CryptoBridge

AML/CFT POLICY AND PROCEDURES

This Anti-Money Laundering and Combating the Financing of Terrorism Policy ("AML/CFT Policy") has been adopted by us to prevent the use of services for money laundering and terrorist financing activities. We are committed to complying with all applicable laws, regulations, and guidance regarding AML and CFT as defined below.

AML/CFT Policy intends to protect Company from being used as a tool for illegal activities such as money laundering or terrorist financing. AML/CFT Policy sets out specific procedures to achieve this goal, including the implementation of robust client identification process, ongoing Transaction Monitoring to detect Suspicious Activity.

By using our services via our Website, crypto exchanges or otherwise, or by using our Website by our customer, he/she/it expressly agrees with AML/CFT Policy.

Cryptobridge Spółka z Ograniczoną Odpowiedzialnością (the "Company"), registered in Poland under KRS No. 0001058371, NIP 7011164795, REGON 526399029, with its registered office (adres siedziby) at Hoża 86 / 210, 00-682 Warsaw, Poland, is committed to meeting all applicable Anti-Money Laundering and Counter-Terrorist Financing ("AML/CFT") requirements and to maintaining effective controls to prevent the misuse of its services for money laundering, terrorist financing, and other financial crime.

1. Main Objectives.
    a. Company's main objectives establishing AML policy are:
        i. Clients' identities are satisfactorily verified in accordance with the firm's risk based approach before Website does business with them;
        ii. Website knows its clients and understands their reasons for doing business with us both at the client acceptance stage and throughout the business relationship;
        iii. Our staff are trained and made aware of both their personal legal obligations and the legal obligations of Website;
        iv. Our staff is trained to be vigilant for activities where there are reasonable grounds for suspicion that money laundering could be taking place and to make the reports to the Compliance Officer
        v. Sufficient records are kept for the required period;
        vi. We establish, maintain and implement appropriate procedures to achieve these objectives;
2. Definitions
    a. AML Act – the Polish Act of 1 March 2018 on Counteracting Money Laundering and Financing of Terrorism, as amended, together with its implementing regulations and applicable guidance
    b. KYC - Know Your Customer
    c. MiCA - Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets
    d. ML-FT - Money Laundering and Financing of Terrorism
    e. "Company" or "We" – Cryptobridge Spółka z Ograniczoną Odpowiedzialnością, registered in Poland under KRS No. 0001058371, NIP 7011164795, REGON 526399029, with its registered office at Hoża 86 / 210, 00-682 Warsaw, Poland, providing services in line with applicable Polish AML/CFT laws and, where relevant, applicable EU regulations relating to crypto-assets and virtual asset services
    f. Politically exposed person. A politically exposed person means a natural person who is or has been in a significant public office of national or regional importance, such as, in particular, a head of state, the head of the government, the head of a central government body and his deputy (deputy, secretary of state), a member of parliament, a member of the governing body of a political party, a leader of a local authority, a judge of the supreme court, constitutional court or other supreme judicial body, against

whose decision, generally with exceptions, no appeal may be lodged, a member of the board of a central bank, a senior officer of the armed forces or a corps, a member or representative of a member, if a legal entity, of the statutory body of a State-controlled commercial corporation, an ambassador or head of a diplomatic mission, or a natural person who holds or has held a similar office in another State, in a body of the European Union or an international organisation.

g. Virtual asset:
    i. crypto-assets under MiCA and
    ii. a crypto-asset that is unique, not fungible with another crypto-asset and cannot be used for payment or investment.
h. Virtual asset services:
    i. providing custody and administration of crypto-assets on behalf of clients;
    ii. operation of a trading platform for crypto-assets;
    iii. exchange of crypto-assets for funds;
    iv. exchange of crypto-assets for other crypto-assets;
    v. execution of orders for crypto-assets on behalf of clients;
    vi. placing of crypto-assets;
    vii. reception and transmission of orders for crypto-assets on behalf of clients;
    viii. providing portfolio management on crypto-assets;
    ix. providing transfer services for crypto-assets on behalf of clients.
    x. The Company provides or intends to provide virtual asset services in accordance with applicable European Union regulations, including Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), and applicable Polish implementing legislation. The Company limits its activities to the scope of services permitted under applicable law and, where required, under the authorisations, registrations, or licences obtained or to be obtained from the competent authorities.

