INTERNAL ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM POLICY
adopted in
17th March 2022

by the decision of the Board of Directors no 1/03/2022

Last modification: March 2022

c. **§ 1. DEFINITIONS**

1. Ilekroć w dalszej części niniejszej Procedury jest mowa o:

1.1. **Beneficial owner** – this shall be understood in accordance with the AML Act i.e. as every natural person who controls, whether directly or indirectly, a client through their powers which result from legal or factual circumstances and enable exerting a decisive impact on client's acts or actions, or every natural person on whose behalf business relationships are being established or an occasional transaction is being conducted, including:

d. in the case of a legal person other than a company whose securities are admitted to trading on a regulated market that is subject to disclosure requirements in accordance with the EU law or subject to corresponding third country law:
   - a natural person being a shareholder and holding the ownership right to more than 25 per cent of the total number of shares of such legal person,
   - a natural person holding more than 25 per cent of the total number of votes in the legal person's decision-making body, also as a pledgee or usufructuary, or under arrangements with other holders of voting rights,
   - a natural person exercising control over a legal person or legal persons holding in aggregate the ownership right to more than 25 per cent of the total number of shares or holding in aggregate more than 25 per cent of the total number of votes in the legal person's decision-making body, also as a pledgee or usufructuary, or under arrangements with other holders of voting rights,
   - a natural person exercising control over the legal person through holding the powers referred to in Article 3, paragraph 1, subparagraph 37 of the Act of 29 September 1994 on Accounting (Dziennik Ustaw 2021, item 217), or
   - a natural person holding a senior management function in the case of the documented inability to determine or doubts as to the identity of the natural persons referred to in the first to fourth indents and in the case of finding no suspicion of money laundering or terrorist financing;

e. in the case of a trust:
   - the settlor,
   - the trustee,
   - the supervisor, if any,
   - beneficiary,
   - other natural person exercising control over the trust,

f. in the case of a natural person carrying out economic activity with respect of whom no premises or circumstances were found which could indicate that other natural person or natural persons exercise control over him/her, such natural person shall be assumed to be the beneficial owner at the same time..

1.2. **Family members of a politically exposed person** - this shall be understood as:

a. a spouse or a cohabitant of a politically exposed person
b. a child of a politically exposed person and his/her spouse or a cohabitant
c. parents of a politically exposed person.

1.3. **General Inspector or the supervisory authority** – this shall be understood as the General Inspector of Financial Information.

1.4. **Customer** – this shall be understood as a natural person, a legal person or an organizational unit having no legal personality for which the Company performs Transactions or with which the Company establishes business relationships.

1.5. **AML Coordinator** – this shall be understood as a person designated by the Company pursuant to Article 6 of the AML Act.

1.6. **National Assessment of the Risk** – this shall be understood as binding National Assessment of the Risk of Money Laundering and Terrorist Financing developed by the General Inspector.

1.7. **Politically exposed persons -** this shall be understood as, excluding group of middle-ranking or more junior posts, natural persons occupying prominent public posts or fulfilling prominent public functions, including:
   a. heads of State, heads of government, ministers and deputy or assistant ministers
   b. members of parliament or similar legislative bodies
   c. members of the governing bodies of political parties
   d. members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances, including judges of the Supreme Court, the Constitutional Tribunal, the Supreme Administrative Court, provincial administrative courts and judges of courts of appeal,
   e. members of courts of auditors or of the management boards of central banks
   f. ambassadors, chargés d'affaires and high-ranking officers in the armed forces
   g. members of the administrative, management or supervisory bodies of state-owned enterprises, companies with the State Treasury shareholdings in which more than a half of shares are held by the State Treasury or other state-owned legal persons
   h. directors, deputy directors and members of the bodies of international organizations or persons performing equivalent functions in these organizations
   i. managing directors of supreme and central offices of state authorities and managing directors of voivodeship offices,
   j. directors-general in the offices of supreme and central state bodies, directors-general of provincial offices and heads of offices of field bodies of special government administration.
   k. other persons occupying public posts or performing public functions in state authorities or central authorities of the government administration.,

1.8. **persons known to be close associates of a politically exposed person** - this shall be understood as:
   a. natural persons who have beneficial ownership of legal persons, organizational units having no legal personality or trusts with a politically exposed person, or any other close relationships with such a person related to the business activity conducted,
   b. natural persons who have sole beneficial ownership of legal persons, organizational units having no legal personality or a trust which is known to have been set up for the de facto benefit of a politically exposed person.

1.9. **PEP** – this shall be understood as Politically exposed persons, their Family members and Persons known to be close associates of a politically exposed person.

1.10. **Policy** – this shall be understood as this document implemented by the Board of Directors of the Company, as amended and supplemented at any time.

1.11. **Employee** – this shall be understood as a person hired by the Company, regardless of the legal basis of the contract, including under employment contract, as well as any person providing services to the Company based on agency contract or any other contract in this matter and persons who cooperate with the Company under B2B contracts. which scope

1.12. **Register or CRBR** – this shall be understood as the Central Register of Beneficial Owners created under the AML Act i.e. public IT data transmission system used for processing information on beneficial owners of entities.

1.13. **Website** – the Company's website through which Customers are provided with the opportunity to create a user account, register and complete all procedures required for registered users.

1.14. **Company** – this shall be understood as Geocurrency sp. z o.o., a limited liability company incorporated in Poland, with its registered seat in Katowice, address: ul. Jana Kochanowskiego 12A/4, 40-035 Katowice, with company registration number 960924.

