CRYPTOWALLET AML POLICY

ESTX SPÓLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA (also: Estx sp. z o.o.)is a company incorporated in Poland with company registration number 0001039709 and a registered address at Romana Dmowskiego 3 / 9, 50-203 Wrocław, Polska (hereinafter referred to as “Company” or “CryptoWallet”). Company is aware of its corporate duty to assist the fight against anti-money laundering, corruption and against the funding of terrorism.

1. GENERAL TERMS

1.1. VERSION CONTROL

Version	Creation date	Author	Reviewed by	Approved by	Date
V1	01.02.2024	Legal department	AML department	MLRO	01.04.2024

1.2. **POLICY SCOPE**

1.2.1. This policy applies to all employees, officers, directors, contractors, and agents of CryptoWallet. It establishes the framework and guidelines for preventing and detecting money laundering and terrorist financing activities within CryptoWallet's operations.

1.2.2. Security measures within the meaning of this code of conduct are remedies used in economic activities by Company to:

1.2.2.1. define the party to a transaction or an operation;

1.2.2.2. achieve necessary due diligence in turnover;

1.2.2.3. avoid fraud, mistakes or other abuse;

1.2.2.4. appropriately fulfil any obligations laid down in law or other regulations.

1.3. **REGULATORY FRAMEWORK**

1.3.1. This AML policy is designed to comply with all relevant laws, regulations, and guidelines pertaining to anti-money laundering and counter-terrorist financing, including but not limited to:

1.3.2. Polish Money Laundering and Terrorist Financing Prevention Act https://mf-arch2.mf.gov.pl/documents/764034/1010418/ustawa+tekst_EN+_15062018-f+_16072018.pdf

1.3.3. 6th EU Anti-Money Laundering Directive 2018/1673 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1673

1.3.4. The Financial Action Task Force (FATF) Recommendations https://www.fatf-gafi.org/en/topics/fatf-recommendations.html

1.4. **BUSINESS CORE DETAILS**

1.4.1. Estx sp. z o.o. is a registered virtual assets service provider by the Polish Tax Administration, authorized to provide virtual currency services (Authorisation No. RDWW-1134 – VASP registy: https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych)

1.4.2. CryptoWallet offers a range of products and services in the cryptocurrency industry. These include a cryptocurrency exchange platform, digital wallet solutions, and crypto prepaid card solutions. CryptoWallet caters to individuals and businesses looking to explore cryptocurrencies and blockchain technology. Loading methods encompass fiat-to-crypto and crypto-to-crypto, crypto-to-fiat transactions. While CryptoWallet is primarily operating from Poland, it has the legal capacity to onboard clients from other countries, free from any limitations imposed by EU or Poland regulations.

1.5. **DEFINITIONS**

1.5.1. Money laundering means the concealment of the true nature, origin, location, manner of disposal, relocation or right of ownership of property acquired as a result of a criminal activity or property acquired instead of such property or the concealment of other rights related to such property; conversion, transfer, acquisition, possession or use of property derived from criminal activity or property obtained instead of such property for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person’s actions. Money laundering is regarded as such also where a criminal activity which generated the property to be laundered was carried out in the territory of another country.

1.5.2. Terrorist financing means the allocation or collection of funds to plan or commit terrorist acts within the meaning of the Penal Code or finance terrorist associations or knowing that these funds will be used for the purpose.

1.5.3. Politically exposed person means a natural person who performs or has performed prominent public functions, also the family members and persons known to be close associates of such a person. A person who has not performed prominent public functions for at least one year prior to the date of the transaction is not to be deemed a politically exposed person, nor the family members and persons known to be close associates of such person. For the identification of a politically exposed person, public search systems, national and international public databases of politically exposed persons and technical solutions offered by service providers are used. Persons performing prominent public functions within the meaning of this guide of conduct are:

1.5.3.1. head of State or head of government, minister, deputy minister or assistant minister;

1.5.3.2. member of a legislative body;

1.5.3.3. a justice of a supreme court, constitutional court or another court the judgments of which can be appealed against only in exceptional circumstances;

1.5.3.4. a member of the supervisory board of a state audit institution or central bank;

1.5.3.5. ambassador, chargé d'affaires and high-ranking officer;

1.5.3.6. a member of a directing, supervisory or administrative body of a state company. The term includes positions in the European Union and other international companies.

1.5.3.7. A family member of a person performing prominent public functions:

1.5.3.8. their spouse;

1.5.3.9. a partner equal to a spouse under the law of the person's country of residence or a person who as of the date of carrying out the transaction had shared the household with the person for no less than a year;

1.5.3.10. their children and their spouses or partners;

1.5.3.11. their parents;

1.5.3.12. A close associate of a person performing prominent public functions is:

1.5.3.13. a natural person who has a close business relationship with a person performing prominent public functions or with whom a person performing prominent public functions is the joint beneficial owner of a legal person or contractual legal arrangement;

1.5.3.14. a person who as a beneficial owner has full ownership of a legal person or contractual legal arrangement, which is known to have been founded for the benefit of the person performing prominent public functions.

1.5.4. International financial sanction means a financial sanction that fully or partially prevents the subject of an international financial sanction using and disposing of financial means and economic resources or giving thereof to its possession.

1.5.5. Subject to international sanction means a natural or legal person, an authority, a civil law partnership or any other entity which is directly specified in the act on the imposition or implementation of international sanctions and with regard to whom the measures prescribed therein are taken.

1.5.6. Money Laundering and Terrorist Financing Prevention Act regulates the activities of credit and financial institutions and other undertakings and institutions stipulated in the Money Laundering and Terrorist Financing Prevention Act, as well as the activities of the Financial Intelligence Unit in preventing money laundering and terrorist financing.

1.5.7. Money Laundering Officer is an employee appointed by the decision of the management board of the undertaking who is the MLRO with the Financial Intelligence Unit and ensures the implementation of the measures established to prevent money laundering and terrorist financing in the institution. The MLRO appointed by the board is Aleksei Arno.

