

AML POLICY

A. ANTI-MONEY LAUNDERING

This policy is to establish guidelines for **NV Poland SPÓŁKA Z OGRANICZONĄ** (“Company” or “Exchange”), ‘Anti-Money Laundering’ and ‘Know Your Client’ (“KYC”) procedures for new and existing clients.

All of monetary transactions, to the best knowledge of the Company shall be free from any form of money laundering and terrorist activities. The Company operates with integrity and is committed to implementing the measures established. The Client’s failure to comply with the regulations set by the Company would mean termination of the account. If the Client is proven of committing money laundering, he is responsible for any damage or loss which may occur, and the Company is excluded from his fraudulent actions.

In an effort to counter money laundering and other illegal activity, we have decided not to support any cash transactions, regardless of their stated purpose. Our firm has the right to cancel or deny a transaction at any point if there are suspicions regarding its legality.

Obligation

The obligation to observe the policy rests with Management Board members and employees of the Provider of service, including temporary staff, agents of the Provider of service who initiate or establish Business Relationship (hereinafter all together called the Representative). Every Representative must confirm awareness of the policy with the signature. The policy is primarily based on the regulations of Republic of Poland Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter the “Law”) of the Republic of Poland.

Definitions

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

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

Sanctions – mean an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, following human rights and international law or achieving other objectives of the United Nations Charter or the common foreign and security Policy of the European Union.

Terrorist Financing – shall mean any act which constitutes an offence within the meaning of Article 2 of the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999.

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

FSC - Financial Supervision Commission (FSC)

SANS – State Agency ‘‘National Security’’

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

Transaction – cash flow or payment order or cryptocurrency wiring from a Client to the Provider of service.

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

Beneficial Owner – is a natural person, who:

- Taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed taking advantage of his influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.
- Ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means. Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. Indirect ownership is a manner of exercising control whereby a company which is under the control of a natural person holds or multiple companies

which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

- Holds the position of a senior managing official, if, after all possible means of identification have been exhausted, the person specified in clause ii cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner.
- In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations': settlor or person who has handed over property to the asset pool, trustee or manager or possessor of the property, person ensuring and controlling the preservation of property, where such person has been appointed, or the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.

Politically Exposed Person or PEP - is a natural person who is or who has been entrusted with prominent public functions including a head of state, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a state-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials.

- The provisions set out above also include positions in the European Union and in other international organizations.
- A family member of a person performing prominent public functions is the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.
- A close associate of a person performing prominent public functions is a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

- **Local Politically Exposed Person or local PEP** – a natural person, who performs or has performed prominent public functions in Lithuania, a contracting state of the European Economic Area or in an institution of European Union.

Provider of service – NV Poland SPÓŁKA Z OGRANICZONĄ, Number 387744901, UL. PRZESKOK 2, Warsaw 00-032 PL.

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

Equivalent Third Country – means a country not a Member State of European Economic Area but applying an equivalent regime to the European Union corresponding (AML)

Virtual currency - a value represented in the digital form, which is digitally transferable, preservable or tradable and which persons accept Provider of service – as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same directive.

Description of activities of the Provider of service

The Provider of service is the provider of a service of exchanging a virtual currency against another virtual currency and/or exchanging a virtual currency against a fiat currency, and/or vice versa and safekeeping crypto funds on behalf of clients.

Compliance Officer

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

- monitor the compliance of the Policy with the relevant laws and compliance of the activity of the Representatives with the procedures established by the Policy;
- compile and keep updated the data regarding countries with low tax risk, high and low risk of Money Laundering and Terrorist Financing and economical activities with great exposure to Money Laundering and Terrorist Financing;
- carry out training, instruct and update the Representatives on matters pertaining to procedures for prevention of Money Laundering and Terrorist Financing;
- report to the MB once a year (or more frequently, if necessary) on compliance with the Policy, and on Transactions with a suspicion of Money Laundering or Terrorist Financing;

- collect, process and analyse the data received from the Representatives or Clients concerning suspicious and unusual activities;
- collaborate with and report to the FSC on events of suspected Money Laundering or Terrorist Financing, and respond to enquiries of the FSC;
- make proposals on remedying any deficiencies identified in the course of checks.

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

Legal Framework

Polish licensed exchange Companies are required to comply with the Measures Against Money Laundering Act (MAMLA) as well as the provisions of the European 5th AML Directive (the "Law" for the purposes of this policy) regarding the prevention of Money Laundering and Terrorist Financing. The main purpose of the Law is to define and criminalize the laundering of proceeds generated from all serious criminal offences aiming at depriving criminals from the profits of their crimes.

