the above-mentioned photograph must be such as to enable the company to read the information on the identity document clearly, to compare the person in the photograph with the face on the identity document in the same photograph, and to ensure that it is not a photomontage or a tampered or falsified document;

2.2.5.3. a utility bill, bank statement, tax return, etc. document showing the customer's name, address, date of issuance/issuance, the title of the document (invoice, driver's license, etc.), details of the issuer of the document, and which is not older than three (3) months. The address on this document must match the details provided by the custome, must not be a letterbox address and must be in a format (.jpg)/(.png) accepted by the company.

2.2.6. Upon receipt of the information specified in points 2.2.2 - 2.2.5, the company:

2.2.6.1. compares the photograph on the document with the photograph of the customer who will use it to identify him or her to ensure that:

2.2.6.1.1. the person is similar in appearance and age to the person depicted in the photograph and to the information visible on the document;

2.2.6.1.2. it is not a photomontage and that the identity document shown in the photograph has not been tampered with or falsified and verifies that the photograph was taken immediately before or during the customer identification process.

2.2.6.2. checks the validity of the document against an appropriate, freely accessible and trustworthy database;

2.2.6.3. compares the information contained in the document referred to in clause 2.2.5.3 with the information provided by the customer and verifies that the document is not. photomontage or similar. and does not show signs of tampering or deterioration;

2.2.6.4. check whether the issuer of the document in 2.2.5.3 actually exists against public databases;

2.2.6.5. verifies from freely accessible and trustworthy databases that the customer is not a subject of an international financial sanction and/or a person with a national background, including a local person with a national background, a family member or a close associate.

2.2.7. The identity of the customer shall be deemed to be established if the data obtained from the customer and from the databases are consistent and there is no reason to doubt that the customer is that person,who he claims to be.

2.2.8. In the event that the identity of the Customer is in doubt or circumstances indicating a high risk category exist, the provisions of paragraph 2.2.8 or Part V of this Part shall apply.

2.2.9. To fulfill the requirements mentioned in section 2.2, the company may use a professional identification and sanctions screening service provider. Such a company in this case is the service Veriff.

## 2.3. Individual with a high-risk profile

2.3.1. The Company will verify the identity of the Customer in accordance with the procedure set out below if:

2.3.1.1. the customer is permanently resident or domiciled in a high risk country; and/or

2.3.1.2. the expected volume of transactions per year exceeds EUR 30 000; and/or

2.3.1.3. the customer declares that he/she is a PEP, a member of his/her family or a close associate;

and/or

2.3.1.4. there are any other elements of high risk identified in the risk assessment.

2.3.2. In order to verify the identity of the customer, the customer will provide the following information on the company portal the following data:

2.3.2.1. first name and surname;

2.3.2.2. the country in which he or she has his or her permanent residence or domicile;

2.3.2.3. e-mail address;

2.3.2.4. the expected volume of transactions per year (in EUR);

2.3.2.5. address of permanent residence (country, county/city, postcode, street, house, apartment);

2.3.2.6. information on whether he/she is a PEP, a member of his/her family or a close associate;

2.3.2.7. the purpose, reason and nature of the business relationship and transaction;

2.3.2.8. the name of the employer;

2.3.2.9. net income;

2.3.2.10. the source of funds and wealth.

2.3.3. To verify identity, the customer will provide the following confirmations to the Company:

2.3.3.1. he or she is a beneficial owner of the transaction;

2.3.3.2. he/she agrees to the User Terms;

2.3.3.3. he has provided the Company with correct, accurate and truthful information and has not omitted any information in respect of which the Company might have a legitimate interest.

2.3.4. In addition, the Company will send a letter to the customer's e-mail address in which the customer undertakes to confirm the accuracy of his e-mail address as described.

2.3.5. For the purpose of identification, the Customer shall provide the Company with:

2.3.5.1. a colour photograph showing the customer's facial image and the side of the identity document used for identification purposes;

2.3.5.2. a colour photograph of the identity document used for identification purposes, a document showing nationality, identity code or date of birth, document number, issuer and date of issue and validity. The quality of the above-mentioned photograph must be such as to enable the company to read the details of the identity document clearly, to compare what is visible in the photograph with what is not visible in the photograph.

The face of the person in the identity document in the same photograph and check that it is not a photomontage or a falsified or forged document;

2.3.5.3. a utility bill, bank statement, tax return or similar document showing the name, address and date of issue/collection of the customer, the name of the document (invoice, driver's licence, etc.), the identity of the issuer of the document and that it is no more than three (3) months old. The address on this document must match the details provided by the customer on the portal, must not be a letterbox address and must be in a format (.jpg)/(.png) accepted by the company.

2.3.5.4. a document proving the origin of the funds and the source of the wealth, showing the name of the customer, the date of issue/collection, the title of the document (contract for the sale of property, etc.), the identity of the issuer of the document, and which is not older than three (3) months. The information on this document about the origin of the client's funds and the source of the wealth must match the information provided by the client to the company and must be in a format (.jpg)/(.png) acceptable to the company.

2.3.6. . Upon receipt of the information specified in points 2.3.2 to 2.3.5, the company:

2.3.6.1. compares the photo on the identity document with the photo of the customer who uses it for identification purposes to ensure that:

2.3.6.1.1. the person is similar in appearance and age to the person depicted in the photograph and to the information visible on the document;

2.3.6.1.2. the photograph is not a photomontage and that the person in the photograph. The identification document has not been tampered with or falsified and checks that the photograph was taken immediately before or during the identification process.

2.3.6.2. checks the validity of the document against an appropriate, freely accessible and trustworthy database;

2.3.6.3. compares the data contained in the documents referred to in clauses 2.3.5.3 and 2.3.5.4 with the data provided by the customer and verifies that these documents are not photomontages, etc. and do not show signs of falsification or deterioration;

2.3.6.4. check whether the issuer of the documents referred to in clauses 2.3.5.3 and 2.3.5.4 actually exists by consulting public databases;

2.3.6.5. verifies from freely accessible and trustworthy databases whether the client is a person with a national background, including a local person with a national background, a member of his/her family or a close associate, and makes sure that the client would not be. Subject to international financial sanctions.

2.3.7. The identity of the customer shall be deemed to be established if the information received from the customer and from the databases is consistent and there is no reason to doubt that the customer is who he or she claims to be.

2.3.8. In the event that the identity of the Customer is in doubt, the following shall apply in Part V.

2.3.9. To fulfill the requirements mentioned in section 2.3, the company may use a professional identification and sanctions screening service provider. Such a company in this case is the service Veriff.

## 3. Identification of a legal person

At the time of the establishment of the business relationship or during the course of the business relationship, but before the transaction is completed, the identity of the legal entity customer shall be established by means of information technology without the customer being present in the same place as the legal entity customer in accordance with one of the procedures set out in points 3.1 to 3.3.

