AML Policy
Rules of Procedure for prevention of money laundering and terrorist financing

Latest reviewed: September 1, 2024

1. AML Statement

Ebaroter sp. z o.o (“**Company”**) is committed to the highest standards in the prevention of Money Laundering (AML), **Polish Anti-Money Laundering Act** (Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, Dz.U. 2018 poz. 723), **EU AML Directives**, **FATF Recommendations**, Fraud and other punishable criminal acts and Other relevant global standards.

These Rules of Procedure include principles and processes ("Procedure") that are designed to prohibit and actively prevent the use of the Company's services for money laundering, terrorist or criminal financing, or facilitation of any such activity.

To comply with regulatory requirements and combat money laundering, terrorist financing, and other financial crimes, the Company created and implemented this Procedure using a risk-based approach to address risks specific to its services, customers, and business partners.

The Company’s senior management is responsible for establishing and communicating the AML policy and maintaining the Compliance function. Senior management accepts their Compliance responsibilities and understands the key elements of the regulatory regime and how it impacts the activities and aspirations of the Company. Senior management is kept fully informed of Compliance activities and priorities. Senior management lends their full support to the Compliance Department.

2. General provisions

- These Rules of Procedure lay down general standards of Anti Money Laundering and Counter Terrorism Financing processes and controls which are followed by the Company’s management, employees, branches and agents (if any) in order to mitigate the legal, regulatory, reputational and as consequence financial risks, including internal security measures for conducting due diligence and detecting suspicious and unusual transactions in the services provided by EBAROTER SP. Z O.O. (“**Company**”) that are within the scope of the license for the provision of virtual currency services.
- The license for the provision of virtual currency services includes custodial exchange between virtual currency and fiat currency and vice versa and between virtual currencies, as well as the provision of safekeeping or generation of private keys of the customers within the context of the provision of a virtual currency wallet service.

- All relevant employees should know and follow the requirements set out in the Money Laundering and Terrorist Financing Prevention Act (**MLTFPA**), the International Sanctions Act, the relevant EU law, the guidance from the relevant regulator, the Financial Action Task Force (**FATF**) guidance on virtual assets, and other guidelines on compliance with the MLTFPA pertaining to the activities of the Company as well as these Rules of Procedure.

- A copy of these Rules of Procedure shall be available to all relevant employees and staff members.

3. Definitions and abbreviations

3.1 What is money laundering?

- Conversion or transfer of property derived from criminal activity, or, property obtained instead of such property, knowing that such property is derived from criminal activity, or, from an act of participation in such activity, for the purpose of concealing, or disguising the illicit origin of the property, or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions;
- The acquisition, possession or use of property derived from criminal activity, or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein;
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.

3.2 What is terrorist financing?

The allocation or raising of funds to plan or perform acts which are deemed to be acts of terrorism or to finance operations of terrorist organisations, or in the knowledge that the funds allocated or raised will be used for the aforementioned purposes.

3.3 What is a risk country?

Countries or regions of interest where the risk of money laundering or terrorism are high. A risk country is a country or jurisdiction that:

- According to credible sources, such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective anti-money laundering and combating the financing of terrorism (**AML/CFT**) systems.
- According to credible sources, there are significant levels of corruption or other criminal activity.
- Is subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations.
- Provides funding or support for terrorist activities, or that has designated terrorist organisations operating within their country, as identified by the European Union or the United Nations.

3.4 What is a high-risk country?

A country specified in a delegated act adopted on the basis of Article 9(2) of Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The current list is available here.

3.5 Who is a politically exposed person (PEP)?

A natural person who performs or performed prominent public functions as well as their family members and close associates. Persons who, by the date of entry into a transaction, have not performed any prominent public functions for at least one year, as well as their family members or close associates shall not be considered politically exposed persons.

For the purposes of these Rules of Procedure, the following persons shall be persons performing prominent public functions:

- State, head of government, minister and deputy or assistant minister;
- a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors, or of the board of a central bank;
- an ambassador, a chargé d'affaires or a high-ranking officer in armed forces;
- a member of an administrative, management or supervisory body of a State-owned enterprise;

- a director, deputy director or member of the board, or equivalent function, of an international organisation, except middle-ranking or more junior officials.

The following persons are considered family members of a person performing prominent public functions:

- the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or a local politically exposed person;
- a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person;
- a parent of a politically exposed person or local politically exposed person.

The following persons are considered close associates of a person performing prominent public functions:

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

The following persons shall be local politically exposed person: a person who is or who has been entrusted with prominent public functions in Poland, another contracting state of the European Economic Area, or in an institution of the European Union.

3.6 What is the MLTFPA?

The legal act that regulates the activities of credit and financial institutions, other undertakings and institutions specified in the Money Laundering and Terrorist Financing Prevention Act and the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)** and which contains the rules for the prevention of money laundering and terrorist financing.

3.7 What is the International Sanctions Act?

This legal act regulates the national imposition of international sanctions, the implementation and the supervision thereof where the imposition of international

sanctions has been decided by the European Union, the United Nations, another international organisation or the Government of Poland.

3.8 Who is a customer?

A person or a legal entity who uses, or has used, one or several virtual currency services offered by the Company. These services consist of the provision of a virtual currency wallet service and on the provision of virtual currency exchange services (whether fiat currency is involved or not).