1. Legislative Framework

- Measures against Money Laundering Act (MAMLA), last amended 28 February 2020
- Rules of Implementation of the MAMLA, last amended 13 March 2020
- NRA, published by SANS on 9 January 2020
- Measures against Terrorism Financing Act (MATFA), last amended 29 November 2019

2. European Framework

- Directive (EU) 2018/843 - The Fifth Money Laundering Directive of the European Parliament on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing.

In accordance with the Law, Exchanges are obliged to set out policies and procedures for preventing money laundering activities. Those procedures, which are implemented by the Company, as these are requested by the Law, are the following:

- Identification and due diligence procedures of clients.

- Record keeping procedures in relation to clients' identity and their transactions.
- Internal reporting procedures to a competent person (e.g. Anti-Money Laundering Compliance Officer) appointed to receive and consider information that give rise to knowledge or suspicion that a client is engaged in money laundering activities.
- Appropriate procedures of internal control, risk management, with the purpose of preventing money laundering activities.
- The detailed examination of every transaction that due to its nature is considered vulnerable to money laundering, and especially for complicated or unusually large transactions and transactions that are taken place without an obvious financial or legal purpose.
- Measures for making employees aware of the above-mentioned procedures to prevent money laundering and of the legislation relating to money laundering.
- Provision of regular training to their employees in the recognition and handling of transactions suspected to be associated with money laundering.

Policy

The provisions of the Law have been adopted by the Company, which introduces procedures and processes that ensure compliance with the Law and Directives and in line with the latest EU 5th AML Directive on this matter.

Company's AML Policy sets out the general measures which will apply to all clients such as:

- check the identity of the Client
- Verify the Client
- monitor any suspicious Client activities and/or transactions
- have a record of all the related information and/or documents of the Client's financial transactions

Restricted Business and Jurisdictions

Our Company does not provide services to clients that their activities are associated with any high risk or banned activities.

Furthermore, the Company endorses and complies with the latest FATF recommendations, as well as the latest, always, classifications of high-risk countries.

In addition, the Company takes into consideration sanctions list of the following bodies:

- EU Sanction List
- United Nations Security Council Consolidated List

B. KYC PROCEDURE

Client Identification and Due Diligence Procedures

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

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

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

The Company has adopted all requirements of the Law in relation to client identification and due diligence procedures. The client identification and due diligence are as follows:

- *Client Due Diligence Procedure*

Client Due Diligence procedure shall comprise the following:

- i. Identification of the client and verification of the client's identity on the basis of information obtained from a reliable and independent source. This is KYC procedure, which is explained in detail further below.
- ii. Identification of the beneficial owner and taking risk-based and adequate measures to verify his/her identity on the basis of documents, data or information issued by or received from a reliable and independent source. As regards to legal persons, trusts and similar legal entities, taking risk-based and adequate measures to understand the ownership and control structure of the client.
- iii. Obtaining information on the purpose and intended nature of the business relationship.
- iv. Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the data and information held by the firm in connection with the client.

The KYC procedure is a requirement in order to comply with the International law provisions, including the ones designed to prevent money laundering. The following procedure should be followed unless an amendment is sent from the Compliance Department stating otherwise.

When a client applies to open an account with us Client will be asked but not limited to provide:

- **Natural Persons** – (this also applies to natural persons involved in a legal entity such as Directors, Shareholders or authorized persons)
 1. Proof of Identity (POI)
 2. Proof of Residence (POR)
 3. Proof of Signature
 4. Proof of Bank Account Ownership
- **Corporate Accounts**
 1. Certificate of incorporation or equivalent
 2. Certificate of registered office or equivalent
 3. Certificate of directors and secretary or equivalent
 4. Certificate of shareholders or equivalent
 5. Memorandum and articles of association of the legal person
 6. Recent copy (up to three months) of a bank statement or utility bill in order to verify the head office address
 7. Identity of Directors and Shareholders with their relevant KYC documents required of Natural Persons
 8. Authorized person resolution signed by the Board of directors ('BoD')

The company's documentation must be recent (maximum 1 year).

The Company reserves the right to request additional documentation until it satisfies its due diligence.

Our Company does not accept legal clients where the shares are issued in a form of "Bear Shares".

Recordkeeping

Assessment of client documents will be made on an annual basis. All client's documents and record transactions will be kept safely and back-up for a minimum five (5) year period.

Enhanced Client Due Diligence

The Company should apply enhanced client due diligence measures in situations which by nature can present high risk of money laundering or terrorist financing. Relevant list, which is updated whenever is applicable per the relevant publications is listed above.

Also the company applies enhanced due diligence on Politically exposed persons ("PEPs") who are individuals that have or been entrusted with prominent public functions in a foreign country and close associate is someone with a close relationship with the political exposed persons.