3.1. Low-risk profile legal entity customer.

3.1.1. The Company will verify the identity of the legal entity customer in accordance with the procedure below if:

3.1.1.1. the customer is domiciled and has its place of business in a low-risk country;

3.1.1.2. the customer's legal representatives and beneficial owners are permanently resident or domiciled in a low-risk country;

3.1.1.3. the client's business activity is other than a high-risk business activity as set out in the risk assessment;

3.1.1.4. the expected annual transaction volume is up to EUR 25 000;

3.1.1.5. there are no other circumstances indicating medium or high risk as set out in the risk assessment.

3.1.2. For the purpose of verifying the Customer's identity, the Customer shall provide the Company with the following information about the Customer:

3.1.2.1. business name and legal form;

3.1.2.2. the registration number or registration number and the time;

3.1.2.3. the country of actual residence;

3.1.2.4. the country of registered office;

3.1.2.5. telephone number;

3.1.2.6. e-mail;

3.1.2.7. website address;

3.1.2.8. main activity;

3.1.2.9. the name, number, date of issue, period of validity and the issuer of the licence (where required, i.e. where authorisation is compulsory for the pursuit of the activity in question);

3.1.2.10. . the name of the representative and the basis for the right of representation (if the representative is an authorised representative, the names and dates of birth of the members of the board of directors);

3.1.2.11. . details of the owners and beneficial owners holding at least 25%:

3.1.2.11.1. . for the company: company name, registration code, country of registered office, country of establishment, percentage of ownership;

3.1.2.11.2. . for natural persons: name and surname, date of birth, country of permanent residence or domicile, position, percentage of ownership.

3.1.2.12. . information on whether the legal representatives or beneficial owners are PEPs, including local PEPs, family members or close associates of such person.

3.1.3. The Customer shall further provide the Company with the following confirmations:

3.1.3.1. he or she, his or her legal representatives or beneficial owners are not. subjects of international financial sanctions;
3.1.3.2. holds an authorisation, if an authorisation is required for the pursuit of its activity;
3.1.3.3. he/she agrees to the User Terms;
3.1.3.4. he has provided the Company with correct, accurate and truthful information and has not omitted any information in respect of which the Company might have a legitimate interest.
3.1.4. . In addition, the Company will send a letter to the customer's e-mail address in which the customer undertakes to confirm the accuracy of his e-mail address as described.
3.1.5. For identification purposes, the Customer shall provide the Company with:
3.1.5.1. a copy of the document proving registration in the country of residence or any other relevant document not older than six (6) months showing, inter alia, the identity of the legal representative. If necessary, the customer undertakes to provide this document, notarised and apostilled.
3.1.5.2. the basis of the legal representative's right of representation, in case of an authorised representative, a notarised and apostilled power of attorney;
3.1.5.3. a copy of the licence or a reference to the place where the company can check it.
3.1.6. After receiving the information specified in points 3.1.2 to 3.1.5, the company: 3.1.6.1. compares the information contained in the documents provided by the customer with the information provided by the customer and verifies that these documents do not show signs of falsification or tampering and are valid;
3.1.6.1. checks the public databases to verify whether the issuers of the documents submitted actually exist;
3.1.6.2.verifies, from freely accessible and reliable records, that the customer, his legal representatives or beneficial owner. Not be subject to international financial sanctions and/or have a national background, including. A local person of national origin, a member of their family or a close associate.
3.1.7. The identification of the representative of a legal person shall be subject to the procedures for the identification of natural persons set out in this document.
3.1.8. The identity of the customer shall be deemed to be established if the data obtained from the customer and from the databases are consistent and there is no reason to doubt that the customer is that person, who he or she claims to be, and there are no indications of medium or high risk circumstances.
3.1.9. In the event that the identity of the Customer is in doubt or circumstances indicating a medium or high risk category exist, the provisions of paragraphs 3.2 and 3.2.9 of this Part and Part V shall apply.

## 3.2. Legal entity client with medium risk profile

3.2.1. The Company will verify the identity of the legal entity Customer in accordance with the procedure below if:
3.2.1.1.. the customer is domiciled and/or effectively domiciled in a medium risk country; and/or

3.2.1.2.. the customer's legal representatives and/or beneficial owners are domiciled in a medium risk country; and/or
3.2.1.3.. the client's business activity is other than a high-risk business activity identified in the risk assessment,
3.2.1.4.. the expected annual transaction volume is between EUR 25 000 and EUR 50 000;
3.2.1.5.. there are no other elements of high risk identified in the risk assessment.
3.2.2. For the purpose of verifying the Customer's identity, the Customer shall provide the Company with the following information about the Customer:
3.2.2.1.. business name and legal form;
3.2.2.2.. the registration number or registration number and the time;
3.2.2.3. the country of actual residence;
3.2.2.4. address of registered office (country, city/county, street, house, apartment);
3.2.2.5. telephone number;
3.2.2.6. e-mail;
3.2.2.7. website address;
3.2.2.8. the principal activity;
3.2.2.9. tax identification number, if the customer is a registered taxable person;
3.2.2.10. the name, number, date of issue, period of validity and the issuer of the licence (if required, i.e. if the licence is compulsory for the activity in question);
3.2.2.11. the name of the representative and the basis for the right of representation (if the representative is an authorised representative, the names and dates of birth of the members of the board of directors);
3.2.2.12. details of the owners and beneficial owners holding at least 25%:
3.2.2.12.1. for the company: company name, registration code, country of registered office, country of establishment, percentage of ownership;
3.2.2.12.2. for natural persons: name and surname, date of birth, country of permanent residence or domicile, position, percentage of ownership.
3.2.2.13. information on whether the legal representatives or beneficial owners are PEPs, including local PEPs, family members or close associates of such person.
3.2.3. The Customer shall further provide the Company with the following confirmations:
3.2.3.1. he or she, his or her legal representatives or beneficial owners are not subject to an international financial sanctions;
3.2.3.2. holds an authorisation, if the activity is subject to an authorisation;
3.2.3.3. he/she agrees to the User Terms;
3.2.3.4. he has provided the Company with correct, accurate and truthful information and has not omitted any information in respect of which the Company might have a legitimate interest.
3.2.4. In addition, the Company will send a letter to the customer's e-mail address in which the customer undertakes to confirm the accuracy of his e-mail address as described.
3.2.5. For identification purposes, the Customer shall forward to the Company:
3.2.5.1. a copy of the document of registration in the country of residence, which is not older than six (6) months and which, inter alia, indicates the identity of the legal representative. If necessary, the Customer undertakes to provide this document, notarised and apostilled;