1.5.8. Senior Manager/Responsible person is an employee appointed by the decision of the management board of the undertaking who is the responsible person with the Financial Intelligence Unit and ensures that the institution that appointed them fulfils the requirements of the International Sanctions Act. The responsible person appointed by the board is Aleksei Arno.

1.5.9. Client is a person who uses or has used a single service or multiple services provided by the institution based on a contract concluded by CryptoWallet.

2. SENIOR MANAGEMENT AND RESPONSIBLE PERSON

2.1. Within CryptoWallet, it is the duty and authority of senior management to appoint a designated individual to assume the role of the Responsible Person/Senior Manager. The Responsible Person is bestowed with explicit duties and responsibilities concerning the proficient and effective administration of CryptoWallet's operations. The responsible person appointed by the Senior Management and board is Aleksandr Smirnin.

2.2. The duties of the Senior Manager/Responsible Person are:

2.2.1. prepare a formal policy statement that outlines CryptoWallet's commitment to the prevention and risk assessment of money laundering and terrorist financing activities;

2.2.2. check the client if the amount of the transaction exceeds 50,000 euros and if there are changes in the management bodies, owners, or representatives. If the client is a legal body, their representative, members of management bodies and actual beneficiaries must be checked;

2.2.3. check the entire client base and automated monitoring systems at least once a month.

2.2.4. In accordance with the International Sanctions Act, the responsible person collects and preserves for five years the following information:

2.2.4.1. inspection time;

2.2.4.2. the name of the inspecting person;

2.2.4.3. results of the inspection;

2.2.4.4. measures taken.

2.2.5. If there is a doubt whether a person with whom Company is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, is the subject of international financial sanction, additional, information must be requested from the respective person to determine whether these suspicions are correct.

2.2.6. If a person with whom Company is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, refuses to provide additional information or it is impossible to identify by means thereof if the person is a subject of international financial sanction, the person having specific obligations or a person authorized by them refuses to make a transaction or operation, takes measures provided for in the act on the imposition or implementation of international financial sanction and notifies immediately the Financial Intelligence Unit and the management board of Company of their doubts and of the measures taken.

2.2.7. If the activity of a person does not fully qualify as an activity that must be reported to the Financial Intelligence Unit, according to these instructions, the client’s further activity must be taken under increased attention. The Financial Intelligence Unit must be notified as soon as there is a reasonable suspicion of suspicious behaviour by the client.

3. MONEY LAUNDERING REPORTING OFFICER

3.1. The Senior Management is responsible to appoint a designated individual to serve as the Money Laundering Reporting Officer (MLRO). The MLRO is entrusted with specific duties and responsibilities related to the detection and prevention of money laundering activities within CryptoWallet.

3.2. The duties of the Money Laundering Reporting Officer are:

3.2.1. checking compliance with anti-money laundering requirements and regulations;

3.2.2. transferring of information to the Financial Intelligence Unit in case of suspicion of money laundering or terrorist financing or other illicit activity;

3.2.3. responding to requests made by the Financial Intelligence Unit and complying with its orders;

3.2.4. collection of data received on suspicious and/or unusual operations and processing and storage of such data either in a designated electronic file or on paper, in which the details of the suspicious or unusual transaction, data provider, date and place can be seen;

3.2.5. submitting periodic written reports to the management board on compliance with procedural rules;

3.2.6. informing the management board in writing about deficiencies in compliance with internal control regulations, guidelines, and other legislation.

3.2.7. commissioning an annual report and promptly addressing any identified deficiencies outlined in the report.

3.2.8. provide regular updates on system and control performance issues to interested third-party providers if such sharing is not restricted by applicable laws and regulations.

3.3. The rights of the MLRO are:
3.3.1. checking transactions and their formalization in accordance with the legislation
3.3.2. during the provision of the service, monitoring of activities to ensure their compliance with activities to prevent money laundering and terrorist financing.
3.3.3. The MLRO may only transmit information or data that has become known to them in connection with suspected money laundering:
3.3.3.1. to the management board and the employee appointed by the board;
3.3.3.2. Financial Intelligence Unit;
3.3.3.3. to the preliminary investigation authority in connection with criminal proceedings;
3.3.3.4. to the court based on a court order or decision.
3.3.4. Regarding suspicious or unusual transactions, the following information is recorded in a format which can be reproduced in writing:
3.3.4.1. details of a suspicious or unusual transaction;
3.3.4.2. person(s) involved in the transaction;
3.3.4.3. date and location of the transaction.
3.3.5. Notifications prepared by the MLRO are stored, used and preserved analogously to other information in accordance with the provisions of this policy.
3.3.6. CryptoWallet is committed to cooperating with regulatory authorities and supporting the fight against financial crimes, including money laundering and terrorist financing. As part of this commitment,

4. RISK ASSESSMENT OVERVIEW

CryptoWallet is dedicated to conducting comprehensive risk assessments to identify, evaluate, and manage risks associated with its activities and client activities. Set of rules provide an overview of the risk assessment framework to address potential threats, including money laundering, terrorist financing, fraud, cybersecurity, and other risks related to the crypto industry.