1.15. **Business relationship** – this shall be understood as relationships of the Company with the Customer which are connected with the professional activities of the Company and which are expected, at the time when relationships are established, to have an element

of duration. Business relationship Transactions are deemed to include, but are not limited to, Transactions performed with registered Customer, who creates a user account and completes all procedures required for registered users, including those provided for in this Policy, and then performs Transactions using this account.

1.16. **IT System** – it shall be understood as IT system implemented by the Company containing appropriate analytical tools designed to automate the customers risk assessment, including facilitating the fulfilment of the Company's statutory obligations.

1.17. **Transaction** – this shall be understood as an act in law or factual act performed by the Company on behalf of the Customer on the basis of which the transfer of ownership right or possession of property values is done or an act in law or factual act performed in order to transfer of ownership right or possession of property valuers.

1.18. **Occasional transaction** – this shall be understood as a transaction which is not conducted as part of business relationships, in particular actions performed by the Company on behalf of unregistered / one-time Customer through Company's API, with the aim of exchanging Virtual Currencies for FIAT or exchanging FIAT for Virtual Currencies or Virtual Currencies for Virtual Currencies.

1.19. **Suspicious transaction** – this shall be understood as Transaction which circumstances regarding its execution indicate, that it may have connection with money laundering or terrorism financing, regardless of the value of the Transaction or its nature.

1.20. **AML Act** – this shall be understood as the Act of 1 March 2018 in combating money laundering and the financing of terrorism (in current writing).

1.21. **Virtual currency** – this shall be understood as digital representation of value which is not a legal tender issued and guaranteed by central bank or any other public administration authorities, do not have to be related to any legal tender and do not have legal status of currency or money, although which is accepted by natural or legal persons as a commodity and may be transferred, stored or sold electronically, including but not limited to Bitcoin (BTC).

1.22. **Property values -** this shall be understood as property rights or other movable property or immovable properties, means of payment, financial instruments within the meaning of the Act of 29 July 2005 on Trading in Financial Instruments, other securities, foreign exchange values, and virtual currencies**.**

g. **§ 2. INTRODUCTION**

1. Bearing in mind the safety of Customers and the applicable regulations on combating money laundering and the financing of terrorism, the Company, as an obliged institution, pursuant to Article 50 section 1 of the AML Act, implemented this Policy, which sets out the principles for assessing and analysing the risk of combating money laundering and terrorist financing, as well as other principles, which are required to be taken into account by generally applicable laws.
2. Provisions of the Policy are established in particular pursuant to the following acts:
   a. the Act of 1 March 2018 on combating money laundering and the financing of terrorism;
   b. the Act of 6 June 1997 Penal Code;
   c. the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

3. The Board of Directors adopted this Policy by its decision before the first Transaction was performed by the Company. Amendments and supplements to this Policy shall be adopted in the same manner.
4. The Policy shall be communicated to all Employees without any delay.

5. It is the AML Coordinator responsibility to communicate the Policy to Employees and to implement it, as well as constant evaluation of the need to update the Policy's content.
6. Whenever amounts expressed in EUR are indicated in the Procedure, they shall be converted at the average exchange rate announced by the National Bank of Poland (NBP), in force on the day of effecting the Transaction, on the day of the order to effect the Transaction or on the day of the decision on imposing a fine.

h. § 3. KEY PERSONEL

1. Pursuant to Article 7 of the AML Act, the Board of Directors of the Company shall appoint from among its members, by resolution, an AML Board Member to ensure compliance with the ati-money laundering and countering the financing of terrorism provisions in the Company and to execute duties provided for in the AML Act and the Policy. The first AML Board Member shall be appointed no later than the date of adoption of this Policy.
2. In the case of a single-person Board, the AML Board Member shall become the only member of the Board without the need for an additional resolution of the Board in this matter.
3. Pursuant to Article 6 and 8 of the AML Act, a permanent position of the AML Coordinator shall be established in the Company, appointed by the Board of Directors by resolution from among the Employees holding managerial positions in the Company.
4. Pursuant to Article 6 and 8 of the AML Act, a permanent position of AML Coordinator is created in the Company, appointed by the Company's Management Board by way of a resolution from among the Company's Employees holding managerial positions in the Company. The AML Coordinator shall ensure that the Company and its Employees comply with the provisions of the Act and shall give notices on behalf of the Company in all cases where it is required to do so by law. The AML Coordinator's role is, in particular, to implement, perform and supervise the obligations set out in the Act and to comply with the procedures set out in this Procedure, including approving Employees' activities in assessing the risk of a Customer or transaction or carrying out such activities. The first AML Coordinator shall be appointed no later than on the date of execution of the first Transaction. The AML Coordinator in performing his duties set forth in the Procedure reports directly to the Member of the Management Board responsible for AML.
5. The AML Coordinator shall concurrently perform the functions pursuant to Article 6 and 8 of the AML Act. As the staff of the Company increases, the Company may appoint, in addition, separately from the AML Coordinator, an Employee acting as a senior executive responsible for carrying out the duties set out in the Act, in Article 6 of the AML Act. In such case, the AML Coordinator will be required to consult with such person on any material actions taken under the Procedure and any concerns regarding the fulfilment of obligations under the AML Act, in particular the AML Coordinator will be required to consult on updating the overall risk score, o referred to in § 4 Procedure.
6. Each Employee of the Company, regardless of the form and type of employment, is responsible for fulfilling his/her obligations in the area of anti-money laundering and counteracting the financing of terrorism, and in particular is obliged to become familiar with this Procedure, implement its provisions and comply with them. Each Employee confirms that he/she is familiar with the Procedure by putting his/her handwritten signature on the Declaration, the specimen of which constitutes Appendix No. 1 to the Procedure.
7. Persons performing duties in connection with the prevention of money laundering and terrorist financing are also obliged to maintain the secrecy of the information they obtained in the course of performing activities within the scope specified in the Procedure. This obligation continues even after the termination of the employment relationship or performance of activities under civil law contracts.