3.2.5.2. the basis of the legal representative's right of representation, in the case of an authorised representative, a notarised and apostilled power of attorney;
3.2.5.3. a copy of the licence or a reference to the place where the company can check it;
3.2.5.4. a document evidencing registration or exemption from registration as a taxable person, which shows the name, address, date of issue, title of the document, details of the issuer of the document and which is not older than six (6) months.
3.2.5.5. The taxable person's information on this document must be the same as the information provided by the client on the portal and must be in a format (.jpg)/(.png) accepted by the company. Where applicable, the customer undertakes to provide this document notarised and apostilled;
3.2.6. After receiving the information specified in points 3.2.2 to 3.2.5, the company:
3.2.6.1. compares the data contained in the documents submitted by the customer with the data submitted by the customer and verifies that the said documents do not show signs of falsification or deterioration and are valid; 3.2.6.2. checks whether the issuers of the submitted documents actually exist in public databases;
3.2.6.2.. verifies from freely accessible and trustworthy databases that the customer, his legal representatives or beneficial owner is not the subject of an international financial sanction and/or a person with a national background, including a local person with a national background, a member of his family or a close associate.
3.2.7. The identification of the representative of a legal person shall be subject to the procedures for the identification of natural persons set out in this document.
3.2.8. The customer is deemed to be identified if the data received from the customer and from the databases are consistent, including the identity of the customer's representative has been properly established and there is no reason to doubt that the data provided are not true.
3.2.9. In the event that the Company becomes suspicious of the identity of the Customer or if there are circumstances indicating a high risk category, the provisions set out in paragraph 3.2.9 of this Part and in Part V shall apply.

## 3.3. Legal entity with a high risk profile

3.3.1. The Company will establish the identity of the legal entity Customer in accordance with the procedure below if:
3.3.1.1. the customer is domiciled and/or effectively domiciled in a high-risk country; and/or
3.3.1.2. the customer's legal representatives and/or beneficial owners are permanently resident or domiciled in a high risk country; and/or
3.3.1.3. the client's business is a high-risk business as defined in the risk assessment; and/or
3.3.1.4. the expected annual transaction volume exceeds EUR 50 000; and/or
3.3.1.5. the legal representatives or beneficial owners of the customer are PEPs, including. local PEPs, family members or close associates of such a person.
3.3.2. For the purpose of verifying the Customer's identity, the Customer shall provide the Company with the following information about the Customer:
3.3.2.1. business name and legal form;
3.3.2.2. the registration number or registration number and the time;

3.3.2.3. the country of actual residence;
3.3.2.4. address of registered office (country, city/county, street, house, apartment);
3.3.2.5. telephone number;
3.3.2.6. e-mail;
3.3.2.7. website address;
3.3.2.8. the purpose of the business relationship;
3.3.2.9. the principal activity;
3.3.2.10. the tax identification number, if the customer is registered taxable person;
3.3.2.11. financial information for the last period and last year for which the accounts have been drawn up;
3.3.2.12. information on the countries of residence of the main customers;
3.3.2.13. the origin of the financial resources and source of wealth of the actual beneficiaries and PEPs, including local PEPs;
3.3.2.14. the name, number, date of issue, period of validity and the issuer of the licence (if required, i.e. if the licence is compulsory for the activity in question);
3.3.2.15. the name of the representative and the basis for the right of representation (if the representative is an authorised representative, the names and dates of birth of the members of the board of directors);
3.3.2.16. details of the owners and beneficial owners holding of at least 10%:
3.3.2.16.1. for the company: company name, registration code, country of registered office, country of establishment, percentage of ownership;
3.3.2.16.2. in the case of a natural person: first name and surname, date of birth, permanent address, date of birth, country of residence or domicile, position, percentage of ownership (%).
3.3.3. The Customer shall further provide the Company with the following confirmations:
3.3.3.1. he or she, his or her legal representatives or beneficial owners are not subject to international financial sanctions;
3.3.3.2. holds an authorisation, if the activity is subject to an authorisation;
3.3.3.3. he/she agrees to the Portal User Terms;
3.3.3.4. he has provided the Company with correct, accurate and truthful information and has not omitted any information in respect of which the Company might have a legitimate interest.
3.3.4. In addition, the Company will send a letter to the customer's e-mail address in which the customer undertakes to confirm the accuracy of his e-mail address as described.
3.3.5. For identification purposes, the Customer shall forward to the Company:
3.3.5.1. a copy of the document of registration in the country of residence, which is not older than six (6) months and which, inter alia, shows the details of the legal representative. If required, the Customer undertakes to provide this document, notarised and apostilled;
3.3.5.2. the basis of the legal representative's right of representation, in the case of an authorised representative, a notarised and apostilled power of attorney;
3.3.5.3. a copy of the licence or a reference to the place where the company can check it;
3.3.5.4.a document certifying registration or exemption from registration as a taxable person, showing the name, address, date of issue/issuance, title of the document, details of the issuer of the document, and which is not more than six (6) months old. The taxable

person information on this document must match the information provided by the client on the portal and must be in a format (.jpg)/(.png) accepted by the company. Where applicable, the customer undertakes to provide this document notarised and apostilled;

3.3.5.5.. a document proving the origin of the funds and the source of the wealth of the beneficial owners and PEPs, indicating the name of the person concerned, the date of issue/issuance, the title of the document, the identity of the issuer of the document and which is not older than six (6) months. The information on this document must match the information provided by the customer on the portal and must be in a format (.jpg)/(.png) accepted by the company. Where applicable, the Client undertakes to provide this document notarised and apostilled.

3.3.6. . After receiving the information specified in points 3.3.2 to 3.3.5, the company:

3.3.6.1.. compares the data contained in the documents provided by the customer with the data provided by the customer and verifies that the said documents do not show signs of falsification or tampering and are valid;

3.3.6.2. checks the public databases to verify whether the issuers of the documents submitted actually exist;

3.3.6.3. verifies from freely accessible and reliable databases that the customer, his legal representatives or beneficial owner are not subject to international financial sanctions.

3.3.7. The identification of the representative of a legal person shall be subject to the procedures for the identification of natural persons set out in this document.

3.3.8. The customer is deemed to be identified if the information received from the customer and from the databases is consistent, including the identity of the customer's representative has been properly established and there is no reason to doubt that the information provided is accurate.

3.3.9. In the event that the Company becomes in doubt as to the Customer, the provisions of Part V shall apply.

## 4. Identification and verification of identity in the following procedures

If the identity of the customer has been established by one of the means set out in points 2 or 3 of this Part and there are no circumstances which would oblige the firm to identify the customer again in the same way, the customer will be identified in the following way:

4.1. . on the basis of the unique e-mail address and password specified by the Client at the time of registration, which the Client uses to log in to the Portal;

4.2. . to log in to the Portal via a social media account (Facebook, Google+, LinkedIn, etc.) in accordance with the instructions provided on the Portal.