3. General Principles
    a. We have implemented policies, procedures and controls designed to prevent criminals from using Website to launder the proceeds of crime. These policies and procedures are tailored to the risk posed to individual customers.
    b. The Company has established customer due diligence procedures to identify the users of its services and, in respect of higher risk customers, the primary beneficial owners and origin of funds. These procedures include knowledge of the nature of our

customers' business and vigilance for anomalous transactions.

c. The initial customer identification and due diligence are activities designed to fulfil the KYC principle. Based on an adequately conducted CDD, the Company understands the ML-FT risk its customers pose.
d. Customer identification. Full name and contact information: verification of the customer's identity through reliable documents.
e. Risk assessment
    i. Country of origin: assessing the inherent risk associated with the customer's country of origin, including whether it is classified as a high-risk jurisdiction.
    ii. Politically Exposed Persons (PEPs): determining if the customer is a PEP and, if so, investigating their wealth source. The Company may determine whether a customer or a beneficial owner is a politically exposed person based on information provided by the customer, including declarations made under criminal liability for false statements, information obtained from reliable public or commercial databases, and other reasonable measures applied in accordance with the Polish AML Act and a risk-based approach.
    iii. Sanctions compliance: confirming that the customer is not subject to any international sanctions.
f. Ownership and Control Structure:
    i. Structure: outlining the customer's ownership and control structure, identifying key individuals and entities involved.
    ii. Beneficial ownership: identification of the ultimate beneficial owner(s) of the customer and verifies their identity and PEP status.
    iii. Sanctions screening: checking whether the customer, the beneficial owner(s), and any persons within the customer’s ownership or control structure (including authorised representatives and key managers, where applicable) are subject to applicable international sanctions, including EU and UN sanctions regimes (and any other sanctions applicable to the Company under Polish and EU law).
g. Business purpose and source of funds
    i. Reason for engaging with the Company: the customer's intended purpose for using virtual asset services is clearly understood.
    ii. Source of funds: verifying the legitimate source of funds involved in any potential transactions or business relationships.

iii. Transaction profile: outlining the anticipated volume, nature, and geographical scope of transactions with the customer.

h. Customer background
   i. Business activities and income: gathering information about the customer's business activities, income sources, and geographical reach.
   ii. Existing relationship with the Company: if applicable, the Company reviews the customer's past transactions and business relationship with the Company.

i. Verification and credibility
   i. Information sources: information is collected from the customer and other reliable sources, such as public registries and official documents.
   ii. Risk-based due diligence: the level of due diligence required for each piece of information is proportional to the assessed risk of the customer and transaction.
   iii. Source credibility: multiple independent sources are used to corroborate information, especially when relying on less credible sources like affidavits.

j. This list represents a general overview of KYC requirements and may not be exhaustive. Specific requirements may vary depending on the individual customer and the nature of the proposed transaction or business relationship.

4. Risk factors

A risk factor is any characteristic of the customer, the virtual asset services provided to them, or how services are provided, increasing the likelihood of virtual asset services being misused for money laundering and terrorist financing.

5. Categorisation of the customer risk profile

The customer risk profile is a customer assessment that represents the potential risk that the customer may misuse virtual asset services for ML-FT purposes. As part of the risk profile, customers are classified into the following groups according to the risk factors they have experienced:

a. A customer with “Low risk” profile - i.e. the customer poses a low risk: no risk factors have been identified concerning the customer, or factors that pose negligible risk about the identified risk factors and can be tolerated.

b. A customer with “Medium risk” profile - i.e. the customer poses a medium risk: risk

factors have been identified to the customer, which is general, but these factors cannot be tolerated; therefore, the customer cannot be unambiguously classified as category "Low risk", but, on the other hand, the customer cannot be considered high risk either.

c. A customer with a “High risk” profile - i.e. the customer poses a high risk: risk factors have been identified to the customer that pose a higher risk and require enhanced measures to eliminate these risks;

d. A customer with “Reject risk” profile - i.e. an unacceptable customer: risk factors have been identified to the customer that represents an extremely high risk, and such customer will not be provided with virtual asset services or, if applicable, services will be terminated. Such Reject risk profile is assigned to customers who have any risk factor that requires EDD and the customer has not provided sufficient information and documentation to address the identified risk factors or red flags, as well as when, for example:

   i. the customer's country(ies) of origin is(are) categorised as "blacklist" according to Annexe No. 5 of the *Know Your Customer (KYC) and Customer Due Diligence (CDD) Procedures* document;

   ii. the customer's activity is categorised as "rejected" according to Annexe No. 6 of the *Know Your Customer (KYC) and Customer Due Diligence (CDD) Procedures* document;

   iii. no identification or CDD has been performed against the customer;

   iv. a reasonable suspicion arises that the purpose of the transaction or business relationship is to provide virtual asset services to a person other than himself (i.e. the customer is merely acting as an intermediary or identity provider, a so-called "nominal person") and the customer does not refute this suspicion;

   v. the customer, a person in the customer’s ownership or control structure (member of the statutory body/management board, beneficial owner, etc.), or an authorised representative is subject to applicable international sanctions (including EU and UN sanctions regimes, and any other sanctions applicable under Polish and EU law), or the transaction would result in a breach of sanctions obligations; in such case the Company will refuse onboarding, reject the transaction, and/or terminate the business relationship as required, and where applicable will take reporting or other actions in accordance with the requirements of the competent authorities, including the Polish Financial