3.9 Who is a relevant employee?

An employee or contractor of the company who is conducting KYC/AML measures about the customer in the Company or directly involved in the company's operations, such as: IT, business development, marketing, sales, customer support.

3.10 What is a business relationship?

For the purposes of these Rules of Procedure, a business relationship is a continued contractual relationship with a customer.

3.11 What is an occasional transaction?

It is a transaction that occurs outside the scope of the business relationship and that consists of amounts equivalent to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or is a transaction that consists on a transfer of funds that exceeds EUR 1,000 carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same.

3.12 What is a transaction monitoring?

An element of an institution's Anti-Money Laundering program in which customer activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are monitored using software that weighs the activity against a threshold of what is deemed "normal and expected" for the customer.

3.13 Who is an ultimate beneficial owner of a legal entity (UBO)?

Ultimate beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being

conducted. It also includes those persons who exercise ultimate effective control over a legal entity or arrangement. Reference to “ultimately owns or controls” and “ultimate effective control” refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. This definition should also apply to beneficial owner or a beneficiary under a life or other investment-linked insurance policy. Without derogating from the above, UBO is a private individual owning or controlling more than 25% of a legal entity.

3.14 What is an identification document

An identity card issued by a public administration and bearing the holder’s name, surname, and date of birth together with an image and potentially other identification features allowing for the identification of the bearer as the true holder.

3.15 What is an a transaction

Any interaction of the company with another person should an interaction lead to attempted handling of the other person’s property or providing services to such other person.

3.16 What is Risk-Based Approach (RBA)

The assessment of the varying risks associated with different types of businesses, clients, accounts and transactions in order to maximize the effectiveness of an anti-money laundering program.

3.17 What are three lines of defence

System where the company’s compliance is ensured by active involvement of the Management board, Compliance Officer and middle management along with employees of the company.

3.18 What is Risk Assessment (RA)

Risk Assessment as an internal tool to identify and document ML/TF and other risks and analyse the efficacy of the mitigation measures.

3.19 What is Tipping Off

Improper or illegal act of notifying a suspect that he or she is the subject of a Suspicious Actvitiy Report or is otherwise being investigated or pursued by the authorities.

3.20 What is Customer Due Diligence (CDD)

- identifying the customer and verifying the customer's identity on the basis of documents, data or information;
- identifying where there is a beneficial owner who is not the customer;
- obtaining information on the purpose and intended nature of the business relationship.

3.21 What is Enhanced Due Diligence (EDD)

Enhanced due diligence designates additional steps of examination and caution to identify the customers and confirm that their activities and funds are legitimate.

3.22 What is Simplified Due Diligence (SDD)

Means that it is not required for a business to apply the standard customer due diligence measures, where the business has reasonable grounds for believing that a client falls into the relevant categories representing low risk for money laundering or terrorism financing.

3.23 What are Know Your Client (KYC) and Know Your Business (KYB)

Are the processes used by the Company to verify the identity of their clients either individuals or legal entities. Know your customer policies are becoming increasingly important globally to prevent identity theft, financial fraud, money laundering and terrorism financing.

3.24 What is National Risk Assessment (NRA)

National Risk Assessment performed by local regulators. The NRA annually identifies risks for the payment industry in the country.

3.25 What is Internal Suspicious Activity Report (SAR)

Suspicious activity report filed by an employee of the Company to the Compliance Officer of the company.

3.26 What is External SAR

Report made by the Compliance Officer to **:-**

- Report the transaction to the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)**.

- Submit a Suspicious Transaction Report (STR) within the time frame required by Polish law.
- Maintain records of all reports submitted.

3.27 Who is Compliance Officer

Compliance Officer is a person who acts as the contact person for the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)** ensuring the compliance of the measures put in place to prevent money laundering and terrorist financing at the Company with the regulatory requirements.

4. Responsibilities. The person in charge of the performance of the AML/CFT obligations

- At least one designated management board member is in charge of the compliance with the MLTFPA and relevant guidelines.
- The management board appoints a Compliance Officer for performance of AML/CFT duties and obligations.
- The Compliance Officer needs to have the adequate education, professional suitability, abilities, personal qualities, experience and impeccable reputation required for performance of its duties.

4.1 Compliance Officer shall have the following duties:

- Design, execute, document and update if needed the money laundering prevention requirements in the Company, in compliance with the respective legislation, in the form of this Procedure and other internal documents, process descriptions etc.
- Design, execute and document a training program for the employees and contractors of the company.
- Assess risks of the company's services in the form of the annual Risk Assessment, or when the change in the critical business function is required.

Carrying out preliminary analysis of submitted internal reports about suspicious or unusual transactions and deciding whether or not to refer a report to the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)**.

Submitting the external SARs to the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)** in the case of suspected money laundering and responding to queries and precepts made by the GIIF.

- Analyse both data and inputs made by employees in order to previse the emerging suspicious and/or unusual actions, processing such information and keeping records pursuant to the prescribed procedure.
- Prepares written overviews on compliance with money laundering and terrorist financing prevention requirements to the management board.
- Notifying the management board in writing of any problems with compliance with these internal Rules of Procedure, guidelines and other legal acts and making periodic submission of written statements on compliance with the requirements arising from the MLTFPA.
- Issue approval to onboard a corporate client based on account application and DD collected .
- Issue approval to onboard or to keep high risk individual clients
- Issue approval to proceed with high risk transactions
- Manual audit of transaction monitoring system including sanctions monitoring.
- Manual audit of the KYC/KYB system.
- Vetting new employees of the Company.
- Change management.
- Lead the AML regulatory audits.