4.1. RISKS ARISING FROM THE ACTIVITIES OF CryptoWallet.

4.1.1. CryptoWallet prepares a risk assessment to identify, evaluate and analyses the money laundering and terrorist financing risks associated with its activities, considering at least the following risk categories:
4.1.1.1. client-related risks;
4.1.1.2. risks related to countries or geographic areas or jurisdictions;
4.1.1.3. risks related to products, services or transactions;
4.1.1.4. risks related to the communication or mediation channels between CryptoWallet and clients or the delivery channels for products, services, or transactions.
4.1.2. As a result of the risk assessment, CryptoWallet determines:
4.1.2.1. risk appetite, including the volume and scope of products and services offered in the course of business;
4.1.2.2. risk management model, including enhanced due diligence measures to mitigate identified risks.
4.1.3. Risk appetite is a set of risk levels and risk types that CryptoWallet is willing to take in order to realize its economic activities and strategic goals and which is confirmed in writing by the senior management of CryptoWallet. The implementation of the above must take into account the risks that CryptoWalletis willing to take or that it wants to avoid in relation to its economic activities, as well as qualitative and quantitative compensation mechanisms, such as planned income, measures implemented using capital or other liquid assets, or other circumstances, such as reputational risks and legal and other risks related to money laundering and terrorism financing or other unethical activities.
4.1.4. When applying the risk appetite, CryptoWallet determines as a minimum which person with which characteristics it wants to avoid doing business with and in which cases it applies enhanced due diligence measures, including assessing the risks associated with such persons for CryptoWallet and determining appropriate measures to mitigate these risks.
4.1.5. The risk assessment and determination of the risk profile are documented, and these documents are updated on the basis of necessity and the published results of the national risk assessment. At the request of the competent supervisory authority, CryptoWallet submits the documents prepared on the basis of this section to the supervisory authority.

4.1.6. CryptoWallet should discover that the law of a third country does not allow the application of procedural rules and internal control standards that meet the requirements of the Money Laundering and Terrorist Financing Prevention Act in its representative office, branch, or majority-owned subsidiary, it informs a competent supervisory authority of such circumstances. The competent supervisory authority informs the countries of the client and, if applicable, the European supervisory authorities, if, according to the first sentence of this paragraph, it has become clear that the law of the third country does not allow the group to implement procedural rules and internal control standards that meet the requirements of Directive (EU) 2018/843 of the European Parliament and of the Council. In such cases, CryptoWallet. ensures the implementation of additional measures in the respective representative office, branch, or majority-owned subsidiary, which allow effective management of risks related to money laundering or terrorist financing in other ways and notify the competent supervisory authority of the measures taken. In this event, the competent supervisory authority has the right to demand *inter alia*, by injunction, that CryptoWallet. and the representative office, branch, or majority-owned subsidiary of CryptoWallet. do the following:

4.1.6.1. not establish new business relationships in that country;

4.1.6.2. terminate existing business relationships in that country;

4.1.6.3. suspend the provision of the service partially or completely;

4.1.6.4. cease its activities;

4.1.6.5. implement other measures provided for in the regulatory technical standards established by the European Commission on the basis of Article 45(7) of Directive (EU) 2015/849 of the European Parliament and of the Council.

4.2. CLIENT RISK LEVELS

4.2.1. For the purposes of this policy, clients are classified and categorized based on the Client Risk Assessment Policy, assigning them the following risk levels:

4.2.1.1. low risk clients;

4.2.1.2. moderate risk clients;

4.2.1.3. high-risk clients.

4.2.2. For all clients with low and moderate risk levels, CryptoWallet applies Client Due Diligence when establishing business relationships and in the course of business relationships.

4.2.3. CryptoWallet. may also apply enhanced due diligence to a client with a low and moderate risk level should the behaviour of the client or executed transactions cause doubts about the reliability of the client and the purpose of using the services.

4.2.4. Special attention must be paid to a client with whom CryptoWallet is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, and whose actions and circumstances indicate the indirect possibility that the person is the subject of an international financial sanction.

4.2.5. If the sanction monitoring service provider's initial or ongoing screening identifies any direct association between the client or/and a sanction regime, sanctioned individuals, or sanctioned companies, the client's relationships with CryptoWallet. will be promptly terminated.

4.3. CLIENT DUE DILIGENCE (CDD)

4.3.1. Client due diligence (CDD) is a procedure conducted by CryptoWallet, aimed at confirming the client's personal information and validating their personal identification documents.

4.3.2. CryptoWallet applies the following procedural rules every time before establishing a business relationship and request client to provide the following information:

4.3.2.1. given name and surname;

4.3.2.2. date of birth

4.3.2.3. place of birth;

4.3.2.4. telephone number and email

4.3.2.5. Nationality

4.3.2.6. address of place of residence;

4.3.2.7. document name, number, name of the issuing authority and date of issue

4.3.2.8. clarifies the purpose of the transaction and the nature of the business relationship and profession or activity;

4.3.3. CryptoWallet. will deny an initial and further onboarding and reject conducting relationships:

4.3.3.1. with a person who refuses to provide the data specified in the previous clause, as well as with a person who the employee suspects to be a front;

4.3.3.2. with a person, who does not submit the required documents and relevant information or if the employee suspects, based on the submitted documents, that money laundering or terrorist financing may be involved.

4.3.3.3. with a person, who has confirmed and direct connections with personal sanctions, sanctioned companies or persons, sanctioned regions;

4.3.3.4. with a person, who has confirmed and direct connections with money laundering, terrorism financing or other illicit activities.

4.3.3.5. with a person who does not comply with the age range of 18 to 65 years old

4.3.4. The following documents may be used to identify a natural person (should be valid at least 6 months):

4.3.4.1. a valid national identity card;

4.3.4.2. a valid passport;

4.3.4.3. a valid national residence permit

4.3.5. CryptoWallet. possesses the authority to apply additional verification measures under the following circumstances:

4.3.5.1. To verify the client's identity and meet the prerequisites for establishing a business association.

4.3.5.2. To offer an additional service provided by CryptoWallet..

4.3.5.3. When it is required to comply with contractual obligations between CryptoWallet. and third parties service providers.

4.3.6. CryptoWallet. will request the following documents to comply with 3rd party contractual obligations, governmental authority legal obligation or as additional measure of Customer Due Diligence:

4.3.6.1. Proof of address (e.g., gas, electricity, bank statement, governmental authority issued document) not older than 3 months.

4.3.6.1.1. To utilize the Card Programme service, clients must fulfil a distinct condition by furnishing evidence of their address prior to accessing the service. Failure to do so will result in the unavailability of the service to the client.