Intelligence Unit (GIIF), and the Company's internal escalation and decision-making procedures;

vi. the customer's or beneficial owner's source of funds or source of wealth is suspicious;

vii. the information provided by the customer about him/herself and his/her activities is grossly inconsistent with the facts established from reliable sources, and the customer has not justified the inconsistency;

viii. there is a reasonable suspicion that the customer provides false, distorted or incomplete information or submits false or altered documents during the business relationship;

ix. the transaction or business relationship with this customer has already been terminated in the past at the Company's initiative, and the customer is making repeated attempts to re-establish it and the factors that caused the refusal to provide the service have not been eliminated;

x. the customer, a person in the control or ownership structure (member of the statutory body, beneficial owner, etc.) is connected to another customer with whom the transaction or business relationship has been terminated in the past on the Company's initiative;

xi. the customer otherwise poses a significant risk to the company from the perspective of ML-FT;

xii. any of the factors listed above if it occurs in a legal entity in which the customer has a direct or indirect interest or is otherwise in a position to exercise influence.

The Company has developed a system for assessing the risks of the customer and the virtual asset services provided to determine the customer risk profile using the Risk Assessment questionnaire.

6. Primary determination of customer risk profile

a. The type and increase of identification and due diligence measures to be applied to a customer during onboarding are determined based on the customer's primary risk profile. In the course of obtaining or confirming information, screening for PEPs and sanctions, and as a result of other measures, the customer's risk profile may change. However, even initial measures should be based on the specific risk factors identified

for the customer to apply the risk-based approach correctly.

b. For these purposes, the company has identified the factors by which the customer's risk tolerance is initially assessed, namely, the customer's country of origin, activity, and planned turnover.

c. The qualities of these factors correlate with customer categorisation as follows:

   i. A customer is categorised to the “Low risk” profile if meets one of the characteristic options:

      1. The customer has the following characteristics: the customer's country(ies) of origin is(are) categorised as "Low risk" and the customer's activity is categorised as "Low risk" and the customer's planned turnover does not exceed EUR 5 000 per month for natural persons, for legal persons EUR 15 000 per month.

      2. The customer has the following characteristics: the customer's country(ies) of origin is(are) categorised as "Low risk" and the customer's activity is categorised as "Medium risk" and the customer's planned turnover does not exceed EUR 5 000 per month for natural persons, for legal persons EUR 15 000 per month

      3. The customer has the following characteristics: the customer's country(ies) of origin is(are) categorised as "Medium risk" and the customer's activity is categorised as "Low risk" and the customer's planned turnover does not exceed EUR 5 000 per month for natural persons, for legal persons EUR 15 000 per month there are no known factors under which it is necessary to take EDD measures concerning the customer.

   ii. A customer is categorised to the “Medium risk” profile if meets one of the characteristic:

      1. The customer has the following characteristics: the customer's country(ies) of origin is(are) categorised as "Low risk" or "Medium risk" and the customer's activity is categorised as "Low risk" or "Medium risk" and the customer's planned turnover does not exceed EUR 15 000 per month for natural persons, for legal persons EUR 25 000 per month.

      2. The customer has the following characteristics: the customer's

country(ies) of origin is(are) categorised as "Medium risk" and the customer's activity is categorised as "Medium risk" and the customer's planned turnover does not exceed EUR 5 000 per month for natural persons, for legal persons EUR 15 000 per month and

3. There are no known factors under which it is necessary to take EDD measures concerning the customer.

iii. A customer is categorised to the “High risk” profile if meets one of the characteristic: the customer's country(ies) of origin is(are) categorised as "high risk", or the customer's activity is categorised as "High risk" or the customer's planned turnover exceeds: EUR 100 000 per month and the customer is a natural person, or EUR 250 000 per month and the customer is a legal entity.

iv. A customer is categorised to the "Reject" risk profile if:

a) the customer's country(ies) of origin is(are) categorised as "Blacklist", or

b) the customer's activity is categorised as "Blacklist".