Participate in resolution of the following issues and accidents including ‘’lessons learned’’:

- Chargebacks and bank recalls - review and immediate report to the CEO;
- Internal, client’s and any other third party’s complaints or requests related to regulatory compliance - review and immediate report to the CEO.
- Requests from authorities - review and immediate report to CEO;

4.2 Monitor the media:

- News and publications about our high volume, virtual currencies clients;
- Publications related to partner financial institutions;
- Review of industry practices and issues;
- Regulatory trends.

4.3 Rights of the Compliance Officer:

- Making proposals for amending these Rules of Procedure, AML policy, and any other policies of the Company that are related to anti-money laundering and the prevention of terrorist financing;
- Monitoring the activities of the employees in pursuing the measures to prevent money laundering and terrorist financing.
- Receiving data and information required for performance of the duties of the Compliance Officer.
- Making proposals for re-organizing the process of submission of notifications of suspicious and unusual transactions.
- Receiving training in the field.

4.4 The Compliance Officer may send the information or data that have become known to him or her in connection with suspected money laundering only to:

- The management board of the Company or to an employee especially appointed by the management board;
- The Financial Supervision Authority;
- The Financial Intelligence Unit;
- A preliminary investigating authority in connection with criminal proceedings;

4.5 The court on the basis of a court ruling or judgement:

In the event of a well-founded suspicion concerning money laundering or terrorist financing, the Compliance Officer shall promptly report it to the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)**.

A report shall be sent to the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)** using Copies of the documents that serve as the basis for a transaction, as well as the data or copies of the documents used as the basis for identifying a person, shall be enclosed with the filled-in reporting form.

- The customer shall never be notified about any report sent about him or her to GIIF.

If the activities of a customer are not, in accordance with these Rules of Procedure, fully classifiable as activities which are to be reported to the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)**, any future activities of such customer shall be under increased scrutiny. GIIF shall be notified immediately if there is a well-founded suspicion about the behaviour of the customer.

No company, employee, the Compliance Officer or any other person acting on behalf of the Company shall be liable for any damage which may arise from non-completion or late completion of a transaction that is incurred by the customer because of suspicions about terrorist financing or money laundering that have been reported in good faith to the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)**.

Reporting to the **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)** and sending relevant information shall not be deemed to be a violation of the duty of confidentiality laid down by law or a contract and no liability prescribed by legislation or a contract shall be attributed to those persons for disclosure of such relevant information.

- Middle management and all staff of the company should be fully aware and understand their legal and regulatory responsibilities and obligations with regards to money laundering and terrorist financing activities. AML training programmes will be organized with respect to operational tasks and responsibilities.

Any employee found to have violated this Procedure will receive a warning letter. Multiple (two or more) violations will result in termination of employment of the employee. Deliberate breach of this Procedure might result in dismissal for gross misconduct and external report to authorities.

Employees have to pass mandatory AML compliance training arranged by the Institution and be aware about the consequences of their failure to comply with the Procedure, including reporting potential fraudulent/suspicious activities that may lead to the employee's voluntary or involuntary involvement in criminal activities .

Any third-party partner found to have violated this Procedure will be subject to contract termination as well as any other remedial measures available under applicable law including reporting to **Polish Financial Intelligence Unit (Generalny Inspektor Informacji Finansowej, GIIF)**.

The company will never ignore AML concerns or information from its partners: Financial Institutions, Merchants, Customers and/or law enforcement agencies. Each such concern, information, request will be carefully considered and investigated by the Compliance Officer, and relevant necessary measures will be taken by the Company.

5. Standard procedure for customer identification and verification

The relevant employee must identify all customers who want to use the Company's services on the basis of an identity document and shall record the identification and transaction data regardless of whether the customer is a regular customer or not, and regardless of the transaction amount.

5.1 A person must be identified and verified:

- prior to establishing a business relationship;
- upon suspicious customer behaviour;
- upon verification of information or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered beforehand while updating relevant data;
- again upon making or mediating occasional transactions outside a business relationship where a payment of over 15 000 euros or an equal amount in another currency is made, regardless of whether the financial obligation is performed in the transaction in a lump sum or in several related payments over a period of up to one year, unless otherwise provided by law;

If the customer is a private individual, he or she must provide:

- their full name;
- their personal identification code or, if none, the date and place of birth and the place of residence;
- if the customer is in fact representing another private individual being the real customer (under a power of attorney, or in the case of inheritance, or any other way) information on the identification and verification of the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer;

5.2 The following valid documents serve as basis for identification:

- an identity card;
- a passport;
- a diplomatic passport;
- an ID card of the citizen of the European Union;

- a driving licence if the document shows the name, photo or face image, signature or signature image and date of birth or personal identification code of its holder.
- In identifying a person, the relevant employee is obliged to check the validity of the identity document, make sure the person matches the information on the document and check the age of the person. If in doubt about the identity of the person, the relevant employee is obliged to request additional information about the person. Upon sending a document that does not match the person or is invalid, the relevant employee must refuse the customer registration and notify the Compliance Officer.
- The relevant employee verifies the correctness of the customer data, using information originating from a credible and independent source for that purpose. Where the identified person has a valid document specified in section 4.4 or an equivalent document, the person is identified and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document, or can be identified using means of electronic identification and trust services for electronic transactions, no additional details on the document need to be retained.