i. § 4. RISK ASSESSMENT OF THE MONEY LAUNDERING AND TERRORIST FINANCING INVOLVING COMPANY'S OPERATIONS

1. The Company has conducted an initial assessment of the money laundering and terrorist financing risks relating to the Company's business, and in accordance with Article 27 of the AML Act, the Company shall also periodically assess such risks (hereinafter referred to as the **"business risk assessment"**).
2. The business risk assessment shall be prepared by the Company in paper or electronic form. The business risk assessment in electronic form requires the implementation of a dedicated computer application, which cannot be used to delete or change electronic records once entered and should guarantee the correctness of the layout of the data transmitted to the General Inspector.
3. In assessing business risks, the Company takes into account risk factors relating to: Customers, countries, geographical areas, product, services, Transactions and their delivery channels, the level of value of the Transactions carried out, the purpose, regularity od duration of the business relationship, and is further guided by the results of the applicable National Risk Assessment, the outcome of internal controls and audits. In order to conduct a risks assessment of operations, the Company:

    a. Identifies and defines risk factors in its operations,
    b. Assigns measures to individual risk factors,
    c. Collects the necessary data and subjects it to verification,
    d. Assigns scores to individual risk factors,
    e. Analyses irregularities and weaknesses identifies in the Company's internal controls,
    f. Takes into account the overall scoring of the individual risks,
    g. Obtains the residual risk level and determines the residual risk acceptance level,
    h. Formulates the conclusions of the assessment and possible remediation plans.

4. The risk assessment of the activity is documented in a report containing at least: a description of identified risk factors of money laundering and terrorist financing as part of activity, the level of risk determined together with a justification and an indication of measures to eliminate or reduce the identified risk.
5. The business risk assessment is prepared by the AML Coordinator individually or with the assistance of the Company's Employees. The risk assessment is each time approved by the Member of the Management Board responsible for AML.
6. Upon request by the General Inspector, the AML Coordinator will provide the Inspector General with an initial and periodic risk assessment of the activity and other information that may affect the National Risk Assessment.
7. The Company shall update its business risk assessment at least once every 2 years, in addition, The Company is required to update its periodic risk assessment when:

    a. its risk mitigation measures prove ineffective,
    b. the company will implement a new range of services or transactions,
    c. the Company determines that there has been a change in the risk factors of Customers, products or services, their delivery channels,
    d. the Company will expand its operations into new geographic areas,
    e. there will be a change in the National Risk Assessment.

j. **§ 5. RISK ASSESSMENT OF CLIENTS AND TRANSACTIONS**

1. The Company assesses the risk of money laundering and terrorist financing associated with the business relationship or the Occasional Transaction, evaluates the level of risk identified and documents the assessment performed.
2. As a consequence of the risk analysis, each Customer is classified to the appropriate risk category. The principles and method of classifying the Customer to the proper risk category are described in Appendices no 2 and no 3 – Risk assessment of the Customer (individual – natural person and institutional, respectively). Customer's risk assessment may be partially or fully automated with the use of adequate IT systems.
3. The Company distinguishes the following categories of Customer's risk:

    a. The Company distinguishes the following categories of Customer risk:

b. Normal – normal financial security measures apply to this risk category,
c. Increased – enhanced financial security measures apply in this risk category,
d. PEP – this is a higher risk type, and enhanced financial security measures apply in this risk category,
d. unacceptable – business relationships are not established and Occasional Transactions are not conducted in this case.

4. The Company shall analyse the risk of money laundering or terrorist financing associated with a business relationship or Occasional Transaction taking into account, the following factors:

a. Transactions value,
b. Customer type,
c. Geographical area, taking into account the high-risk country defined in in Appendix no 5 to the Procedure and other countries referred to in Article 43 (2) (10) of the Act.
d. connections with PEP,
e. operating in high-risk money laundering industry,
f. the method of establishing relationships,
g. provide risk assessment information,
h. the purpose, regularity and duration of the business relationship.

5. Circumstances that may indicate a higher risk of money laundering include, in particular:

a. Reluctance to provide information or documents,
b. establishment of business relationships under unusual circumstances,
c. unusual behaviour of the Customer,
d. the circumstance that the Customer or the Beneficial Owner is a resident of a high-risk third country within the meaning of the Act or another of the countries specified in Article 43 (2) (10) of the Act, or other connection of the business relationship or Occasional Transaction with such a country,
e. the circumstances that the Customer is a company in which bearer shares have been issued, whose securities are not admitted to organised trading, or a company in which rights from shares are exercised by entities other than shareholders or shareholders,
f. the fact that the Customer is a legal person or an organizational unit without legal personality, whose activities are used to store personal assets
g. establishing or maintaining a business relationship or carrying out occasional Transaction without the physical presence of the Customer - if the related higher risk of money laundering or terrorist financing has not been reduced in any other way, including by using a notified means of electronic identification, the requirement to use a qualified electronic signature or signatures confirmed by the trusted profile ePUAP,
h. Customer's use of service or products that promote anonymity or make identification difficult,
i. atypical or excessively complex ownership structure of the Client, taking into account the type and scope of its business activity,
j. establishment of business relations in unusual circumstances,
k. carrying out by Customer a large number or large amount of Cash Transactions,
l. ordering by unknow or unrelated third parties of Transaction where the Customer is the beneficiary,
m. other circumstances indicating that the Customer's actions may be related to money laundering or terrorist financing, including other circumstances indicated in the Act.