## 5. Data collection, updating and storage.

5.1. The company collects data about the customer:

5.1.1. . from the client, either through a questionnaire or video interview;
5.1.2. from independent and reliable public or paid registers and databases and internet searches.
5.2. The company updates customer data:
5.2.1. . if the customer has provided new information about himself/herself; and/or
5.2.2. within the time limits specified in Part III, points 2.1.6 or 2.2.4.
5.3. When updating the data, the Company will ask the customer to confirm the accuracy of the data and the validity of the documents previously provided or, if the data has changed or the document has become invalid, the Company will ask the customer to provide the new data and copies of the valid documents.
5.4. The company will make a note in the customer file of each update of data and documents, indicating the reason, method, time and place of the update.
5.5. The company will store and retain all documents in accordance with the following:
5.5.1. paper documents shall be systematised in folders according to the type of document, its content and/or the client for whom the document is drawn up;
5.5.2. the electronic documents are systematised as paper documents and stored on the company's main server disk in the EEA Member State in electronic folders in a systematic manner;
5.5.3. documents stored on the company's main server disk are backed up to the company's EMP to a disk on a backup server in a Member State;
5.5.4. the database controller is responsible for the preservation of the document stored in the database until the document is archived;
5.5.5. the Board of Directors or a person appointed by the Board of Directors shall be responsible for the archived documents.
5.6. The Company shall keep customer data as follows:
5.6.1. transaction records - 7 (seven) years after the transaction has ended;
5.6.2. other data (for identification and verification purposes and for the purposes of the transaction) the necessary information, including. (e.g. information on notifications) - 5 (five) years after the end of the transaction, unless requested by the competent authority. In the latter case, the right to keep the data for a further 5 (five) years.

# V. REPORTING SUSPICIONS OF MONEY LAUNDERING AND TERRORIST FINANCING.

1. The Company is obliged to report suspicions of terrorist financing or money laundering to the RAB in good faith, i.e. on the basis of its best understanding and belief, not biased against the interests of the Company, its customers or other third parties, in the cases provided for in these Rules and in the legislation.
2. The member of staff is obliged to inform the contact person immediately if:
   2.1. has suspicion or knowledge that a person involved in a transaction may be involved in money laundering or terrorist financing, in particular the activity or circumstances indicate the suspicious transaction indicator described in Annex 1;
   2.2. the customer submits documents that are unusual, i.e. the document does not meet the formal requirements, is not valid or may be forged;
   2.3. the customer refuses to provide the information and documents necessary for the proper implementation of the due diligence measures provided for in these Rules;
   2.4. has become aware that the access data used to identify the customer may be used by a third party;
   2.5. the customer refuses to enter into a business relationship or to enter into a transaction and/or act on the grounds that the company wishes to apply due diligence measures in accordance with these rules;
   2.6. the reassessment carried out during the monitoring process shows that the risk profile of the client meets the characteristics of a client with whom the firm does not have a business relationship (Part III, point 4);
   2.7. in other cases specified in these Rules.
3. In order to comply with the above obligation, the member of staff shall immediately notify the contact person in a readily understandable written form. A member of staff shall not be entitled to inform persons other than the contact person of the submission of the notification and its circumstances.
4. The liaison officer shall, without delay, inform the Executive Board of the receipt of the notification referred to in point 3 of this Section and shall decide on the sharing of information with other members of staff and third parties, if necessary for the performance of their duties.
5. In the justified cases set out in Annex 1, the contact person shall, without delay, inform the RAB of the receipt of the notification referred to in point 3 of this Section.
6. A member of staff and a contact person are prohibited from informing a client of a notification made to the RAB in accordance with these Rules and of the procedure relating thereto. Same the duty of confidentiality also extends to third parties. A contact person may
7. decide to inform the customer of the restrictions imposed by the RAB if the RAB's injunction has been complied with.The liaison officer is responsible for compliance with the RAB's injunction.
8. If the customer's conduct does not qualify as money laundering or terrorist financing, should be notified to the RAB, as set out in Annex 1, the customer should be placed under heightened scrutiny and/or, where appropriate, assigned a higher risk profile.

# VI. RESTRICTIONS ON ENTERING INTO A BUSINESS RELATIONSHIP OR TRANSACTION

1. A member of staff shall not:
   1.1. settle in cash;
   1.2. establish a business relationship:
      1.2.1. a person whose identity has not been established in accordance with these Rules;
      1.2.2. with an anonymous and unidentified person;
      1.2.3. with a person whose documents or other information raised doubts as to their accuracy and the client is unable to provide an adequate explanation;
      1.2.4. a person who does not produce documents proving the legal origin of the money or other property that is the subject of the transaction;
      1.2.5. a person whose identity or right of representation cannot be verified;
      1.2.6. a person whose beneficial owners cannot be identified;
      1.2.7. whose activity is related to the arms industry, the sale or brokering of arms;
      1.2.8. who is the subject of an international financial sanction;
      1.2.9. a person in respect of whom there are other grounds for suspecting that the person may be involved in money laundering or terrorist financing.
   1.3. occasionally enter into transactions contrary to the provisions of Part III.4 of the Rules.
2. In the aforementioned circumstances, the Company shall immediately suspend the establishment of a business relationship or transaction with the customer and inform the contact person thereof.
3. Failure by the Customer to provide the Company with the documents or information necessary for the due performance of the due diligence measures described in Part III, in spite of requests to do so, shall be deemed to constitute a material breach of the terms and conditions of use and the Contract shall be terminated immediately without notice.
4. In cases where the suspension of service and/or termination of the business relationship may prevent the apprehension of a possible money laundering or terrorist financing offender, the member of staff shall consult the contact person before taking any action.

# VII. TRANSACTION MONITORING AND ANALYSIS.

1. When conducting transactions, the firm and the member of staff must monitor and analyse unusual and suspicious transactions, which will enable the identification of circumstances in the business activities of customers that may indicate money laundering or terrorist financing. The purpose of the monitoring is also to identify transactions with subjects of international financial sanctions and persons with a national background, and to detect and report on transactions with a limit exceeding the amount of the transactions defined in the client's risk profile.
2. In case of any doubt, the member of staff or contact person should ask the customer for further information to clarify the purpose of the business relationship and the origin of the funds or assets. In assessing the circumstances, the member of staff will apply the principle of reasonableness and, in cases of doubt, will assess the circumstances to the detriment of the customer. All the information obtained must be recorded in the system under the customer profile.
3. Customer transactions and their possible links to money laundering or terrorism are analysed by a liaison officer.
4. To monitor transactions, the company uses scrubbing (the use of IT tools to track transactions and their compliance with specified parameters in real time) and monitoring.(analysis, including subsequent analysis after the transaction).
5. The main objectives of screening are to identify whether:
   5.1. the customer, his legal representative or beneficial owner is subject to an international financial sanctions;
   5.2. the client, his/her legal representative or beneficial owner is a PEP or a member of his/her family or close associate;
   5.3. the customer's nationality, actual residence or domicile is in a high-risk third country;
   5.4. whether the size of the transaction assigned to the client corresponds to the risk profile assigned to him, etc.
6. The main purpose of monitoring is to detect suspicious transactions, the purpose, reason and nature of which should be further investigated. The monitoring parameters are the major transactions carried out during the monitoring period, both in terms of amounts and types of customers.
7. In the event that the Company or a member of its staff discovers that the requested information about the customer is missing or incomplete, the Company will refuse to enter into the transaction until it has received further information from the customer.
8. In the event that the customer refuses to provide the information or documents requested by the company or a member of staff, the company will refuse the transaction and may decide to termination of a business relationship, including a user agreement, without notice. In this case, staff member undetakes to inform the contact person immediately.