5.3 If the customer is a legal entity (for example a company), it must provide:

- the business name of the legal person;
- the registry code or registration number and the date of registration;
- the names of the director, members of the management board or other body replacing the management board, and their authorization in representing the legal person.

5.4 the details of contact information to the legal person:

- The relevant employee identifies a legal person based on a registry card of a relevant register or a registration certificate of a relevant register, or another document equal to such card or certificate.
- The relevant employee must identify the UBOs and, for the purpose of verifying their identities, taking measures to the extent that allows the relevant employee to make certain that he/she knows who the beneficial owners are, and understands the ownership and control structure of the customer, or of the person participating in the transaction.

- The relevant employee verifies the correctness of the information of a legal entity, using the information originating from a credible and independent source for that purpose. When the relevant employee is able to verify the information through such direct access, the submission of the documents specified in section 4.8 does not need to be demanded from the customer.
- If the relevant employee does not have an original of legal entity registry card or does not have a direct access to the registers, the relevant employee shall require in addition to the information in section 4.7, a Commercial Registry (or Company House or similar, depending of the country of origin) extract copy which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.
- A representative of a legal person of a foreign country must, at the request of the relevant employee, for example when the right of representation does not appear in the submitted document/s, submit a document certifying his or her powers (a power of attorney), which has been authenticated by a public notary and/or legalised and/or certified with an Apostille, unless otherwise provided for in an international agreement.
- The relevant employee may ask additional information about the customer in case of any suspicion about the customer's identity information or the customer's behaviour. Such additional information asked should be relevant to the raised risks which, when obtained, may prove that the risks are in fact explainable.

5.5 Procedure for identification of person and verification of data using information technology means:

- The relevant employee must identify a person and verify data with the help of information technology means when a business relationship is established with a person from a contracting state of the European Economic Area or whose place of residence or seat is in such a country and whose total sum of outgoing payments relating to a transaction or a service contract exceeds 15 000 euros per calendar month or, in the case of a customer who is a legal person, 25 000 euros per calendar month; and/or when the due diligence measures are not applied while being physically in the same place as the person or their representative.

- The relevant employee must identify a person and verify data with the help of information technology means where a business relationship is established with an e-resident or a person from a country outside the European Economic Area or whose place of residence or seat is in such country and where the due diligence measures are not applied while being physically in the same place as the person or their representative.
- When identifying and verifying customer's data with the help of information technology means, the relevant employee must comply with the technical requirements and procedure established by the regulation of the Ministry of Finance. The requirements are further included in the following subsections after the table.
- Level of due diligence measures applied to a particular customer depends on its risk level according to the risk matrix of the Company.

5.6 When the Company needs to identify and verify person's data with information technology means, the Company must use a document intended for the person's identification and comply with the following preconditions:

- Use highly reliable technical means which consists of a working camera, microphone, the hardware and software required for digital identification and an internet connection of adequate quality;
- Use information technology means that allow to compare biometric data. Biometric data includes facial image, fingerprint images, signature or image of signature and iris images;
- Receive from the customer the confirmation that s/he has read the information about the use of information technology means and agree to the conditions of identification and verification of his/her identity with information technology means;
- Receive confirmation from the customer that s/he carries out the identification and verification procedures using information technology means personally, that the data submitted is true and complete and that s/he meets the conditions established by the Company for the establishment of the business relationship and the conclusion of occasional transactions;
- Receive agreement from the customer on the applicability of Poland law;

Request the person (if foreigner) to show in front of the camera the personal data page of the valid travel document issued by the foreign country.

5.7 The identification and verification of a customer using information technology means is unsuccessful if any of the following occur:

- The person intentionally submitted data that does not correspond to the identification data entered in the identity documents database or does not coincide with the information or data obtained with other procedures;
- The session expires or is interrupted during the process of identification and verification using information technology means. Session expires when the person has not completed any activity for 15 minutes;
- The person has not given the confirmations identified in section 5.5;
- The person refuses to comply with the instructions regarding framing the face and document while using the information technology means: The person's head and shoulders must be visible and framed, the face must be clear of shadows and uncovered, clearly distinguishable from the background and other objects, and recognisable;
- The person uses the assistance of a third person without the Company's permission;
- There is suspicion of money laundering or terrorist financing.
- The relevant employee prepares the client profile and the risk profile based on the identification questionnaire, interview, other accessible information and the systematised collection and analysis of data and clarification of facts. Additionally, the relevant employee must give an opinion of the results of the procedure for onboarding using the information technology means and make a proposal on the regime of monitoring business relationships to be applied to the person. The opinion of the relevant employee of the service provider is the basis on which the decision to establish a business relationship is made.
- The Company builds a customer profile based on the information received from the customer. The relevant employee of the service provider must assess the data in the profile and record his or her opinion and the circumstances that are the basis thereof in the client profile and risk profile.