- **Client Risk Assessment**

Each Client who wishes to receive our services to exchange fiat to digital currency or the opposite shall be assigned to one out of following three categories:

Low Risk (Level I)

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk.

Medium Risk (Level II)

Customers that are likely to pose a higher than average risk to the exchange may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

High Risk (Level III)

The Company will apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. The examples of customers requiring higher due diligence may include:

- High Net worth individuals
- Trusts, charities, NGOs and organizations receiving donations,
- Companies having close family shareholding or beneficial ownership
- Firms with 'sleeping partners'
- Politically Exposed Persons (PEPs) Those with dubious reputation as per public information available, etc.

The criteria used for risk assessment for this category are:

- Risk from the country of origin
 - Can be determine as per the geographical risk, i.e. risk from country of origin. The evaluation of the risk from country of origin is performed according to the following:
 - For natural persons: The residence country
 - For legal entities: The country in which is the legal entity's seat.

When referring to high risk countries, it refers to countries with high corruption index, unsecure economical and political systems, inefficient legal system or small number of requirements for the documentation needed for opening businesses, countries known for production, processing and trafficking drugs and weapons.

As additional factors that would influence the decision whether some country represents a risk, could be:

- States under sanctions, embargos or similar measures, issued, for example, from the United Nations
- States identified, by credibility sources, as states having incompatible regulation for prevention of money laundering and financing terrorism with the international regulation from this area,
- States identified, by credibility sources, as states financing and supporting terrorism

Senior Management approval must be sought before establishing a relationship with such a person. It is also a requirement to establish the high risk client's source of wealth/source of funds and the beneficial owners.

- **Source of Funds**

For High Risk clients, whether these are legal entities or individuals, the Company further to the enhance due diligence as per the previous section, will apply the request of additional documentation (whatever applicable) in order to identify the source of funds.

These may include, but not limited to.

Individual clients:

- Curriculum Vitae ("CV")
- Bank Statements of last six months
- Previous year/s Tax reports
- Tax payment
- Etc

For Legal Entities

- Audited Financial Statements – for newly formed companies, latest management accounts
- Bank Statements of last six months

Establishing the purpose and actual substance of a Transaction

For the purpose of preventing movement of illegally obtained funds through the Provider of service it is essential upon entering into a Business Relationship, in addition to identification of the Client, to establish the business profile of the Client, which consists of mapping the main areas of operation and possible payment practices. Notice is to be taken on persons that the Client has transactional relationships with, and their location.

It is necessary to bear in mind that certain circumstances, which are suspicious or unusual for one Client, could constitute a part of normal economic activities of another. Establishing the area of activity, work or profession of a client allows assessing whether or not the Business Relationship or the Transactions are in conformity with the Client's normal participation in commerce, and whether the Business Relationship or the Transaction has an understandable economic reason for the Client.

Implementation of International Sanctions

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

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

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

Transfer of funds

General Practice

When transferring money for purchasing digital currency, the sender's name and the information held on file provided by the Client upon the agreement, should match.

Money transfers from another party other than the account holder is strictly prohibited. Furthermore, we will refuse any third-party transfers towards one of our Clients.

In case there is any discrepancy on a transaction, we reserve the right to automatically cancel or suspend the transaction. Further to this, third parties are forbidden to conduct the transaction in replace of the Client.

Likewise, the information about transferring digital currency for sale, the recipient's name and the account holder has to be the same. Transferring through the online payment system is allowed ONLY at the same account and/or wallet from where it was first used.

1. Credit Card transactions

To ensure that the owner of the account matches the cardholder, we ask that the client sends to us a clear coloured copy of the card. For security reasons, we ask that the 8 middle digits of the card number used for the transaction for all amounts are covered. We ask that the credit card is a valid credit card where the name of the card holder is shown.

Not card will be accepted where it does not bear a name of the owner. Such example is a prepaid card or internet card. In such cases the money will be rejected and send back to the sender.

2. Wire Transfers

When client is making a wire transfer, he is requested to provide the company with proof of the wire transfer for 2 reasons:

- a. To eliminate any possibility of errors such as wrong client
- b. To be alerted for incoming funds

Important Notes

- Have the Senior Management approval prior of opening a "Political Exposed Person" account.
- When a PEP is a potential client we need to obtain a bank reference letter.
- Where the documents are not in English:
 - We need translation from a translator (external and/or an employee of the Company).
 - If there is no one to translate the documents, we ask the client to send us an official translation from a notary.

NV Poland SPÓŁKA Z OGRANICZONĄ has the right to refuse any client without giving reason.

These guidelines have been implemented to protect NV Poland SPÓŁKA Z OGRANICZONĄ and its clients.