# VIII. CONTACT

1. The contact person shall be appointed by decision of the Management Board. The Management Board shall also supervise the activities of the Liaison Officer.
2. The contact person has the right to require all staff members to comply with these rules and to put an immediate end to any possible breach.
3. The main tasks of the contact person are:
   3.1. carrying out money laundering and terrorist financing risk assessments, the resulting identifying new risk factors and reporting them to the Board;
   3.2. organising, analysing and archiving information on unusual transactions or transactions suspected of money laundering or terrorist financing;
   3.3. the transmission of information to the RAB in the event of suspicion of money laundering or terrorist financing and abnormal transactions, in accordance with the requirements set out in Annex 1 and the applicable law in force at the time the information is provided. The RAB notification form and instructions for completing it.
   3.4. to check the compliance of these rules with the legislation at least once a year and, if necessary, to propose amendments to the Board;
   3.5. identifying the training needs of staff members in the field of prevention of money laundering and terrorist financing, including the introduction of these rules to new staff members upon their employment and, if necessary, conducting additional training;
   3.6. Ensuring that the company complies with the RAB's prescriptions;
   3.7. at least once (1) a year, the company's compliance with these rules. verifying and reporting to the Governing Board any deficiencies/suggestions found. The review forwarded to the Governing Board must include:
      3.7.1. the control period and the time at which the control is carried out;
      3.7.2. the name and title of the person who carried out the inspection;
      3.7.3. a brief description of the checks carried out;
      3.7.4. a list of notifications submitted to the RAB;
      3.7.5. an overview of the enquiries made by the RAB and the responses to them;
      3.7.6. an overview of the warnings issued by the RAB, the responses to them and the actions taken and/or actions taken in response to them;
      3.7.7. an overview of the proceedings undertaken and pending against the company in relation to the prevention of money laundering and terrorist financing and compliance with international financial sanctions;
      3.7.8. an overview of compliance with the requirements of the prevention of money laundering and terrorist financing and international financial sanctions (including the requirements of this Procedure), including statistics on cases of establishment of a business relationship and/or refusal to enter into a transaction and on the application of international financial sanctions;
      3.7.9. proposals for amendments to these procedures and other observations, if any, to improve the organisation of the company's work in order to ensure compliance with the requirements set out in the rules and legislation;
      3.7.10. if the inspection reveals deficiencies, the time limit for rectifying them and the recommended measures, and the time for a follow-up inspection;

3.7.11. analysis of the results of the ex-post controls and a list of actions taken.

# IX. THE THREE LINES OF DEFENCE PRINCIPLE

1. The corporate structure is based on three lines of defence against money laundering and terrorist financing:
   1.1. The first line of defence, the customer service representatives, are responsible for the establishment of the business relationship and the normal monitoring of the business relationship, including the application of the required due diligence measures;
   1.2. The second line of defence, or liaison officer, will be responsible for the money laundering and terrorist financing risk management and compliance function, including monitoring the activities of the first line of defence and advising the first line of defence. It shall also be responsible for developing and updating methodologies and reporting;
   1.3. The third line of defence, the board of directors, provides independent oversight of the overall money laundering and terrorist financing risk management of the company.
2. The Management Board considers that it is important to continue to ensure that staff members are trained and informed about the risks of money laundering and terrorist financing in order to mitigate the risks.

# X. MEASURES TO IMPLEMENT THE INTERNATIONAL FINANCIAL SANCTIONS

1. Members of staff undertake to pay particular attention to the activities of any person who has a business relationship with the Company, or is engaged in and/or contemplating a transaction or activity with the Company, and to any circumstances that indicate the possibility that such person is or may be the subject of an international financial sanction.
2. The contact person regularly monitors the relevant databases/websites to identify changes in the list of subjects of international financial sanctions and the sanctions imposed on them. legislation and cross-checks them against a database of customers. When comparing the lists, the liaison officer shall take into account, inter alia, distortions of personal data, such as, but not limited to, the following errors or discrepancies in the translation, handling or processing of personal data and names:
   2.1. transcription of foreign names, including: differences in Latinisation of Russian and Scandinavian names, e.g.:
      2.1.1. the use of the terms "hooks", "bubbles" and "bubbles" in the names of Sweden, Norway, Denmark, Spain, etc.
      "strikethroughs" may have been ignored when entering data into the database, for example, may be replaced by Å = A; Č = C, Ñ = N; Ø =O; Æ = Ä; OE = OE;
      2.1.2. if 'SH' is used in the identity document, the 'SH' should be entered in the same form in the company database, for example in the Russian Federation passport: Fishelovitch, Vladimir. The exception is if the customer's name on the identity document is written with 'Š', then 'Š' is replaced by 'SH' in the company's database (as the technical solution does not allow 'Š' to be entered today). Similarly, Ž has been replaced by ZH;
      2.1.3. different word order of a name or designation consisting of several words, for example:
      AS JAAN TAMM or TAMM JAAN AS;
      2.1.4. use of abbreviations;
      2.1.5. spelling numbers in text, for example 2 FAST 4 YOU or TWO FAST FOUR/FOR/YOU;
      2.1.6. the use/misuse of prefixes and suffixes; and other factors such as:
         2.1.6.1. errors due to human error;
         2.1.6.2. switching between hard and soft pronunciation, e.g. AS GAASI KÜTE and AS KAASI GÜTE;
         2.1.6.3. the occurrence of a name or part of a name within or as part of another name.
   2.2. When identifying personal names, the contact person shall base his/her identification primarily on personal data, the main characteristics of which, in the case of natural persons, are their name and personal identification number or date of birth. In case of doubt or inconsistencies, other known data must be used.
   In the case of natural persons, the following, among others, are considered as other data:
   ▪ Place of birth;

- passport or identity document number, place and date of issue; sex;
- place of residence;
- other personal data (growth, hair/hair, glasses); and
- contact details.

2.3. In case of doubt, the contact person may request additional information from the customer as appropriate.

2.4. If a customer has been added to, removed from, or subjected to sanctions under an international financial sanctions regime, or has been the legislation imposing the sanctions has expired or is no longer in force, the liaison officer shall make the appropriate changes to the customer database and inform without delay, in a readily reproducible written form, the members of staff for whom this is essential for the performance of their duties.

2.5. The contact person also undertakes to take or designate a person who undertakes to take all necessary steps to implement, amend or terminate the international financial sanctions imposed on the customer in order to achieve the purpose of the international financial sanctions imposed by the customer. the objective pursued by the enactment, amendment, repeal or termination of the legislation and the avoidance of infringement.