5.8 In case the person is a natural person, the answers to the questionnaire must indicate the following data:

- residential address;
- activity profile;
- area of activity;

- purpose and nature of establishment of a business relationship;
- connection of the person's economic or family interests with Poland;
- expected volumes of the services used by the person in appropriate cases;
- the beneficial owner;
- whether the person is a politically exposed person;
- other important information.

5.9 In case the person is a legal entity, the answers to the questionnaire must indicate the following data:

- business name;
- registry code;
- location and places of operation, including branches located in foreign countries;
- the legal form;
- legal capacity;
- lawful and contractual representatives;
- beneficial owner(s) and whether the beneficial owner is a politically exposed person;
- economic connections with Poland, contracting states of the European Economic Area and third countries;
- most important business partners;
- activity profile;
- main and secondary areas of activity, purpose and nature of establishment of a business relationship and other important information.

- The relevant employee, if needed, shall conduct an interview for identification and verification of a person's data during which the relevant employee asks partly structured questions, proceeding from the results of the questionnaire. The relevant employee must carry on the mandatory interview for the establishment of a business relationship in real time. The Company can authorise that the person uses the assistance of another person to eliminate any

technical problems when the identification questionnaire is carried out. The relevant employee must assess the person's reaction during the interview, the reliability of the information and data provided by the person with the data obtained through other procedures, and record his/her opinion and the circumstances that are the basis for the person profile and risk profile, which must be reproducible in writing.

- The Company has to allow for digital identification of a person and digital signing.
- The Company must ensure that when video is used (e.g. the real time interview from 5.9), the transmission of clear, recordable and reproducible synchronised sound and image, which is sufficient to understand the transmitted content unambiguously and reliably, is guaranteed. The video has to be recorded in a way that allows for it to be reproduced with a quality equal to the initial transmission.

The data collected from the questionnaire, identification of a person, unsuccessful identification of a person, and mandatory real time interview must be recorded with the following requirements:

- contain a time stamp, which must be tied to the data concerning it in such a manner that any later changes in data, the person who made the changes, and the time, manner and reason thereof can be identified;
- contain the person's IP address;
- contain the personal identification code of the person to be identified;
- contain the birth date and place and country of residence (if there is no personal identification code);
- be reproducible within five years of the end of the business relationship.
- Inspection of the performance of the identification of person and verification of data using information technology means is done by the Compliance Officer according to section 15 of these Rules of Procedure.

6. Simplified and Enhanced Due Diligence Procedure

6.1 The Company may apply simplified due diligence if a factor characterizing a lower risk has been established and at least the following criteria are met:

- a long-term contract has been concluded with the customer in writing, electronically or in a form reproducible in writing;
- payments accrue to the obliged entity in the framework of the business relationship only via an account held in a credit institution or the branch of a foreign credit institution registered in the Polish commercial register or in a credit institution established or having its place of business in a contracting state of the

European Economic Area or in a country that applies requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council;

- the total value of incoming and outgoing payments in transactions made in the framework of the business relationship does not exceed 15 000 euros a year.
- Before the application of simplified due diligence measures, factors referring to a lower risk are taken into account and the obliged entity determines whether these factors will be implemented on the whole, in part or as separate grounds.

Upon assessment of factors referring to a lower risk, the following is deemed a situation reducing risks relating to the customer type:

- the customer is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner;
- the customer is a legal person governed by public law established in Poland;
- the customer is a governmental authority or another authority performing public functions in Poland or a contracting state of the European Economic Area;
- the customer is an institution of the European Union;
- the customer is a credit institution or financial institution acting on its own behalf or a credit institution or financial institution located in a contracting state of the European Economic Area or a third country, which in its country of location is subject to requirements equal to those established in Directive (EU) 2015/849 of the European Parliament and of the Council and subject to state supervision;
- a person who is a resident of a country or geographic area having the characteristics specified in sections.

6.4. Upon assessment of factors referring to a lower risk, at least the following situations where the customer is from or the customer's place of residence or seat is in, may be deemed a factor reducing geographic risks:

- a contracting state of the European Economic Area;
- a third country that has effective AML/CFT systems;
- a third country where, according to credible sources, the level of corruption and other criminal activity is low;

- a third country where, according to credible sources such as mutual evaluations, reports or published follow-up reports, AML/CFT requirements that are in accordance with the updated recommendations of the FATF, and where the requirements are effectively implemented.some text

The relevant employee shall undertake enhanced due diligence (EDD) if there is a higher risk of money laundering or terrorist financing such:

  - there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
  - the customer is a politically exposed person;
  - the customer is from a high-risk third country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country;
  - the customer is from a risk country, or from a territory that is considered a low tax rate territory.

Complete list of the risk matrix factors (Risk Matrix).