6. The Company strictly applies the enhanced financial security measures referred to in § 6.5 of the Procedure, when the Customer:

a. has PEP status,

b. comes from a high-risk third country or has its registered office in such a country, subject to the exclusions contained in the Act,
c. has provided information regarding the Beneficiary that is inconsistent with the contents of the CRBR.

7. In the case of a Transaction involving a high-risk third country identified by the European Commission in a delegated act adopted pursuant to Article 9 of Directive 2015/849, the Company shall also:

a. undertakes additional actions within the framework of applicable enhanced financial security measures referred to in § 6 Sec. 5 of the Procedure,
b. imposes increased obligations in respect of information provision or reporting of Transactions,
c. limits the scope of business relations or Transactions or does not enter into business relations or Transactions.

k. § 6. KEY SECURITY MEASURES

1. The Company shall apply financial security measures when:

a. establishing a business relationship:
b. carrying out an occasional Transaction:
- of the equivalent of 15,000 euro or more, regardless of whether the Transaction is carried out as a single operation or several operations that appear to be linked, or
- which represents a transfer of funds of an amount exceeding the equivalent of 1,000 euros, or
- in cash with a value of the equivalent of 10,000 euros or more, regardless of whether the transaction is carried out as a single operation or as several operations that appear to be linked,
- with the use of Virtual Currency of the equivalent of 1,000 euros or more;

c. suspicion of money laundering or terrorist financing;
d. doubts about the veracity or completeness of the Customer’s identification data obtained to date.

2. The financial security measures employed by the Company include:

a. Identification of the Customer and verification of his/her identity;
b. Identification of the Beneficial Owner and taking reasonable steps to:
– Verify its identity,
– Identification of the Beneficiary and taking reasonable steps to: verify his identity, determine the ownership and control – in the case of a Client who is legal person or a organizational unit without legal personality or trust
c. Assessing the business relationship and, as appropriate, obtaining information on its purpose and intended nature;
d. ongoing monitoring of the Customer's business relationships, including::
– analyzing the Transactions conducted in the business relationships to ensure that the Transactions are consistent with the Company’s knowledge of the Customer, the type and scope of the Customer’s business and consistent with the risk of money laundering and terrorist financing associated the that Customer
– examining the source of origin of the assets at the Customer's disposal - in cases justified by the circumstances,
– ensuring that the documents, data or information held in relation to the business relationship are kept up-to-date..

3. The Company shall apply financial security measures with respect to Clients on the basis of risk assessment determined in accordance with the principles laid down in § 5 of the Procedure.
4. If the Company cannot apply one of the financial security measures:

   a. Does not establish a business relationship;
   b. Does not carry out an accessional transaction;
   c. Does not carry out a Transaction through a bank account;
   d. Terminates a business relationship.

5. In the case of high-risk Customers, including Customers with PEP status, the Company applies enhanced financial security measure consisting in:

   a. obtain additional detailed information about the Customer directly from the Customer, or by using additional sources;
   b. requesting additional documents or information from the Customer in order to verify his/her identity
   c. requesting additional documents from the Customer, which will clarify doubts regarding the executed Transactions, indicate the source of funds and which will help to establish the purpose and circumstances of executing Transactions
   d. intensification of the Customer's risk analysis and monitoring of the Transactions executed;
   e. intensification the analysis of business relations with the Customer;
   f. applying appropriate additional measures for verifying the identity of the Customer or Beneficial Owner;
   g. acquiring additional information on the intended nature of the business relationship;
   h. obtaining the approval of the AML Board Member to establish or continue a business relationship;
   i. obtaining information about the reasons and circumstances;
   j. providing the Customer with a document certified by an appropriate authority or notary public.

6. The Company applies financial security measures also with regard to the Customer with whom it has business relations, taking into account the identified risk of money laundering and terrorist financing, in particular when:

   a. There has been a change in the previously established nature or circumstances of the business relationship;
   b. There has been a change in previously established data concerning the Customer or the Beneficial Owner;
   c. The Company was obliged during the calendar year in question by law to contact the Customer in order to verify the information concerning the Beneficial Owners, in particular when such obligation resulted from the provisions of the Act of 9 March 2017 on the exchange of tax information with other countries.

7. In case of an Occasional Transactions not exceeding the amount of EUR 1,000, the Company does not apply financial security measures unless the circumstances indicate that the Transaction is executed in order to circumvent the limits set out in the Act
8. The Company shall apply enhanced financial security measures in cases of the establishment of business relations or the occurrence of Transactions related to a high-risk third country, identified by the European Commission in the delegated act adopted pursuant to Article 9 of Directive 2015/849, for which purpose it is mandatory for the Company to take the measures specified in paragraph 5(d-i). In addition, the Company shall apply the other measures indicated in the Act.