2.6. In case of doubt and/or if the customer refuses to provide information and documents that would remove the doubt, the contact person will follow the provisions of points 2.3 and 2.4 of this section.The liaison officer consults with the Board when necessary.

2.7. The company, the member of staff and the liaison officer are prohibited from informing the person of the notification and the action taken in accordance with section 2.4 of this Part.

2.8. The Company shall collect and maintain the following records in relation to the performance of the obligations set out in this Part:

2.8.1. . the time of inspection;

2.8.2. . the name of the person who carried out the check;

2.8.3. . the results of the checks;

2.8.4. . the measures taken (if any).

The Company will keep this data for 5 (five) years from the date of collection.

# ANNEX 1 - CHARACTERISTICS OF SUSPICIOUS TRANSACTIONS

## 1. General information

1.1. The purpose of this Code is to provide guidance to company personnel to facilitate the detection of money laundering or terrorist financing.
1.2. A person may not be notified of a notification to the RAB under this Code except in the case of the imposition of an international sanction.

## 2. Obligation to inform

STR or reasonable suspicion of money laundering or other money laundering offences (p. 3 ), it is prohibited to enter into a transaction or business relationship, except in the cases set out in section 2.1.3 of this Code.
In the case of UTR or unusual transactions (p.4), the transaction may be finalised, but a RAB message may be issued.
In the case of a UAR or unusual activity (p. 5 ), the transaction is completed but the RAB is informed. If there is a reasonable suspicion of a criminal offence, the final or pending transaction is reported as an STR notification and the transaction is suspended, if possible, pending feedback from the RAB. In the case of a TFR, or terrorist financing suspicion, or a transaction involving a risk country (p. 6), a terrorist financing suspicion must be reported to the RAB and the transaction may not proceed. In the case of a risk country transaction or other unusual circumstances relating to the risk country, a terrorist financing notification must be submitted. The transaction may be completed or the business relationship continued, but enhanced due diligence measures must be applied.
In the case of an ISR or international financial sanction (p. 7), the transaction may not be completed without the authorisation of the RAB. When submitting a notification to the RAB, the reason for the notification must be given according to the type of indicator.

2.1. Money laundering or suspicion of terrorist financing

2.1.1. When a suspicion of money laundering or terrorist financing arises:
2.1.1.1. At the time of the establishment of a business relationship or at the time of an occasional request to carry out a transaction, if the doubt is not removed by compliance with point 2.1.3 of this Guide, an STR must be submitted. notice and may not establish a business relationship or occasionally enter into a transaction.
2.1.1.2. When preparing or executing a transaction, if the doubt is not removed by complying with paragraph 2.1.3 of this Instruction, the transaction must be postponed and a STR/TFR message with the indication CLEAR must be sent,

the transaction may not be executed. The RAB will provide feedback on the submitted notification (marked KIIRE) within two (2) working days.

2.1.1.3. In the course of the ex-post monitoring, if, in the case of a breach of 2.1.3 if the doubt is not removed, an STR/TFR notification will be made and the business relationship, if any, will be terminated.

2.1.2. Where suspicions of money laundering or terrorist financing arise, enhanced due diligence measures must be implemented with a view to eliminating the suspicion:

2.1.2.1. If the suspicion is eliminated, there is no need to notify the RAB and the business relationship/case-by-case transaction can continue.

2.1.2.2. If the suspicion of money laundering or terrorist financing is eliminated, but the transaction or activity is unusual, a report must be submitted to the RAB (UTR, UAR, TFR), the business relationship or occasional transaction may continue.

2.1.2.3. If the suspicion remains, the transaction may not be carried out or a business relationship established and the transaction must be postponed and a notification (STR, TFR) must be submitted to the RAB, marked CLEAR

2.1.3. In the case of suspicion of money laundering or terrorist financing, a transaction may be carried out notwithstanding the provisions of the Code:

2.1.3.1. if the postponement of the transaction may cause substantial damage;

2.1.3.2. it is not possible not to do so; or

2.1.3.3. may hinder the apprehension of a potential money launderer or terrorist financier.

In this case, the transaction is carried out and a notification (STR, TFR) is then submitted to the RAB

2.2. Suspicion of an abnormal transaction or activity

2.2.1. In case of establishment of a business relationship or a request to carry out an occasional transaction, if the abnormality is not eliminated by compliance with paragraph 2.3 of this Instruction, a notification (UTR, UAR, TFR) must be submitted to the RAB, but the business relationship may be established or an occasional transaction may be carried out. In the event that the statements or substantiation provided, the general risks of the specific sector or the procedural rules raise suspicions of money laundering or terrorist financing, the provisions of point 2.1 of this Guidance should be followed.

2.2.2. When a transaction is being prepared or executed, if the abnormality is not eliminated by compliance with section 2.3 of this Code, a notification (UTR, UAR, TFR) must be submitted to the RAB, but a business relationship may be established or an occasional transaction may be executed. In the event that the testimony or reasoning to be provided, the general risks of the specific area or the suspicion of money laundering or terrorist financing arises under the procedural rules, the provisions of point 2.1 of this Code shall apply.

2.2.3. In the course of the ex-post monitoring, if the abnormality is not corrected by compliance with paragraph 2.3 of this Code, a notification (UTR, UAR, TFR) must be submitted to the RAB, but the business relationship may continue. In the event that, on the basis of the testimony or reasoning provided, the general risks of the

specific area or the procedural rules, there is a need for suspicion of money laundering or terrorist financing should be guided by point 2.1 of this Code

2.3. Where an abnormal transaction or activity is identified, enhanced due diligence measures must be implemented with the aim of eliminating the abnormality:

2.3.1. If the abnormality is eliminated, the person justifies the abnormal transaction or activity with economic or other plausible explanations, it is not necessary to notify the RAB and the business relationship/case-by-case transaction may continue. If the abnormality persists, the person is unable to justify the transaction or activity with economic or other plausible explanations, a notification (UTR, UAR, TFR) must be submitted to the RAB, but the business relationship or transaction may continue.

2.3.2. When identifying anomalous transactions and activities, a member of staff shall be guided by the rules of procedure, the profile of the customer with whom he/she has a business relationship, or the reasoning of the person occasionally seeking to enter into a transaction. Depending on the circumstances of the case, the characteristics of an abnormal activity or transaction may give rise to suspicion of money laundering or terrorist financing.

## 3. Indicators for money laundering or other money laundering related crime (STR) indicators

3.1. Suspicion of money laundering arising from the establishment of a business relationship

3.1.1. the person is suspected of money laundering or has been suspected of money laundering in the course of due diligence.

3.1.1.1. the person has a history of money laundering or other criminal activity, or other indications of a negative background, which significantly increase the level of risk and, as a natural person, a representative of a company or a self-employed person, the business relationship is likely to be used for criminal purposes. For example, the person's previous criminal behaviour is known from public sources, or the business relationship has been refused in the recent past for the same reasons.