Other factors that are referring to a higher risk pertaining to the customer:

- When there are unusual factors in the customer onboarding, or when there are unusual transactions patterns without clear economic or lawful purpose;
- Customer is a legal person or a legal arrangement, which is engaged in holding personal assets;
- Customer is a cash-intensive business;
- The customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;
- The ownership structure of the customer company appears unusual or excessively complex, given the nature of the company's business.some text

Other factors that are referring to a higher risk pertaining to the product, service, transaction or delivery channel:

  - Products/services that favours anonymity;
  - Payments received from unknown or unassociated third parties;
  - A business relationship is established without the customer or the customer's representative being physically met in the same place except when a document issued by the Republic of Poland for digital

identification of a person or another electronic identification system with assurance level 'high';

- new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.some text

The relevant employee must identify what the risks are in every particular case and undertake all appropriate measures to mitigate those risks. Depending on the case, the relevant employee may apply one or several of the following due diligence measures:

- verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;
- gathering additional information on the purpose and nature of the business relationship, transaction or operation and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
- gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to rule out the ostensibility of the transactions;
- gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the business relationship in order to rule out the ostensibility of the transactions;
- making of the first payment related to a transaction via an account that has been opened in the name of the customer participating in the transaction in a credit institution registered or having its place of business in the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force;

7. Collecting data and record-keeping

- The Company is obliged to retain all records about the customer and the customers' behaviour in such a way that it can always be presented to inspectors checking the recorded transactions.
- The relevant employee shall put his or her name and, if the document is in a paper format, his or her signature at the end of each entry.

- The Compliance Officer is responsible for keeping all relevant data.

The relevant data includes:

- information about the circumstances of refusal of the establishment of a business relationship or the completing an occasional transaction;
- information if it is impossible to take the due diligence measures using information technology means;
- originals or copies of the documents that serve as a basis for the establishment of identity and verification of the submitted information;
- the transaction date or period and a description of the substance of the transaction;
- the list of payment accounts kept in the name of the Company, along with each payment account's unique feature and the account manager's name.
- The personal data of a customer, a customer's transaction and other relevant information must be stored for no less than 5 years after termination of the business relationship.
- If a customer fails to submit all necessary documents and relevant information, or, if on the basis of the documents provided the relevant employee has a suspicion that money laundering or terrorist financing might be involved, the relevant employee shall not make a transaction with that customer and shall immediately inform the Compliance Officer and record as many customer details as possible that will later help to identify the customer.

8. Interaction with the customer

- The relevant employee may contact the customer to clarify the information given or ask for additional information, which is needed for the customer identification, or to address the risks identified.
- The relevant employee should not request unnecessary or irrelevant information. A request for additional information must be related to the risks of the case, and after receiving the customer's response, the relevant employee may close or report the case to the Compliance Officer. If the risk of money laundering or terrorist financing is very high, the relevant employee shall report the case to the Compliance Officer without asking additional information from the customer.
- The relevant employee shall never express themselves using words that give a reason for the customer to understand that his/her activity is suspicious and may be a subject for further report to the Compliance Officer.

9. Monitoring the business relationship

- A transaction monitoring shall be initiated based on a behaviour trigger of the customer or manually by the relevant employee or by the Compliance Officer. A relevant employee must investigate every initiated case.
- The relevant employee cannot be working on a case if the customer in question is a close person to that relevant employee, or a customer that is in any other way connected with that relevant employee.
- The relevant employee should determine what the risks of the case are. Each risk should be addressed and documented.
- The relevant employee must conduct customer research to determine the customer's profile and identify the source and origin of the funds used in a transaction.
- The relevant employee must conduct research on all the counter-parties if it is applicable in the case.
- The relevant employee must document all the findings about the customer and customer's behaviour which support the decision of the relevant employee about closing or reporting the case to the Compliance Officer.

10. Understanding the risk profile of a customer and risks related to new and existing technologies

During the monitoring of the business relationship, the relevant employee must collect enough evidence to mitigate the risks alerted. For this reason, the relevant employee should research and use the following information:

- Source of wealth or the source of fund of the transaction (employment status, role or title in a company, employer, approximate salary, additional source of income, industry type etc.);
- The customer's age;
- Location of the customer and the customer's counterparties;
- The history of the customer's transactions;
- The type of transactions;
- Any negative information associated with the customer;
- Any factors that cause the customer to be considered a high risk;
- The relationship between the customer and the customer's counterparties;
- The relationship between the customer and customer's place of residence.

- Other information which helps to understand the customer, the customer's activity and its counterparties.
- The relevant employee shall always be aware that new, existing and emerging technologies may give the customer a possibility to hide his or her real identity or to make a fraud. Therefore, the relevant employee shall assess the risk of new and emerging technologies and address them within the process of onboarding the customer and within the transaction monitoring.

11. Decision-making

After each transaction monitoring review, the relevant employee will make a final decision about whether to report the case to the Compliance Officer or close the case, based on the evidence collected for the case, and provide a final conclusion that supports the decision made.

While making a final decision, the relevant employee should:

- Finish the research about the customer, the customer's behaviour and the customer's counter-parties;
- Understand the evidence collected and look for indications of unusual activities;
- Consider each piece of evidence on its own and consider all evidence at the same time;
- If two pieces of evidence contradict each other, look at them together;
- Identify which pieces of evidence have the greatest impact on its analysis;
- Identify each piece of evidence that has the least impact on its analysis;
- Determine which theory is most strongly supported by the evidence.

12. Risk appetite and PEP requirements

The risk appetite is determined by the Company according to the principles of proportionality and reasonableness and observing the context presented by the following risks:

- the risks associated with the products and services offered, their volumes and complexity, including in different jurisdictions;
- the risks of the customers consuming the products and services and the structure of the customer portfolio;
- the risks of sales channels, incl. risks associated with outsourcing;
- geographic risks, including presence in other countries or provision of services to cross-border customers from distance.