4.3.6.2. Source of funds (bank statements, employment contract, loan agreement, property sale agreement) not older than 3 months.

4.3.6.3. Source of wealth (business ownership, employment contract, gift documentation, investment portfolio).

4.3.6.4. Under certain requirements of the Card Programme, clients are mandated to submit Source of Funds and Source of Wealth information if their card transactions, encompassing purchases and ATM withdrawals, surpass 25,000 EUR over a span of 12 months. CryptoWallet. will continually oversee the client's expenditure and will conduct further Source of Funds/Source of Wealth assessments if the previously gathered documentation does not align with the client's present spending patterns.

4.3.7. CryptoWallet. has the option to utilize reputable and specialized electronic service providers to obtain technical identity data. Additionally, the company may choose to employ the following alternative methods for verifying identity without relying solely on documentary evidence:

4.3.7.1. The company may independently verify the client's identity by cross-referencing the information provided by the client with data obtained from consumer reporting agencies, public databases, or other reliable sources.

4.3.7.2. The company may conduct reference checks with other institutions to confirm the client's identity.

4.3.7.3. The company may analyse the consistency of the identifying information provided by the client, including their name, street address, postal code, and date of birth, to ensure logical coherence.

4.3.7.4. The company may utilize advanced techniques like "digital fingerprints" or IP geolocation checks to identify and authenticate client devices

4.3.7.5. The company may require a notarized or certified true copy of a governmental authority-issued identification document for valid identification purposes.

4.3.7.6. By incorporating these methods, the company aims to enhance its identity verification processes and ensure the accuracy and reliability of client information.

4.3.8. CryptoWallet. retains the right to conduct ongoing monitoring of its business relationship with a client, employing a risk-sensitive approach. This monitoring involves the following actions:

4.3.8.1. Periodically reviewing the documents, data, and information obtained by CryptoWallet. to ensure their currency and accuracy.

4.3.8.2. Diligently examining the Transactions and activities carried out by Clients to ensure their alignment with CryptoWallet.'s understanding of the User's business and risk profile. Additionally, CryptoWallet. verifies that such Transactions and activities are consistent with the User's declared sources of funds and wealth.

4.3.8.3. Identifying transactions that display unusually large amounts or exhibit patterns that deviate from the norm, lacking any discernible economic or legal justification.

4.3.9. CryptoWallet. might apply Enhanced Due Diligence (EDD) measures instead or in additionally to Client Due Diligence (CDD) procedures. Section 4.4 outlines the factors or events that may trigger the application of EDD measures.

4.4. ENHANCED DUE DILIGENCE

4.4.1. The purpose of this section is to provide guidance and direction for the application of enhanced due diligence (EDD) measures in situations where a high risk is identified. EDD measures are additional measures taken to verify a customer's identity and assess the legitimacy of their transactions and are used when the risk of money laundering or terrorist financing is higher.

4.4.2. The Situations that require enhanced due diligence (EDD), but not exhaustive:

4.4.2.1. if the client is assigned a high-risk status as a consequence of the Customer Risk Assessment (CRA).

4.4.2.2. during the identification of the person or verification of the provided information there is doubt as to the accuracy of the provided data or the authenticity of the documents;

4.4.2.3. a person using a professional service, or a client is related to a high-risk third country;

4.4.2.4. the nature of the situation entails a high risk of money laundering or terrorist financing.

4.4.2.5. at the discretion of a compliance specialist enhanced due diligence measures may be applied to mitigate unknown risk associated with client.

4.4.2.6. possible involvement of politically exposed persons (PEPs) or their close associates, operation from high-risk jurisdictions, or engaging in high-value transactions;

4.4.2.7. significant changes in a client's risk profile, client account volumes or sources of funds;

4.4.2.8. regulatory updates or changes that mandate periodic or event-driven EDD reviews;

4.4.2.9. client is unable to provide adequate explanations or documentation for the source of their funds or wealth, or who’s financial activities are inconsistent with his known income or business activities;

4.4.2.10. Information suggesting client involvement in the illicit activities, associations with criminal organisations, or exposure to reputational risks.

4.4.2.11. engages in high-volume transactions (exceeding 10,000 EUR), and there is a significant abnormal increase

4.4.2.12. transactions that involve complex structures or unusual patterns of behaviour.

4.4.3. In the aforementioned cases the company must apply the following enhanced due diligence measures:

4.4.3.1. Enhanced customer due diligence measures, which involve obtaining additional information about the customer, the customer's source of funds and source of wealth, and the customer's beneficial ownership.

4.4.3.2. Enhanced customer activity control measures, which involve requesting additional information or documents regarding latest activity on client accounts or latest completed or initiated transactions.

4.4.3.3. Enhanced monitoring of transactions and client accounts, which involves more frequent and detailed reviews of transactions, accounts activity and assessment of the connections with fraudulent, sanctioned or illicit activities, entities or individuals.

4.4.3.4. Enhanced record-keeping, which involves maintaining additional records related to the customer and the transactions conducted.

4.4.4. After assessing the risks and their effects, CryptoWallet. evaluates the most appropriate countermeasures to mitigate specific risks to the appropriate level for CryptoWallet. and arranges the implementation of countermeasures, if necessary. The risks associated with anonymity and fraud are avoided by identifying persons by requiring the person concerned to provide a copy of an identity document and confirm its authenticity. In addition, the person is asked to provide copies of utility bills showing the address of their place of residence as well as the connection of this address to this specific person. If the person does not prove the aforementioned facts or CryptoWallet. has doubts about the authenticity of the submitted documents, no service will be provided to the person.

5. TRANSACTION MONITORING

5.1. Before engaging in any transaction, CryptoWallet. conducts thorough Know Your Client (KYC) procedures and Customer Due Diligence and verifies the identities of the individuals or entities involved.