3.1.1.2. during the implementation of the due diligence measures, there is a suspicion that the business relationship is being established for the purpose of committing criminal activities, money laundering or other criminal offences. For example, a newly established business asks unreasonably and abnormally high limits for transactions, and indicates as counterparties companies from countries with a high money laundering risk.

3.1.1.3. Prior information received from law enforcement authorities about the person's suspicious transactions.

3.1.2. Doubts as to the veracity of the information provided by the person.

3.1.2.1. . There are grounds to believe that the person has provided false documents, incorrect or incomplete material information about himself or herself or the person represented, or concealed the beneficial owners of the person represented. For example, the paper format, date format, etc. provided does not conform to the practices of the geographical location of the issuer of the document, the signatures of the same person on different documents are identical (stamp-signature), or are applied using a cut-and-paste technique (also possible to distort the image). The person uses outside help to answer simple questions in the context of his business and/or position.

3.1.2.2. The person is not acting in his/her own name or under the control of a third party. The representatives of the legal person are not clearly identifiable in the documents (no identification code or date of birth) or do not have the right of representation. The person's behaviour is monitored or otherwise controlled remotely.

3.1.2.3. . there is a suspicion that the person is acting in the interests of another.

3.1.2.4. There is a suspicion that the person is attempting to establish a business relationship with an invalid authorisation or identification document.

3.1.2.5. . Documents submitted are suspected to be forged.

3.1.2.6. . the business model presented by the person is not plausible or feasible and, as a result, there is a suspicion that the purpose of the business relationship or occasional transaction is money laundering or other criminal activity.

3.1.3. the company refuses to enter into a business relationship with a person or terminates a business relationship with a person in accordance with Section 42 of the Money Laundering Act, due to the inability to carry out due diligence.

3.1.3.1. It is not possible to unambiguously identify or verify the identity or the right of representation.

3.1.3.2. The person refuses to provide additional information or documents requested.

3.1.3.3. It is not possible to identify the beneficial owner, except in the case of housing associations, public and listed companies.

3.1.3.4. The person or the capital represented shall consist of bearer securities.

3.2. Suspicion of money laundering in the course of transactions

3.2.1. the person is suspected of money laundering or has been suspected of money laundering in the course of due diligence.

3.2.1.1. it has become known in the past, or during the course of establishing the business relationship, that the natural person has been involved in money laundering or related criminal activities, or there are other indications of a criminal background, and the transaction raises suspicions of money laundering. For example, money has already been received into the account of a previous suspected fraudster, or the amount received has come from an unusual source for the person.

3.2.1.2. a person suspected of a known criminal offence sells immovable property, valuable movable property or securities (including shares in a company).

3.2.1.3. the implementation of the due diligence measures has led to the suspicion of a front company and the transaction is indicative of money laundering.

3.2.2. Suspicions of money laundering against a business associate in the course of due diligence measures.

3.2.2.1. A business associate is a person who is known to be associated with a criminal group or whose website or other public information indicates the provision of criminal services (e.g. for money laundering purposes) opening a bank or payment account, brokering payments under a power of attorney, carrying out transactions on behalf of another person, for example, depositing cash into an account or for a third party) or other criminal activity (for example, the transaction partner's website contains references to trade links with North Korea or illegal arms trafficking, reliable information is published about the person's corrupt links with a national government, etc.).

3.2.2.2. The other party to the transaction or its bank is a non-resident shell bank.

3.2.2.3. In the case of an abnormal transaction, no due diligence measures8 can be applied to the counterparty of the person in a business relationship.

3.2.3. the person fails to provide explanations or documents on the transaction to the extent necessary to comply with the due diligence measures, or the explanations or documents provided are not plausible (Money Laundering and Securities Supervision Act § 43 (43)).

The circumstances set out in 1 and 2)

3.2.3.1. the person's transaction is in doubt or sufficiently unusual to require further information and documentation on the transaction and the origin of the property. The person refuses to provide explanations or documents, or his explanations are not plausible, or the documents are suspected of falsification (e.g. the format of the paper provided, the date format, etc. does not correspond to the practice of the geographical location of the issuer of the document, the signatures of the same person on different documents are identical (stamp-signature) or added by a cut-and-paste technique (also possible distortion of the image), the dates of the documents and the alleged events are inconsistent, etc.).

3.2.3.2. The foreign civil court or arbitral tribunal's decision on the basis of which the transfer is made is not credible or is manifestly fictitious.

## 4. Unusual transaction (UTR) indicators

4.1. Upon conclusion of the contract

4.1.1. Unusual circumstances at the time of entering into a User Agreement that indicate possible criminal intent or the creation of a fraudulent impression of a person.

4.2. the person has previously been known to be, or the due diligence process has revealed, circumstances that give rise to doubts as to the person's trustworthiness.

4.2.1. the person is suspected of having a prior suspicion of stowaway or it arises during the due diligence process.

4.2.2. the legal person is registered in a high-risk country.

4.2.3. The number of employees of a legal person is clearly, in view of the activity concerned, not economically unjustified.

4.2.4. The person does not wish correspondence to be sent to a home address or the address of the legal person is indicated as a P.O. Box.

4.2.5. Documentation to identify the client and to verify the profession or activity of the intermediary who has no clear reason to be involved in the transaction. 4.2.6. The ownership structure of the legal person is not transparent.

4.3. The person is behaving in an abnormal manner.

4.3.1. the appearance and behaviour of the person is not in line with the customer relationship and/or the services the person wishes to provide.

4.3.2. the person uses unauthorised assistance in completing the documents or does not know how to complete them.

4.3.3. the person does not know the nature of the activities of the person being represented, cannot justify the necessity of the services ordered, there are inconsistencies in the explanations.

4.3.4. The person does not know or is not trying to conceal information about the person being represented (e.g. beneficial owners, owners, location, contact details, etc.).Where due diligence by the debtor is required.

4.3.5. The person does not know how to describe his/her potential partners and/or areas of activity.

4.3.6. The person has an unusually strong interest in the implementation of anti-money laundering measures.

4.3.7. The person proposes or seeks to avoid due diligence.

4.4. Unusual documents submitted by the person concerned

4.4.1. the person submits false or non-existent contact details or the legal person does not have a contact telephone number.

4.4.2. Documents proving the person's right of representation are invalid.

4.4.3. The person uses an address that does not exist in the documents.

4.4.4. Inconsistencies in the documentation of the legal person or other entity. 4.4.5. The paper dimensions or date format of the documents submitted do not conform to the standards of the place where the document was drawn up.

4.5. Unusual practices when ordering services

4.5.1. the person requests unusually high limits which are not commensurate with the person's appearance, ability and experience to operate in the given field, expected turnover, or in the case of an entrepreneur, the size of the business.

4.5.2. Documentation to identify the client or to verify the profession/place of business is provided by the intermediary who has no clear reason to be involved in the transaction.