- The Company's management board has determined that business relationships can not be established with persons from a country outside the European Economic Area or with e-residents.
- The relevant employee shall check whether the customer is a politically exposed person (PEP), a family member of a PEP or a person known to be a close associate with a PEP.some text

In order to allow a PEP to become a customer, the following must be fulfilled:

  - An approval from the Company's management board for establishing a business relationship with that person.
  - Adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship.
  - When a business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

The relevant employee shall refuse to onboard a new customer or, if an account is already opened, block the account and report to the Compliance Officer in case the relevant employee finds out that:

  - the customer is accessing the service from a high-risk country being a high-risk country citizen;
  - the customer is under sanctions from the European Union or the USA;
  - the customer is known to be accused with money laundering or terrorist financing.

13. International sanctions

- The relevant employee shall check every customer on being subject to international sanctions. The check needs to be done during onboarding process and on a regular basis afterwards. If the relevant employee has doubts about the matching results and the customer in question, the relevant employee needs to consult with the Compliance Officer.
- The customer shall not be informed that he/she is screening under international sanctions' lists.

The Compliance Officer shall be responsible for the implementation of international sanctions. The Compliance Officer shall:

- regularly follow the webpage https://www.sanctionsmap.eu/#/main and check the list of persons under international sanctions and immediately take measures provided for in the act on the imposition or implementation of international sanctions;
- upon entry into force of an act on the imposition or implementation of international sanctions, the amendment, repeal or expiry thereof, immediately check whether any of the customers is subject to international sanctions with regard to whom the financial sanction is imposed, amended or terminated;
- keep an updated record of subjects of international sanctions and submit this information to the employees in the form that allows to use this information in the course of their activity;
- provide training to the employees that allows them independently establish the subjects of international sanctions;
- assist the employees if they have doubt or knowledge that a customer is a subject to international sanctions;
- supervise the application of the Rules regarding the implementation of international sanctions by the employees;
- review and keep updated the Rules regarding the implementation of international sanctions;

AML Training and Awareness

- The Company will ensure that all employees are trained in AML procedures. Training will cover:
- The legal obligations related to money laundering and terrorist financing.
- How to identify and report suspicious activities.
- The Company's internal AML procedures.
- Training sessions will be conducted regularly to ensure compliance with evolving regulations and risks.

The following information shall be recorded about each single check about the customer:

- Check time;

- Name of the relevant employee who made a check;
- Check results;
- Measures taken.

If in the course of the check, it shall be detected that a customer or a person who used to be a customer is subject to international sanctions, the Compliance Officer shall notify the employees, who dealt with this customer, the management board and Polish authorities. The notification shall be submitted at least in the way that allows its reproduction in writing. The report will be issued by using the web form without delay but not later than within 2 business days.

If the customer is subject to International Sanctions, then those sanctions will be applied by the management board along with input from the Compliance Officer. In case the assets of the customer should be frozen, the management board will take the steps necessary, including segregating the assets of the customer, who is subject to sanctions from others and restricting the disposal of those assets.

14. Reporting procedure of suspicious and unusual transactions

- If the relevant employee has a suspicion that he or she may be dealing with a suspicious or unusual transaction, the employee shall promptly report this to the Compliance Officer. In addition to the above-mentioned transaction and customer data, the Compliance Officer should also receive the reason for reporting and identification information about the customer.
- The relevant employee is not allowed to notify the customer about the fact that the customer has been reported to the Compliance Officer.
- In case of any suspicion, the relevant employee must notify the Compliance Officer by filling out the special notification form.
- **Record-Keeping**
- The Company will keep detailed records of:
- All customer identification documents.
- Transaction histories and supporting documentation.
- Reports of suspicious activities.
- These records will be retained for at least 5 years, or as required by Polish law.

The relevant employee must report to the Compliance Officer when he or she discovers any suspicious customer's behaviour related to money laundering, including, but not limited to cases where:

- The customer makes transfers to other persons in different countries that do not conform to the person's usual activities;
- The customer informs that the funds will be withdrawn by a third party acting on his/her behalf and on his/her account;
- The customer's profile does not conform to the nature of the transaction being executed by him/her.
- In case of suspicion of terrorist financing, the relevant employee must identify the risk related to the customer and report to the Compliance Officer if the risks related to a customer cannot be reasonably mitigated or explained.some text

The risks of terrorist financing include, but are not limited to:

  - The individual was born in a high-risk country;
  - The individual is a citizen of a high-risk country;
  - The individual has a place of residence in a high-risk country or the legal entity is incorporated in a high-risk country;
  - The natural person is associated with a legal person or another entity registered in a high-risk country.

15. Internal control rules

The Compliance Officer is responsible for checking the work done by the relevant employee.

The Compliance Officer shall check the work of the relevant employee on a quarterly basis in accordance with the following criteria:

- the work of the relevant employee does not breach this Rules of Procedure;
- the relevant employee has done sufficient research on the customer;
- the relevant employee has documented all the evidences about the customer;
- the relevant employee has made a decision relaying on the evidences collected and documented.

The relevant employee may get a low-quality notification from the Compliance Officer if the relevant employee constantly breaches the criteria set forth in 15.2. In case the

quality of the employee's work has not been improved after the first notification, this may lead to extraordinary termination.

16. Training for employees

The Compliance Officer or other expert in the field of anti-money laundering shall carry out the money laundering and terrorist financing prevention training for the employees of the Company.