5.2. CryptoWallet. has integrated efficient systems and tools to ensure effective monitoring of cryptocurrency transactions. These monitoring systems incorporate special software, blockchain analysis tools, and other appropriate methods to identify any suspicious activities.

5.3. All transactions, both incoming and outgoing, shall be subject to monitoring to identify any suspicious or potentially illegal activity.

5.4. CryptoWallet. conducts periodic client risk assessments to reassess the risk profile of clients. This will involve reviewing their transaction history, monitoring their behaviour and activity patterns, and updating risk ratings accordingly.

5.5. Service Providers:

5.5.1. **Sumsub** offers advanced blockchain analysis and investigation tools to track and analyze crypto transactions. It provides insights into initial and ongoing crypto transaction monitoring, transaction flow, and identifies high-risk addresses. In addition to monitoring high-risk addresses, SUMSUB aims to provide insights about the originators and beneficiaries VASPs (virtual assets service provider) of cryptocurrency transfers. It analyzes transactional data and attempts to link wallet addresses to real-world entities whenever possible. This could involve identifying the parties involved in a transaction, such as the individuals or organizations associated with the cryptocurrency wallet addresses. Regarding sanctions compliance, SUMSUB may also attempt to identify wallet addresses that originate from or have connections to sanctioned countries. By analyzing transactional data and applying known sanctions lists, it can flag addresses that may be associated with individuals or entities in sanctioned jurisdictions.

5.6. Monitoring types

5.6.1. Manual monitoring entails a comprehensive and meticulous examination of client transactions to identify suspicious or unusual activity. This process involves analyzing transaction patterns, account activities, the source of funds, and other relevant factors to ensure compliance with AML-CTF regulations and identify potential red flags. The aim is to detect any transactions that deviate from the established patterns or that may indicate money laundering, terrorist financing, or other illicit activities. To achieve this, the Company employs a risk-based approach, tailoring the level of scrutiny to the assessed risk level of the client and transaction.

5.6.1.1. Frequency and Responsibility:

5.6.1.1.1. Daily Monitoring: Employees from the Compliance Team are responsible for conducting manual monitoring on a daily basis. This ensures that any suspicious activity is promptly identified and acted upon in a timely manner. The Compliance Team examines transactional behaviour, such as transaction frequency, amounts, and types of transactions, to identify any unusual patterns or sudden changes that may warrant further investigation.

5.6.1.1.2. Account Activity: Account-level analysis is performed to understand the overall financial behaviour of the client. This includes reviewing incoming and outgoing transactions, the flow of funds, and the nature of the client's interactions with other accounts.

5.6.1.1.3. High-Risk Indicators: The Compliance Team considers a range of high-risk indicators, such as transactions involving politically exposed persons (PEPs), clients from high-risk jurisdictions, and non-face-to-face relationships, which may warrant enhanced due diligence and monitoring.

5.6.1.1.4. Crypto Transaction Analysis: For clients engaging in crypto transactions, the Compliance Team investigates the wallet addresses involved, transaction hashes, and the underlying purpose of the crypto activity. Engaging in restricted actions, like employing privacy coins with active privacy functionalities or intricate mixing services, results in the termination of associations with CryptoWallet..

5.6.1.1.5. Source of Funds: A critical element of manual monitoring is verifying the legitimacy of the source of funds for specific transactions. The Compliance Team investigates the origin of funds to ensure they align with the client's stated business or financial activities.

5.6.2. Automatic monitoring is a critical component of the CryptoWallet. Compliance framework, facilitating real-time or near-real-time surveillance of transactions to swiftly detect patterns, deviations, or anomalies that may signal potential risks or suspicious activities. The automated monitoring system employs sophisticated algorithms and risk-based triggers to analyze vast amounts of transactional data, enabling timely identification of suspicious behaviour and supporting proactive risk mitigation.

5.6.2.1. Ongoing Transaction Monitoring:

5.6.2.1.1. The automatic monitoring system provided by SUMSUB operates in real-time or near-real-time, continuously scanning incoming and outgoing transactions across all channels and financial products offered by the CryptoWallet..

5.6.2.1.2. The automatic monitoring system allows for swift identification of suspicious activity as it occurs, enabling the Compliance Team to promptly investigate and take appropriate action.

5.6.2.2. Risk-Based Triggers and Alert Generation:

5.6.2.2.1. The automated monitoring system employs risk-based triggers, which are pre-defined parameters based on the Company's risk assessment and regulatory requirements. Such as: Sanctions, Child Abuse, Material Custom Address, Darknet Market, Decentralized Exchange, Contract Exchange, Fraud Shop, High risk Gambling, High Risk Exchange, High Risk Jurisdiction, Illicit Actor-Org, Infrastructure as a Service Lending Contract, Malware Merchant Services, Mining, Mining Pool, Mixing, Other P2P Exchange Protocol, Privacy Ransomware, Sanctions Scam, Stolen Funds, Terrorist Financing

5.6.2.2.2. These triggers generate alerts when transactions meet or exceed specified thresholds, deviate from historical patterns, or match predefined suspicious activity indicators.

5.6.2.2.3. High-risk indicators, such as large transactions, rapid and frequent transfers, or transactions involving high-risk jurisdictions, are included as part of the alert-generating mechanism.

5.6.2.3. System-Generated Reports and Analysis:

5.6.2.3.1. In addition to real-time alerts, the automatic monitoring system generates comprehensive reports that provide a holistic view of transactional activities over a specific period.

5.6.2.3.2. These reports aid the Compliance Team in identifying trends, detecting emerging risks, and conducting periodic reviews of transactional behaviour.

5.6.2.3.3. The analysis may involve data visualization techniques, anomaly detection algorithms, and trend analysis to highlight potential areas of concern. Integration of Crypto Transaction

5.6.2.4. Monitoring:

5.6.2.4.1. The automatic monitoring system includes specialized tools and capabilities provided by key service providers to monitor crypto transactions and wallets.