l. § 7. IDENTIFICATION AND VERIFICATION OF CLIENTS AND BENEFICIARY OWNERS

1. In situations, where the Company is required to apply financial security measures, the Company shall identify the Client. Identification of the Client consists in:
   a. Checking the identity of the Client who is a legal entity by determining and recording:
      - name (company),
      - organisational form,
      - address of the registered office and/or business address,
      - Tax Identification Number (NIP), and if there is no such number – the country of registration, the name of the appropriate register and the number and date of registration,
      - Name and surname and PESEL number or date of birth and country of birth of the person representing the Customer;
   b. Verifying the identity of the Customer who is a natural person by determining and recording:
      - name and surname,
      - nationality,
      - PESEL number or date of birth – in case no PESEL number was assigned country of birth,
      - Series and number of the identity document,
      - Address of residence - if the Company has this information,
      - If the Customer is a natural person conducting business activities – additionally the name, Tax Identification Number (NIP) and the address of the main business activity.
   c. Identifying and verifying the identity of the Beneficial Owner by determining and recording:
      - name and surname,
      - nationality,
      - and, if the information is held by the Company, also:
        - PESEL number or date of birth – if no PESEL number has been assigned,
        - country of birth,
        - series and number of the identity document,
        - address of residence.

2. Verification of the identity of the persons indicated in paragraph 1 consists in confirming the established identification data on the basis of a document stating the identity of the natural person, a document containing current data from an extract from the relevant register (National Court Register, Central Register of business activity, other) or other documents, data or information from a reliable and independent source, including, where available, from electronic identification means or from the relevant trust services as defined in Regulation 910/2014. The Company verifies the identity of the persons indicated in paragraph 1 in particular using the user registration procedure available on the Company Website, during which, inter alia, the Company collects the required information and statements, a copy of the identity document of the Customer or its representative, a photograph of the Customer or its representative, documents regarding the ownership structure of the Customer. Identity verification may be carried out partially or fully in an automated manner using the IT Systems implemented by the Company.
3. In the case of the Customers who are not natural persons, covered by the obligation to report data to the Central Register of Beneficial Owner (hereinafter: "CRBR") the Company shall each time verify the information provided by the Customer and available from other sources concerning the identity of the Beneficial Owner with the content of information gathered in the CRBR, including with the use of IT Systems implemented in the Company. When verifying the Beneficiary, the Company may not rely solely on the information contained in the CRBR.
4. The Company will record the Customer's image in the form of a photograph in a situation when it carries out the verification of the Customer's identity remotely.

5. The Company takes steps to determine whether the Customer or the Customer's Beneficial Owner has PEP status. For this purpose, in particular it receives from the Customer an appropriate declaration in written or documentary form (by e-mail or through the Service), the specimen of which is attached as Appendix No. 7 to the Procedure, and applies IT Systems aimed at verifying the Client's and Beneficiary's data against the databases of persons having PEP status available in a given application.
6. In the event that the Company has, or is about to enter into a business relationship with PEPs, it shall apply enhanced financial security measures, including the mandatory obtaining of written approval of the AML Member of the Board of Directors to enter into or continue a business relationship with PEPs. The approval to enter into a business relationship shall be attached to the Customer's risk assessment.
7. The Company implements IT systems also aimed at verifying the Customer and Beneficial Owner from the perspective of the Financial Supervision Authority's warning list. In such case, section 6 above applies accordingly.
8. The Company shall take steps to determine whether the Customer or the Customer's Beneficial Owner has been entered on the sanction lists referred to in section 118 of the Act. For this purpose, in particular, it uses IT Systems aimed at verifying the data of the Customer and the Beneficial Owner with the databases of persons entered on sanction lists available in the given application. In the event that the Client or Beneficiary is found to have been entered on sanction lists, § 12 of the Procedure shall apply.

m. § 8. RECORDING OF DISCREPANCIES WITH INFORMATION HELD IN THE REGISTER

1. If a discrepancy is found between the CRBR and the Beneficial Owner information provided by the Customer or determined by the Company, this circumstance shall be noted in the Client's risk assessment form and in the Transaction analysis note. If a discrepancy is found, the Company applies enhanced financial security measures.
2. The Company shall record in the risk assessment form and in the Transaction analysis note all impediments resulting in the impossibility to determine or doubts as to the identity of natural persons who are the Beneficial Owners and actions taken in connection with the identification as the Beneficial Owner of a natural person holding a senior management position. The Company may recognise as the Beneficial Owner a person referred to in Article 2(2)(1)(a) indent 5 of the Act (i.e. a person holding a senior management position), provided that the conditions under the Act are met and in addition previously::
    a. Has carried out all steps available to it for the purpose of identifying the Beneficiary in accordance with the rules set out in Article 2 (2) (1) (a) indents 1-4,
    b. The doubts or impossibilities of identifying the Beneficial Owner in accordance with letter a. above has been documented in accordance with the Procedure,
    c. there was no suspicion of the money laundering or terrorist financing.
3. In the cases, referred to in subsection (1) and subsection (2), the person who noted the discrepancies or impediments shall immediately notify the AML Coordinator.
4. AML Coordinator shall conduct a gap analysis and apply one or more of the enhanced financial security measures and take additional action to address the concerns.
5. In a more serious situation where circumstances indicate an increased likelihood of money laundering or terrorist financing, the AML Coordinator shall obtain the approval of the AML Board Member to establish or continue a business relationship or to conduct an Occasional Transaction.

n. § 9. MONITORING OF ECONOMIC RELATIONS

1. The Company in the course of its business, monitors and analyses the executed Transactions, business relationships on an ongoing basis and reviews Customers on a periodic basis for the purpose of::

a. verification of the timeliness of data on the Customer, including data identifying the Customer, its beneficial owners and persons authorized to act on its behalf;
b. verification of data concerning business relations with the Customer, including their purpose and intended nature;
c. verification of the sources of origin of the property values held by the Customer - in cases justified by the circumstances, in particular if the Company applies increased financial security measures with respect to the Customer;
d. reviewing Transactions carried out by the Customer.