The employees must be informed about the requirements for the prevention of money laundering and terrorist financing and the implementation of due diligence measures and reports on suspicion of money laundering. It includes:

- the principles specified in the risk appetite of the company;
- the risks arising from the activities of and services provided by the company;
- the obligations stipulated in these rules of procedure;
- the contemporary methods of committing money laundering and terrorist financing and specific typologies/cases, and the risks associated with them;
- how to recognise actions related to possible money laundering or terrorist financing, and guidelines on how to act in such situations.
- The Compliance Officer is responsible for carrying out regular training. Each relevant employee shall confirm their participation with their signature. It is recommended to organize trainings when necessary, but not less than once per year.
- The Compliance Officer is obligated to provide instructions and an introduction training to all new relevant employees pursuant to the prescribed procedure following the signing of the employment contract no later than within one week after the commencement of employment by the relevant employee and to make the new relevant employee familiar with these Rules of Procedure against signature.
- The Compliance Officer has the right to submit proposals to the management board concerning what trainings should be made.

17. Violation of duty to register information and keep records

Any violation of the duty to register information and to keep records as prescribed by these Rules of Procedure and in the Money Laundering and Terrorist Financing Prevention Act shall be disciplined in accordance with the law.

18. Outsourcing

- Outsourcing of any obligation under these Rules of Procedure is allowed only upon respective resolution by the management board. Outsourcing is allowed only to a party that applies due diligence measures similar to those stipulated in these Rules of Procedure and the MLTFPA and provided the respective party is ready to be subject to supervision similar to one exercised over the Company in accordance with the MLTFPA.
- To outsource an activity, the obliged entity enters into a written contract with the other person.some text

The contract must ensure:

- division of the rights and obligations associated with the outsourcing of the activity;
- that the outsourcing of the activity does not impede the activities of the Company or performance of the obligations provided for in the law and guidelines;
- that the other person performs all the obligations of the Company relating to the outsourcing of the activity;
- that the outsourcing of the activity does not impede exercising supervision over the Company;
- that the competent authority can exercise supervision over the person carrying out the outsourced activity;
- the required level of knowledge and skills and the capacity of the person conducting the outsourced activity;
- that the Company has the unrestricted right to inspect compliance by the person conducting the outsourced activity;
- that documents and data gathered comply with the requirements arising from the law and relevant guidelines;
- the right of the obliged entity to terminate the outsourcing contract with the other person, where necessary, if the latter has failed to perform the contractual obligations or has not performed them properly.

The Company or the relevant employee may rely on the data and documents gathered by another person if the Company or the relevant employee:

- gathers from the third-party information on who is the person establishing the business relationship or making the transaction, their representative

and the beneficial owner, as well as what is the purpose and nature of the business relationship or transaction;

- has ensured that, where necessary, it is able to immediately obtain all the data and documents whereby it relied on data gathered by another person;
- has established that the other person who is relied on is required to comply and actually complies with requirements equal to those established in the relevant law and is under or is prepared to be under state supervision regarding compliance with the requirements.
- In the case of identification of person and verification of data using information technology means described in section 5, identification and data verification and the questionnaire can be carried out by a relevant employee, a partner of the Company (outsourcing) or by an automated system.

19. Prevention of conflicts of interest

In order to identify and manage conflicts of interests, the Company:

- established the risk appetite and risks arising from its activities;
- avoids situations where the personal interests of owners, managers and employees and customers are in conflict with the interests of the Company;
- asks the employees and managers to provide data about their economic interests that may originate a conflict of interests. The Company regularly updates these declarations of economic interests;
- identifies and analyses whether the persons who lead a customer to the Company has a conflict of interests between the Company and the customer. The measure to manage such a conflict of interests may be to avoid establishing such business relationship.

20. Amendments of these Rules of Procedure

These Rules of Procedure may be amended by resolution of the management board based on a majority vote in accordance with the articles of association of the Company.

21. Annexes to these Rules of Procedure

These Rules of Procedure include the following Annexes:

- Weekly compliance meetings agenda;
- Annual Money Laundering Reporting Officer Report;

- Customer Acceptance
- Internal SAR
- Risk Matrix
- SAR Register
- KYC procedure
- KYB procedure
- Red flags and process guide
- Compliance Monitoring Plan
- Compliance Monitoring Plan Checklist

Internal Controls and Independent Audits

- The Company will establish and maintain strong internal controls to prevent money laundering and ensure compliance with this policy. An independent audit will be conducted periodically to assess the effectiveness of the AML controls and procedures.

Data Protection and Privacy

- The Company is committed to protecting the privacy of its customers. Personal data collected during CDD and EDD processes will be handled in compliance with the **General Data Protection Regulation (GDPR)** and other relevant data protection laws.

Penalties for Non-Compliance

- Any employee found to be in breach of this AML Policy will face disciplinary action, which may include termination of employment. Additionally, the Company may face regulatory penalties, including fines and potential revocation of its cryptocurrency license, for non-compliance.

Continuous Review

- The Company will review and update this AML Policy regularly to ensure it remains compliant with changes in laws, regulations, and industry best practices.

Approval and Endorsement:

- This policy is approved by the Board of Directors and will be enforced by all levels of management.

For any questions relating to our policy, write an email to ebaroter@gmail.com