5.6.2.4.2. It tracks blockchain transactions, analyzes crypto addresses, and assesses potential risks associated with cryptocurrencies.

5.6.2.4.3. c. Crypto-related triggers, such as transactions involving privacy coins, mixing services, or suspicious wallet activities, are integrated into the automatic monitoring system.

5.6.2.5. Travel Rule:

5.6.2.5.1. The travel rule applies to crypto assets transfers and crypto companies (VASPs). The rule requires these institutions to collect and transmit specific information about their customers and the transactions they facilitate. CryptoWallet. is responsible for collecting and verifying this information from their customers during the onboarding process and retaining it for the required period. They must also transmit this information securely to the receiving CryptoWallet. or the next financial institution involved in the transaction, ensuring that it accompanies the funds or assets being transferred.

5.6.2.5.2. CryptoWallet has used the solution from Sumsub Travel Rule Integration, that allows easily integrating transaction monitoring, wallet screening, and Travel Rule compliance into our existing transaction and compliance workflows and approvals.

5.6.2.5.3. The Travel Rule requirement, stipulating a 0 EUR Threshold, necessitates that all outgoing and incoming cryptocurrency transactions shall be subjected to the Travel Rule procedure.

5.6.2.5.4. To comply with the Travel Rule regulations, CryptoWallet collects and transmits the following information for each applicable transactions:

5.6.2.5.4.1. For incoming and outgoing transactions

5.6.2.5.4.2. When performing a transaction of exchange or transfer of virtual currency, the transaction initiator’s provider of virtual currency service ascertains the identity of each customer, with respect to the initiator, collects at least the following particulars:

5.6.2.5.4.2.1. Originator's Name: The name of the person or entity sending the funds.

5.6.2.5.4.2.2. Originator's Account Number: The account number or identifier associated with the sender.

5.6.2.5.4.2.3. Originator's Address: The address of the sender

5.6.2.5.4.2.4. Originator’s title and number of the identity document and personal identification code OR date and place of birth and residential address/or registry code and country

5.6.2.5.4.2.5. Beneficiary's Name: The name of the person or entity receiving the funds (FATF recommendations are to ensure the Sanction/PEP list screening of beneficiary is provided as well)

5.6.2.5.4.2.6. Beneficiary's Account Number or Wallet address: The account number or identifier associated with the recipient.

5.6.2.5.4.2.7. Beneficiary's Address: The address of the recipient

5.6.2.5.4.2.8. Transaction Amount and currency: The amount of funds being transferred.

5.6.2.5.4.2.9. Transaction Date: The date when the transfer was initiated.

5.6.2.5.4.2.10. Transaction Identificator: transaction hash

5.7. Transaction risks related triggers.

5.7.1. Deposit:

5.7.1.1. Cardholder Name Discrepancy - The client provides a different name during the card payment step, which does not match the information provided during Know Your Customer (KYC) verification.

5.7.1.2. IBAN Owner Name Mismatch - The name of the account (IBAN) owner provided by the client does not match the information provided during KYC verification.

5.7.1.3. Multiple Card Purchases - The client has utilized more than five different cards for payments throughout their relationship with us.

5.7.1.4. Card Used by Different Clients - The same card has been used for payments on two different client accounts.
5.7.1.5. Repeated 3DS Declines - We have received three consecutive declines of 3D Secure (3DS) authentication codes for a particular transaction.
5.7.1.6. Multiple Cryptocurrency Purchases - The client has made several purchases of cryptocurrencies with fiat currency within a very short timeframe.
5.7.1.7. High-Risk Country Transaction - The transaction originates from a country that is considered to be a high-risk location, either based on the bank card's location or the IBAN country.
5.7.1.8. High-Risk Transaction - The transaction has been flagged as high-risk according to SUMSUB, Fireblocks
5.7.1.9. Bank Antifraud Transaction Cancellation - The bank has declined the payment method (card) used by the customer due to fraud-related concerns.
5.7.1.10. Antifraud: 3DS Declined - The client's attempts to purchase cryptocurrency using various cards were declined by the 3D Secure antifraud system.
5.7.1.11. Wallet Used by Multiple Clients - The same cryptocurrency wallet has been used for payments on two different client accounts.
5.7.1.12. Crypto Travel Rule Declined - A withdrawal transaction was declined due to non-compliance with the crypto Travel rule.
5.7.1.13. High-Risk Wallet - The recipient's cryptocurrency wallet address has been categorized as high or medium risk based on a review conducted by SUMSUB.
5.7.1.14. Three or More Cards Used for Purchase - More than three different cards in succession have been used for a series of purchases in a single day.
5.7.1.15. Crypto Deposit Exceeding 10,000 EUR Equivalent.
5.7.2. Withdrawal:
5.7.2.1. Withdrawal to High-Risk Country - The withdrawal transaction is directed to a country deemed to be high-risk, based on factors related to the card or IBAN issuing bank or the transaction's location.
5.7.2.2. High-Risk Transaction - The withdrawal transaction has been flagged as high-risk according to SUMSUB, Fireblocks, or ClearJunction.
5.7.2.3. High-Risk Wallet - The client is withdrawing funds to a cryptocurrency wallet that has been identified as high-risk by SUMSUB.
5.7.2.4. Wallet Shared by Multiple Clients - An attempt has been made to withdraw funds to an external address that is shared by another client.
5.7.2.5. High-Risk Person - The withdrawal transactions involve a person identified as high-risk, either from a list of sanctioned individuals or individuals with criminal records associated with money laundering and terrorist financing.
5.7.2.6. Crypto Travel Rule Declined - A withdrawal transaction was declined due to non-compliance with the crypto Travel rule.