2. The AML Coordinator shall be the person responsible for carrying out the activities specified in paragraph 1. The execution of the actions specified in paragraph 1 shall be documented in the form of a note.

o. § 10. SELECTING OF TRANSACTIONS

1. The Company monitors and analyse Transactions on regular basis to identify suspicious Transactions and keeps internal records of Transactions. Each Transaction kept in internal records is provided with unique ID number.
2. A transaction should be considered suspicious, regardless of its value and nature, if the Company determines that circumstances exist in relation to it which indicate that it may be related to money laundering or terrorist financing.
3. The Transaction selection procedure consists of the following steps:
   a. to collect information about a given Customer upon the establishment of a business relationship and to update this information on an ongoing basis throughout the duration of that relationship
   b. risk assessment of the Customer,
   c. analysis of Transactions of a given Customer, taking into consideration the results obtained during the risk assessment.
4. Within the scope of the activities specified in paragraph 2, the Company analyses the Transactions in terms of considering them suspicious, the Employee prepares a note on the analysis of the Transactions in accordance with the template specified in Appendix No. 9 - Note on Analysis of Transactions.
5. Persons performing analysis should pay attention to the following types of Transactions and the circumstances surrounding the Transactions:
   a. The sale or purchase or Virtual Currencies occurred at an unfavourable time;
   b. The Transaction was made from a different account or using a different account number than that indicated by the funds holder;
   c. The transfer of funds was made from an account that does not belong to the Customer;
   d. The Transaction made is economically unreasonable;
   e. An unusual pattern of activity by the Customer, not similar to the Customer's previous behaviour or business profile;
   f. Frequent Transactions for amounts below the limits set by the Act;
   g. Transaction below the limits specified in the Act are made by an affiliate of the Customer and by the Customer;
   h. Frequent Transactions for relatively small amounts between the same Customers;
   i. The transaction is unusual, given the knowledge and experience of the person performing the analysis;
   j. Frequent Transactions from accounts originating from different users from different accounts with the same names or other data, if there is suspicion that it may be the same person or a person closely related to that person;
   k. Transactions for very large amounts that occur within a short period of time after the account is opened by the Customer in question;

l. Transaction of a very large amount by a Customer who has not made any Transactions for a very long period of time;
m. A sudden increase in Transactions by a particular Customer that is unusual for the Customer's previous behaviour;
n. Avoidance of registering a user account by frequently making small Transaction;
o. Frequent transfers that appear to be inconsistent with the claimed business activity;
p. The Customer has performed a large number of Transactions for a total amount exceeding EUR 15,000;
q. The Customer avoids or refuses to provide documents to enable its verification;
r. Transactions are made from the same account number but by different Customers;
s. A significant increase in the number of Transactions originating from a single city/geographic area or country;
t. Customer provides unclear, incomplete and suspicious information;
u. The amount of the Transaction has increased abnormally as compared to previous Transactions made by the Customer in question;
v. The Transaction deviates from typical Transactions typically executed by the Customer in question;
w. Cyclical repetition of Transactions involving "round" amounts;
x. The Transaction is unreasonable due to the business profile of the Customer;
y. Taking into account all the circumstances surrounding the Transaction, there are other reasons to suspect money laundering or terrorist financing.

6. Persons monitoring Transactions should pay particular attention to the results of the Customer risk analysis including;

a. The type of Custmer;
b. The country or geographic area from which the Client and Beneficial Owner originate;
c. Whether the Customer is the subject of any law enforcement interest or other proceedings relating directly or indirectly to money laundering or terrorist financing;
d. Information contained in the applicable National Risk Assessment;
e. The value of assets deposited by the Customer;
f. The amount and regularity of transactions;
g. The method of communication with the Customer;
h. Service delivery channel.

7. The Company monitors Transactions an ongoing basis, in particular by:

a. Manually monitoring and analysing data relating to individual Transactions, such as the type of Transaction, the date of the Transaction, the type of Customer and the results of the Customer's risk assessment, the value of the Transaction, the address of the Customer's portfolio, the origin of the Customer's funds, the possibility of linking the Transaction to other Transactions, including by analysing the portfolios used, the Customer's accounts and the Customer's photos, other circumstances found concerning the Transaction,
b. Automated monitoring and analysis of Transactions using the implemented IT Systems, including in particular the iAML scanner implemented by the Company.

8. If a Transaction is found to be a Suspicious Transaction, the AML Coordinator shall prepare a notification to the Inspector General in accordance with the procedure provided for in the Act..

p. **§ 11. HANDING OVER INFORMATION TO GENERAL INSPECTOR**

1. The Company is obliged to provide the General Inspector with information on:

a. accepted deposit or executed withdrawal of funds of the equivalent of more than 15,000 euros;
b. executed transfer of funds of the equivalent of more than 15,000 euros, except for:

- the transfer of funds between a payment account and a term deposit account that belong to the same Customer at the same obliged institution,
- national transfer of funds from another obliged institution,
- A transaction related to the obliged institution's own economy, which was executed by the obliged institution in its own name and on its own behalf, including a transaction concluded on the interbank market,
- Transaction executed on behalf of or for the benefit of public finance sector units, referred to in Art. 9 of the Act on Public Finance of 27 August 2009,
- Transaction executed by a bank associating cooperative banks, if information about the Transaction was delivered by the associated cooperative bank,
- transfer of ownership to secure assets, executed for the duration of the transfer of ownership agreement with the obliged institution.

c. a purchase or sale Transaction of foreign exchange, the value of which exceeds EUR 15,000 or about intermediating in such a Transaction..