7. CDD during the business relationship

a. Regular CDD. The purpose of the regular CDD is ongoing monitoring and verification that the information provided is up-to-date and consistent with what the Company knows about the customer and virtual asset services provided..

b. Operational CDD. The purpose of the regular CDD is ongoing monitoring and verification that the information provided is up-to-date and consistent with what the Company knows about the customer and the service provided. Operational CDD is used in the following circumstances, each involving different procedures, depending on the relevance of the customer data already available.

8. Ongoing monitoring of transactions

a. Company recognizes the importance of Ongoing Monitoring to ensure that customers do not pose a risk of money laundering or terrorist financing. Therefore, it conducts Ongoing Monitoring of customers to ensure that their activities do not change and become a higher risk. This includes Transaction Monitoring for Suspicious Activity, reviewing a customer’s information for any changes, and conducting additional Due Diligence when necessary.

b. Overall, Company's Due diligence process and ongoing monitoring are essential tools for identifying and managing the risks associated with its external relationships and for ensuring that it is complying with applicable laws and regulations related to AML and CFT.

c. Ongoing Monitoring of the customer's business relationships, including:

   i. analysis of transactions carried out within the framework of the business relationship to ensure that these transactions are consistent with our knowledge of the customer, the type and scope of its business, and consistent with the money laundering and terrorist financing risks associated with that customer;

   ii. investigation of Source of Funds, Source of Wealth, assets, funds at the disposal of the customer - in cases justified by the circumstances;

   iii. ensuring that the documents, data or information in its possession regarding business relations are kept up to date.

9. Sanctions screening

   a. Company has a responsibility to ensure that it is not doing business with individuals and legal entities that are prohibited by sanctions laws. To achieve this, Company implements procedures to screen all customers against Sanctions Lists. This will include checking the names of individuals and legal entities against lists of individuals and legal entities that have been designated by government agencies, international organizations as being subject to sanctions, embargoes, or other restrictions on trade or financial transactions.

   b. Company also screens transactions to ensure that they do not involve prohibited individuals or legal entities. This will involve reviewing transaction details, such as the names of parties involved, the amounts, and the location of the transaction, to ensure that they are not connected to any individual or legal entity that is subject to sanctions.

   c. Additionally, Company has procedures in place to investigate and report any potential sanctions violations to the appropriate authorities.

10. Risk Assessment

   a. Company conducts a comprehensive risk assessment of the relationships with customers to identify and evaluate any potential risks. This risk assessment considers a range of factors, including the nature of the relationship, the services provided, the location of the customer, and the customer's industry or sector.

   b. Based on the results of the risk assessment, Company takes appropriate measures to

mitigate any risks identified.

c. Additionally, the Company implements a risk-based approach for its AML/CFT compliance program.

d. Company may provide services to customers who/which have a connection with foreign jurisdictions. In assessing the risk associated with a jurisdiction to which a customer is connected, Company takes account of the following classifications:

   i. Financial Action Task Force (FATF) member countries;

   ii. non-FATF countries whose regimes are not subject to sanctions imposed by the UNSC and are not otherwise deemed as high-risk jurisdictions or prescribed foreign countries below;

   iii. countries with AML/CTF deficiencies, serious organized crime, political instability, corruption and weak rule of law;

   iv. countries subject to UNSC sanctions.

11. Reporting Suspicious Activity

   i. Company recognizes the importance of having a process in place to report any suspicious activities or transactions that indicate money laundering or terrorist financing.

   ii. Reports of suspicious activities will be reviewed and investigated by Company's AML/CFT Compliance Officer, which will be responsible for determining whether the reported activity is indicative of money laundering or terrorist financing. If it is determined that the reported activity is suspicious, AML/CFT Compliance Officer will take the necessary steps to report the Suspicious Activity to the appropriate authorities.

12. Third-Party Service Providers

a. Company takes steps to ensure that Third-Party Service Providers comply with its AML/CFT regulatory requirements. This will involve conducting thorough Due Diligence on these providers, reviewing their reputation and past behavior, and evaluating their own AML and CFT policies and procedures. To ensure Sanctions compliance, Company could include specific provisions related to AML and CFT in agreements with Third-Party Service Providers. Additionally, Company conducts regular monitoring of these providers to confirm they are adhering to the AML and CFT requirements set forth in the contract.