5.8. Escalation and Investigation of suspicious activity and Immediate Alert Notification:
5.8.1. The automatic monitoring system is designed to trigger real-time alerts when it detects transactions that meet predefined risk-based thresholds or exhibit suspicious patterns.
5.8.2. Designated members of the Compliance Team and the MLRO receive immediate notifications of these alerts through secure and authenticated channels, ensuring swift attention to potential risks.
5.8.3. Comprehensive Transaction Details and Customer Profiles:
5.8.3.1. Upon receiving an alert, the automatic monitoring system provides the Compliance Team with comprehensive transaction details, including transaction amounts, timestamps, involved parties, and relevant transactional context.
5.8.4. Visualization:
5.8.4.1. The automatic monitoring system employs advanced data visualization tools that present transactions in a user-friendly format, facilitating a comprehensive understanding of transactional patterns and relationships.
5.8.4.2. Graphs, charts, and interactive dashboards are utilized to display transaction flows and identify potential clusters of suspicious activities.
5.8.5. Customer Enhanced Due Diligence (EDD):

5.8.5.1. If warranted by the nature of the alert or the client's risk profile, the Compliance Team initiates Enhanced Due Diligence (EDD) procedures.

5.8.5.2. EDD involves a deeper examination of the client's background, including the source of funds, business activities, beneficial ownership, and any relevant political or high-risk connections.

5.8.6. Transaction Enhanced Due Diligence (EDD)

5.8.6.1. In cases where red flags or suspicious transactions are identified, CryptoWallet. is responsible to conduct enhanced due diligence on the involved client and transaction.

5.8.6.2. EDD may involve gathering additional information about the transaction, the parties involved, and the purpose of the transaction, such as financial questionnaire, source of funds and source of wealth.

5.8.6.3. If an involved party fails to meet the requirements of Enhanced Due Diligence (EDD), the designated employees must submit the investigation findings and gather information to the MLRO. This will initiate further investigation and the preparation of a report for the Financial Intelligence Unit (FIU) and interested third parties.

5.8.6.4. Any employee, contractor, or agent of the company who suspects or becomes aware of a transaction that may be related to money laundering, terrorist financing, fraud, or other illicit activities must report it to the designated MLRO.

5.8.7. Collaboration and Communication:

5.8.7.1. Throughout the investigation, the Compliance team collaborates closely with other relevant departments, such as Legal and Management, to ensure comprehensive analysis and accurate decision-making.

5.8.7.2. Effective communication channels are established to share critical findings and coordinate actions promptly.

5.8.7.3. Decision-Making and Reporting:

5.8.7.4. Based on the results of the investigation, CryptoWallet. determines whether the flagged activity poses a genuine risk of money laundering, terrorist financing, or other financial crimes.

5.8.7.5. If warranted, the CryptoWallet. prepares a detailed Suspicious Activity Report (SAR) with all relevant findings and submits it to the appropriate regulatory authorities in accordance with the prescribed timeline.

5.9. Cryptocurrency and crypto wallets supporting policy.

5.9.1. CryptoWallet. maintains a steadfast dedication to furnishing a secure and dependable platform for clients to engage in cryptocurrency and token trading, buying, and selling. To uphold the integrity of our platform and safeguard our client base, we have implemented a comprehensive listing policy.

5.9.2. This AML policy's Attachment Nr. 1 includes the list of supported cryptocurrencies, which undergo periodic review and adjustments based on demand and requirements.

5.9.3. Cryptocurrency listing requirements:

5.9.3.1. Transparency: Cryptocurrencies and tokens seeking listing on our platform must exhibit a high level of transparency This includes Publicly identifiable development team with verifiable credentials. Clear and open-source code to allow for community inspection. A well-documented whitepaper explaining the project's purpose, technology, objectives, and use cases.

5.9.3.2. Legitimate Purpose: We strictly prohibit the listing of cryptocurrencies and tokens associated with any illegal, fraudulent, or illicit activities. Projects should have a legitimate purpose within the blockchain and cryptocurrency ecosystem and contribute positively to the industry.

5.9.3.3. Anti-Fraud and Anti-Money Laundering (AML) Compliance: Each listing will undergo a comprehensive SUMSUB check or similar blockchain analysis to ensure compliance with anti-fraud and AML regulations. This involves: Verifying the blockchain contract and its direct connection with sanctioned countries, entities, or individuals, confirmed connection with money laundering and other illicit activity.

5.9.3.4. Community and User Base: We value projects with a strong and active community as it indicates genuine interest and support for the project. Cryptocurrencies and tokens with an established and engaged user base will be given preference during the listing process.

5.9.3.5. Security and Stability: Projects seeking listing must demonstrate a secure and stable network infrastructure. Any history of major security breaches or technological vulnerabilities may result in rejection.

5.9.3.6. Public Exchange Listing: Priority will be given to cryptocurrencies and tokens that are already listed on reputable exchanges. Projects with a proven track record of successful listings on other platforms will be considered favourably.

5.9.4. Listing procedure:

5.9.4.1. Initial Review: The CryptoWallet. team will conduct an initial review of the listing application to determine if it meets the basic listing criteria. Incomplete or misleading applications will be rejected at this stage.

5.9.4.2. SUMSUB Check: After passing the initial review, the cryptocurrency or token will undergo a comprehensive SUMSUB check by CryptoWallet. to ensure compliance with anti-fraud and AML regulations.

5.9.4.3. Community Evaluation: CryptoWallet. may involve the community in the evaluation process, seeking feedback and opinions on the potential listing. While community input is valuable, the final decision rests with CryptoWallet..

5.9.4.4. Approval and Listing: Once the cryptocurrency or token successfully meets all the listing criteria and passes the SUMSUB check, CryptoWallet. will approve the listing, and it will be made available for trading on its platform.

5.9.4.5. Ongoing Monitoring: After listing, CryptoWallet. will continuously monitor the supported cryptocurrencies and tokens to ensure they maintain compliance with the AML policy. Projects found to be in violation of any criteria may face delisting from our platform.

5.9.5. Prohibited cryptocurrency:

5.9.5.1. CryptoWallet. maintains a strict policy against supporting and listing any cryptocurrencies that fall under the category of prohibited cryptocurrencies. As a responsible cryptocurrency platform, we do not endorse, facilitate, or engage in any activities associated with prohibited cryptocurrencies.