4.6. When carrying out transactions

4.6.1. unusual circumstances arise in the course of the transaction which indicate that the true purpose of the transaction is not clear or is being concealed.

4.7. Abnormal transaction with virtual currency

4.7.1. the customer purchases more than EUR 32 000 worth of virtual currencies in a single transaction.
4.7.2. a single large-scale sale or purchase of virtual currencies using one or more services that complicate the identification of the person carrying out the transaction, such as a tumbler or mixer.
4.7.3. the PEP has bought or sold virtual currencies with a value of more than EUR 10 000.
4.7.4. virtual currency transactions use the services of intermediaries that guarantee/advertise the impossibility or difficulty of identifying a person (e.g. service providers that do not allow the transmission of personal data to law enforcement authorities).

4.8. Abnormal conduct in the course of a transaction

4.8.1. the Client authorises a person unconnected with the Company (suspected variation agent) to enter into an unusual or large-scale transaction that is not normal business practice.
4.8.2. the Customer provides confusing information or changes explanations about the transaction or does not know the details of its purpose and the origin of the funds used in it.
4.8.3. the Client unduly hastens the transaction.
4.8.4. the Client modifies or wishes to modify the Transaction after having provided additional documents or additional change the way you ask for clarification.
4.8.5. The person attempts to make a fictitious transaction.

## 5. Unusual Activity Reporting (UAR) indicators

5.1. Unusual behaviour of the person concerned
5.1.1. creating an unreasonably large number of accounts (including virtual card accounts).
5.1.2. Significant increases in unexpected and unjustified limits.

5.2. Characteristics of the provision of non-authorised financial services
5.2.1. the person's transactions have the characteristics of a financial service but lack the necessary authorisation.
5.2.2. The client provides a virtual currency service requiring a licence without holding a licence.
5.2.3. Large-scale initial coin offerings (ICOs) correspond in nature to the definition of a security (§ 2(1) of the Securities Market Act), but there is no corresponding authorisation.

5.2.4. Transactions in securities without holding the relevant authorisation/registration.

5.3. Abnormal transactions with virtual currencies

5.3.1. The Client purchases more than EUR 32 000.
5.3.2. The client sells virtual currencies worth more than EUR 32 000 in several consecutive transactions, the origin of the virtual currencies is unknown.
5.3.3. Regular buying and selling of virtual currencies through the services of intermediaries that guarantee/advertise the impossibility or difficulty of identifying the identity of the person (e.g. service providers who do not allow the transfer of personal data law enforcement authorities).
5.3.4. Regular buying and selling of virtual currencies using one or more services that make it difficult to identify the person carrying out the virtual currency transaction, such as a tumbler or mixer.

5.4. Abnormal commercial practices

5.4.1. The Company pays invoices to legal entities located in high-risk countries.
5.4.2. PEPs participating in the Transaction or persons connected to them who receive or send unusually large sums of money by bank transfer.
5.4.3. the company is a debtor within the meaning of the Money Laundering Act, but does not perform sufficient due diligence.
5.4.4. The company is an obligated person within the meaning of the Money Laundering and Securities Trading Act, but does not comply with the notification obligation.
5.4.5. the person wishes to enter into transactions with the assistance of or on behalf of the lawyer for which there is no economic justification.

## 6. Terrorist Financing Regulation (TFR) indicators

6.1. Abnormal transactions related to risk countries

6.1.1. The execution of the Transaction shall be supervised by an external person.
6.1.2. Inadequate explanation of the origin of the money.
6.1.3. Insufficient awareness of the counterparty.
6.1.4. First transaction with a natural/legal person in the country of risk.
6.1.5. A person makes a transfer to a third country bank account to which he/she has not previously transferred funds.
6.1.6. One party to the transfer is a credit or financial institution registered in a third country.
6.1.7. The IP address of the customer's computer refers to a high-risk country (when making payments, logging into the account).

6.1.8. The person makes the transfer to the account of a non-profit organisation (NGO, NPO) operating in a high-risk country or whose activity is providing assistance to high-risk countries.

6.1.9. what is stated in the Transaction Explanation is not in accordance with the business or usual practice of the company.

6.1.10. Transaction with a non-profit organisation operating in a high-risk country.

6.1.11. .In an international transaction, an explanation that refers to the financing of terrorism or any other explanation that is not comprehensible or interpretable (including, but not limited to, references to a donation, an alms Estonian or another recognisable language).

6.1.12. The nature of international transactions suggests the collection of money.

6.1.13. The natural person involved in the transaction was born in a high-risk country;

6.1.14. The natural person involved in the transaction is a national of a high-risk country;

6.1.15. The natural person involved in the transaction is resident in a high-risk country;

6.1.16. The natural person involved in the transaction is related to a legal person or other entity registered in a high-risk country;

6.1.17. The legal person or other entity involved in the transaction is registered in a high-risk country;

6.1.18. The parent company of the legal entity or other entity branch involved in the transaction is registered in a high-risk country.

6.2. Suspicion of terrorist financing

6.2.1. A person collects or transfers funds or virtual currency to a person associated with terrorist organisations or located in known terrorist areas.

6.2.2. According to public sources (press, etc.), the person is the subject of a criminal case for supporting terrorism;

6.2.2.1. . A party to the transaction is subject to a criminal prosecution pursuant to §237 - § 237(6).

6.2.3. Public sources (press, social media profile, website, etc.) indicate that a natural person has been radicalised;

6.2.3.1. The competent authority has referred to the counterparty of the transaction as a person who supports radical views and/or terrorist activities.

6.2.3.2. references to the counterparty in public sources as a person with radical views and/or as a supporter of terrorist activities.

6.3. Public sources (press, social media profile, website, etc.) indicate that the legal person represents the views of terrorist groups;

6.3.1. The competent authority has referred to the party to the transaction as a person with radical views and/or supporting the activities of a terrorist group.

6.3.2. references to the counterparty in public sources as a person with radical views and/or supporting the activities of a terrorist organisation.

6.4. There are other circumstances indicating the existence of terrorism or terrorist financing.

6.4.1. What is stated in the transaction explanatory memorandum refers to the features referred to in this section.

6.4.2. There are other circumstances indicating the existence of terrorism or terrorist financing.

## 7. International Financial Sanctions (ISR) indicators

7.1. Implementation of the international sanction (sanctioned person has been identified, the prohibition set out in the sanction has been implemented);
7.2. the person suspected of being subject to international sanction (natural persons, legal persons - whether the person is a sanctioned person), if it has not been possible to determine whether the person is.with a sanctioned person.
7.3. Suspicion of the need to apply international sanctions, sanctions (not related to persons) (bans on goods, services, financial access to territories, etc.).

# ANNEX 2. INFORMATION FOR PRODUCERS

I hereby certify that I am familiar with the procedures for complying with the obligation to prevent money laundering and terrorist financing, including these IES, and that I understand the requirements, obligations, rights and recommendations of the law, rules, regulations and guidelines.

Employee name and surname Agency Date of interview