2. The Company shall notify the General Inspector of circumstances that may indicate a suspicion of money laundering and terrorist financing offence. The detailed procedure in this respect is determined by the Act.
3. At the request of the General Inspector, the Company shall immediately provide or make available the information or documents which are necessary for the performance of the tasks of the Inspector General, in the scope specified by the Act..
4. The notifications referred to in this § 11 are prepared by the AML Coordinator.
5. The Company's Employee who learns of a situation requiring a notification to the General Inspector shall immediately inform the AML Coordinator and cooperate with him/her to send the notification.
6. The Company and its Employees shall keep strictly confidential the records of the fact of providing the Inspector General or other competent authorities with information related to the performance of their duties under the Act, including the information indicated in this § 11.

q. § 12. SPECIFIC RESTRICTIVE MEASURES

1. In order to prevent terrorism and terrorist financing, the Company applies specific restrictive measures with respect to persons and entities referred to in Article 118(1) of the Act, consisting in:

   a. freezing of property values owned, held, controlled directly and indirectly by persons and entities, as well as benefits derived from such property values, which means preventing their transfer, alteration or use, as well as carrying out any operation involving such values in any way that may result in a change in their size, value, place, ownership, possession, nature, purpose or any other change that may enable benefits to be derived from them;
   b. not making property values available directly or indirectly to or for the benefit of persons and entities, which means, in particular, not granting loans, consumer credit or mortgage credit, not making donations, not making payments for goods or services.

2. The detailed procedure for the application of the measures referred to in this paragraph, including the rules for making entries in the sanction lists, shall be determined by the Act.
3. The AML Coordinator shall be responsible for the application of restrictive measures by the Company in accordance with this chapter. Information on the application of specific restrictive measures shall be immediately communicated by the AML Coordinator to the AML Member of the Board.

r. §13. EMPLOYEES TRAINING

1. Each person employed by the Company and each other person acting for and on behalf of the Company is required to undergo periodic AML and CFT training.
2. The AML Board Member and the AML Coordinator shall receive AML and CFT training at least once a year.
3. An Employee's participation in AML and CFT training must be documented.
4. Training shall be conducted before the Employee is allowed to work, periodically and when necessary in a given situation
5. The training should cover in particular:

    a. Obligations incumbent on Employees related to the need to implement the procedure on countering money laundering and terrorist financing,
    b. Modern methods on counteracting money laundering,
    c. Identification of risks related to money laundering in the Company,
    d. Recognition and detection of activities related to money laundering,
    e. application of financial security measures,
    f. methods of Customer identification,
    g. typing Transactions,
    h. familiarizing Employees with the Procedure.

s. § 14. RULES ON WHITSLEBLOWING

1. The Company implements an internal procedure for anonymous reporting of actual or potential violations of anti-money laundering and terrorist financing regulations by Employees and other persons performing activities for the Company (hereinafter: "reporting persons"):
2. A report may be submitted as follows:

    a. In writing to the Company's registered address,
    b. Electronically to the e-mail: exchanges@geocurrency.io,
    c. Using the contact form available on the Company's Website.

3. The application does not require disclosure of the identity of the applicant (the Company allows anonymous submissions).
4. The person responsible for receiving reports is the AML Coordinator.
5. Within no more than 14 days of receiving the notification, the AML Coordinator shall carry out activities aimed at verifying the circumstances indicated in the received notification, including determining the circumstances of actual or potential violations of AML and terrorist financing regulations.
6. The AML Coordinator after performing the actions indicated in section 5 above, shall prepare a report containing a description of the breach, actions taken by the Company and findings based on the notification received. If an irregularity is detected, the AML Coordinator shall take appropriate follow-up action in order to prevent such violations from occurring in the future.
7. The AML Coordinator shall keep the data of the reporting person (including personal data) strictly confidential, and where such data can be determined indirectly, he shall be obliged not to determine it. The Company shall ensure the protection of personal data of the reporting persons. Personal data shall be collected in a separate data file. The AML Coordinator shall ensure that the personal data, in particular the reporting person's identification data contained in the notification are removed from the Company's IT systems and the Company's documentation no later than within one month of receiving the notification.
8. The reporting person shall be protected against any oppressive action, discrimination or other unfair treatment either by the Company or its Employees or other persons carrying out activities for the Company. In particular, such a person must not be subject to any formal or informal disciplinary sanctions or threats. In particular, the fact of making a report cannot be the basis for terminating a contract concluded with such a person,

changing his/her employment conditions or limiting his/her access to any benefits available to the Company's Employees or any other actions impairing his/her legal or factual situation..