13. Suspicious Activity

a. Signs of suspicious activity

i. A suspicious activity means a virtual asset service (whether within a business relationship or outside a business relationship) carried out in the circumstances giving rise to a suspicion of an attempt to launder the proceeds of crime or a suspicion that the funds used in the service are intended to finance terrorism, or that the service is otherwise related to or connected with the financing of terrorism, or any other fact that might indicate such a suspicion.

ii. A suspicious activity may also be an act by a customer that is not directly related to the provision of the virtual asset service but gives rise to a reasonable suspicion that the customer's interest may be in the aforementioned fraudulent activity. Suspicious activity may also include the virtual asset service that the Company does not perform or a mere attempt by the customer to conduct a transaction or establish a business relationship.

14. Prohibition to provide virtual asset services

a. We refuse to provide the customer with virtual asses services within or outside the business relationship if:

i. the customer does not provide the necessary cooperation in the initial CDD and initial identification - i.e. does not provide the requested information or does not support it with the relevant documents (if required); or

ii. the customer was identified remotely, and the first payment from the business relationship could not be made to an account in the customer's name (see paragraph Remote identification of the Know Your Customer (KYC) and Customer Due Diligence (CDD) Procedures document); or

iii. doubts arise as to the accuracy or completeness of the information provided by the customer in the course of the initial identification or initial CDD; or

iv. there are reasonable suspicions that the customer has provided false, distorted or incomplete information or that the customer has submitted false, altered or unreliable documents; or

v. for any other reason, it is not possible to carry out the initial identification or initial CDD; or

vi. it is apparent to the customer that the purpose of the intended transaction or business relationship is to provide virtual asset services to a person other than the customer (i.e. acting only as an intermediary or identity provider), and the customer does not provide an adequate justification (e.g. power of attorney) to that effect; or

vii. the customer is subject to EDD, and the Governing Body has not approved the provision of virtual asset services;

viii. the customer is a PEP, and its source of funds is unknown;

ix. the customer is assigned a risk profile of Reject according to the risk assessment.

x. If any of the cases listed above occur, the Account Manager or AML Specialist immediately reports this to the Head of the AML who ensures that the requested virtual asset services aren't provided to this customer and that the business relationship with the customer is terminated (factually and legally), if applicable.

b. We may also determine for individual types of customers other circumstances in which the requested virtual asset services will not be provided.

15. Specific restrictive measures

a. Customers' Transaction Monitoring and analysis of the received data is one of the tools for assessing the risk and detecting suspicious transactions. In case of suspicion of money laundering or terrorist financing, Company controls all transactions and reserves the right to:

i. suspend or terminate the customer's access to account registered at Website;

ii. suspend providing services and freeze, block assets, funds until the circumstances are clarified;

iii. return the customer's assets, funds by canceling the order, instruction;

iv. take other actions allowed by Act, Company's internal policies and procedures.

16. Geo-Blocking and Jurisdictional Access Restrictions

a. The Company may employ geo-blocking or other technical access-restriction measures to limit or prevent access to its platform, website, and mobile applications from certain jurisdictions where the provision of services would expose the Company to regulatory, legal, compliance, or operational risks.

b. As part of its Know Your Customer (KYC) and Anti-Money Laundering (AML) processes, the Company may implement controls to identify and restrict customers connected with restricted jurisdictions. Such controls may include, but are not limited to:

i. Rejecting account registrations where the customer provides a residential address, place of establishment, or identification documents associated with a

restricted jurisdiction.

ii. Restricting or blocking the use of payment methods, including bank accounts and credit or debit cards, issued or maintained in restricted jurisdictions.

iii. Conducting ongoing monitoring to detect and prevent customers connected with restricted jurisdictions from accessing or using the Company's services.

iv. Prohibition of Financial Promotions to UK Customers

c. The Company ensures that no financial promotions, marketing materials, or communications are directed at individuals or entities located in, resident in, or otherwise connected with restricted jurisdictions. This includes refraining from advertising, soliciting, or engaging in any activity that could reasonably be construed as targeting customers in such jurisdictions.

17. Conclusion

a. Company is committed to complying with all applicable laws and regulations related to AML and CFT in its external relationships. By implementing this AML/CFT Policy, Company aims to prevent its services from being used for money laundering or terrorist financing activities. Company will review and update this AML/CFT Policy regularly to ensure that it remains effective in addressing the risks of money laundering and terrorist financing.

b. Company is required to document the financial security measures in place. Records are kept for a period of 5 years from the date of termination of business relations with the customer or from the date of the occasional transaction, unless a longer retention period is required by applicable law or by a competent authority in connection with ongoing proceedings, audits, or investigations. Documents are stored in a manner that ensures their integrity, confidentiality, availability, and security, and in accordance with applicable data protection requirements.

c. Communication with a customer may take the form of telephone or video conference discussions and email correspondence.