9. The reporting person, if exposed to the activities referred to in paragraph (8), shall be entitled to report such activities to the General Inspector. Submission of a report shall not violate the obligation of professional secrecy.
10. The AML Coordinator is responsible for monitoring compliance with the provisions of this §14. In the event of any breach of the Company's obligations under this Section 14, the AML Coordinator shall promptly implement appropriate corrective actions, including calling upon individual Employees to take or refrain from taking certain actions, directing instructions to persons responsible for HR matters, requesting the Member of the Board of Directors responsible for AML matters to take appropriate actions which are within the competence of the Board of Directors..
11. In the event that the AML Coordinator directly accepts a report from a reporting person, the AML Coordinator must advise the reporting person of his or her rights under paragraph 8 and paragraph 9 above.
12. The Company shall store personal data contained in applications for no longer than one year from the time of the report referred to in subsection 6. In the event that during this period the Company begins to conduct litigation or other similar activities, the one-year period for the deletion of personal data begins with the expiry of one year from the completion of these activities.

t. **§ 15. RULES ON RECORD KEEPING AND INFORMATION PROTECTION**

1. The AML Coordinator shall be the person responsible for properly organizing the collection and retention of records related to compliance with the Act and implementation of this Procedure.
2. The Company shall retain for a period of 5 years from the termination of the business relationship with the Customer or in which the Occasional Transactions were carried out documents in the form of:

    a. copies of documents and information, including information obtained by means of electronic identification and trust services allowing electronic identification within the meaning of Regulation 910/2014;
    b. evidence of Transactions carried out and records of Transactions, including original documents or copies thereof necessary to identify Transactions.

3. The Company shall keep the results of the current analysis of the Transactions for five years, starting from the first day of the year following the year in which they were carried out.
4. In particular, the Company archives:

    a. Customer identification forms and copies of documents obtained to verify the data provided therein,
    b. Customer risk assessment forms, including risk assessment updates,
    c. Transaction analysis notes,
    d. Internal audit protocols,
    e. Notifications and information sent to the Inspector General,
    f. Documents confirming that Employees have undergone the training specified in the Procedure.

5. Documentation may be stored and archived in electronic form. This does not apply to documents obtained by the Company in traditional, written form.
6. The AML Coordinator shall ensure that specific procedures are implemented to secure the documentation and protect information related to the implementation of obligations under the Act, including in particular the results of risk assessment of a Customer or Transaction.

7. The Company and its Employees shall keep strictly confidential all documentation related to the performance of their obligations under the Act, in particular, the analyses conducted on money laundering or terrorist financing.

u. §16. RULES OF INTERNAL CONTROL

1. The function of internal control is to implement the provisions of this Procedure and the Act.
2. Internal control in the Company is performed by the AML Coordinator on a permanent and ad hoc basis.
3. The correctness of the internal controls is supervised by the AML Member of the Board.
4. The purpose of internal controls is to examine the proper implementation of the principles contained in the Procedure, the effectiveness of their implementation, the collection of information needed for the proper management of the procedure for the prevention of money laundering and terrorist financing, including for making the right decisions.
5. The Company does not provide for the introduction of a control plan in the field of anti-money laundering and terrorist financing. The AML Coordinator continuously undertakes ordinary control activities in order to detect possible irregularities. Regular control activities consist in particular of:
    a. analysing current documentation regarding the implementation of the Procedure,
    b. ensuring that the Company's Employees are properly trained in anti-money laundering and terrorist financing,
    c. examination of changes in regulations,
    d. introducing innovations in terms of improving the Procedure,
    e. other activities, which the AML Coordinator deems necessary due to the state of his knowledge and experience.
6. Ad hoc inspections are of an intervention nature, and are carried out in case of an urgent need and upon the instructions of the AML Member of the Management Board.
7. If an irregularity is revealed during the internal inspection, the AML Coordinator immediately informs the Member of the Board for AML and takes necessary actions to remove the irregularity.
8. The AML Coordinator is obliged to inform the Board Member responsible for AML about any irregularities detected during the internal audit. In the case of permanent control, the AML Coordinator prepares a report on internal control by the end of January of the following year, to which the internal control pertained, as of December 31st of the previous year.

v. §17. FINAL PROVISIONS

1. This Procedure is confidential and internal, it is forbidden to share it or disseminate it to any third party without the express consent of the members of the Board of Directors.
2. Information on the content of this Procedure may be disseminated in other regulations, procedures and policies, subject to the adoption of such documents by the Board of Directors.
3. The Company, bearing in mind Article 48 paragraph 1 of the Act, may entrust the application of financial security measures and conducting and documenting the results of analysis of Transactions, to another entity under a written agreement.
4. Annexes to the Procedure constitute an integral part of the Procedure. The appendices constituting model statements or forms need to be adjusted to the manner of their submission, in particular, when the statements will be submitted via the Service.
5. In matters not regulated by this Procedure, the provisions of law shall apply, including in particular the provisions of the Act.
6. This Procedure shall enter into force as of the date of its adoption, i.e. 17.03.2022.

w. **ANNEXES:**

1) Annex no 1 – STATEMENT OF EMPLOYEE,
2) Annex no 2 – KYC SURVEY (for individuals),
3) Annex no 3 – KYC SURVEY (for entities),
4) Annex no 4 – STATEMENT REGARDING A BENEFICIAL OWNER,
5) Annex no 5 – LIST OF HIGH-RISK COUNTRIES FOR MONEY LAUNDERING AND TERRORIST FINANCING,
6) Annex no 6 – LIST OF HIGH-RISK INDUSTRIES FOR MONEY LAUNDERING AND TERRORIST FINANCING,
7) Annex no 7 – STATEMENT REGARDING PEP,
8) Annex no 8 – CHANGE OF RISK EVALUATION,
9) Annex no 9 – TRANSACTION ANALYSIS NOTE.

d.

ACCEPTED:

Przemysław Borecki
The AML Board Member
(17.03.2022)

Policy approved in decision no 1/03/2022 dated: 17th March 2022.