5.9.5.2. Prohibited cryptocurrencies may include, but are not limited to, those involved in the following situations:

5.9.5.2.1. Illicit Activities: Cryptocurrencies associated with illegal activities such as money laundering, terrorism financing, drug trafficking, or any other criminal endeavours.

5.9.5.2.2. Fraudulent Schemes: Cryptocurrencies linked to Ponzi schemes, pyramid schemes, or other fraudulent activities designed to deceive investors.

5.9.5.2.3. Scam Projects: Cryptocurrencies tied to projects with no legitimate purpose, deceptive promises, or false claims.

5.9.5.2.4. Privacy Concerns: Cryptocurrencies with enabled crypto privacy feature such as Monero (XMR) Zcash (ZEC) Dash (DASH) Grin (GRIN) Beam (BEAM) Horizen (ZEN) Komodo (KMD) Pirate Chain (ARRR). Whole list available on website: https://coinmarketcap.com/view/privacy/. Usage of these cryptocurrencies is restricted and unavailable in conjunction with the CryptoWallet. service.

5.9.5.2.5. Hacking Incidents: Cryptocurrencies obtained through hacking, theft, or cyberattacks on exchanges or individuals.

5.9.5.2.6. Market Manipulation: Cryptocurrencies involved in pump-and-dump schemes or other forms of market manipulation. Non-Compliance with

5.9.5.2.7. Regulations: Cryptocurrencies failing to adhere to applicable legal and regulatory requirements, such as anti-money laundering (AML) and know-your-customer (KYC) regulations.

5.9.5.2.8. Stolen Funds: Cryptocurrencies resulting from stolen funds or assets that were unlawfully obtained.

5.9.5.2.9. Controversial Content: Cryptocurrencies associated with illegal content, hate speech, or any form of harmful and offensive material.

5.9.5.2.10. Sanctioned Entities: Cryptocurrencies issued or supported by entities or individuals subject to international sanctions or restrictions.

5.9.5.2.11. Vulnerable Smart Contracts: Cryptocurrencies built on insecure or flawed smart contracts that may be prone to hacks or exploitation.

5.9.5.2.12. High Volatility and Risks: Cryptocurrencies with extremely high volatility and no underlying value, posing significant risks to investors.

5.9.5.2.13. Lack of Regulatory Compliance: Cryptocurrencies developed without considering or adhering to applicable financial regulations and standards.

5.9.6. Prohibited crypto wallets.

5.9.6.1. Prohibited crypto wallets is restricted to use with CryptoWallet. service and may include, but are not limited to, those involved in the following situations:

5.9.6.1.1. Unhosted wallets or Untraceable Wallets: Wallets that allow users to remain completely anonymous or obscure transaction history are prohibited in conjunction with the services provided by CryptoWallet..

5.9.6.1.2. Highly Privacy-Centric Wallets: Wallets that implement extremely strong privacy measures, such as CoinJoin, Mimblewimble, or other privacy-focused technologies, are prohibited in conjunction with the services provided by CryptoWallet..

5.9.6.1.3. Wallets Associated with Darknet Markets: Wallets used in connection with illegal marketplaces on the dark web are prohibited in conjunction with the services provided by CryptoWallet..

5.9.6.1.4. Decentralized Wallets with No Oversight: Wallets that function in a decentralized manner without any oversight from a central entity are limited, if wallet could be screened and monitored, or restricted, if their activity cannot be monitored.

5.9.6.1.5. Wallets with Ties to Sanctioned Entities: Wallets linked to individuals, organizations, or countries subject to international sanctions will be prohibited.

5.9.6.1.6. High-Risk Wallet Addresses: Wallets identified as having participated in fraudulent schemes, hacking activities, or scams will be prohibited.

5.9.6.1.7. Wallets Facilitating Prohibited Token Sales: Wallets involved in the distribution of unauthorized securities or tokens will be prohibited.

5.9.7. Prohibited activity

5.9.7.1. CryptoWallet. explicitly prohibits any association, financial dealings, connections, or direct interaction with Defi platforms, cryptocurrencies and crypto wallets, as clearly delineated in articles 5.9.5 and 5.9.6 of this policy. If any such prohibited activities are detected, the consequences will be severe and may result in immediate and irreversible actions, including but not limited:

5.9.7.1.1. Initiating the Enhanced Due Diligence procedure for the concerned client.

5.9.7.1.2. Permanently freezing incoming or outgoing transactions related to the prohibited activities;

5.9.7.1.3. Conducting a thorough investigation in collaboration with the compliance team and CryptoWallet.'s Money Laundering Reporting Officer (MLRO).

5.9.7.1.4. Disclosing relevant information to appropriate third parties.

5.9.7.1.5. Blocking the CryptoWallet. account associated with the prohibited activities, with no possibility of restoration.

5.9.7.1.6. Filing a report with the Financial Intelligence Unit (FIU) in accordance with regulatory obligations.

5.9.8. Direct or indirect connection with High-Risk crypto wallets

5.9.8.1.1. The SUMSUB KYT ongoing monitoring of connections with high-risk triggers in the context of crypto wallets can be categorised into two types: direct and indirect.

5.9.8.1.2. Direct Connection: This occurs when a crypto wallet is directly linked to addresses, transactions, or entities that have been identified as high-risk, sanctioned, or prohibited as per the guidelines outlined in article 5.9.6.

5.9.8.1.3. Indirect Connection: This involves evaluating the services and entities involved in the origination or destination of funds within transactions associated with the target address. The assessment takes into account scenarios where non-service addresses are present between the target address and the aforementioned services or entities.

5.9.8.1.4. In cases where there is a confirmed and direct connection with a high-risk crypto wallet, CryptoWallet. applies Enhanced Due Diligence to thoroughly investigate the source and origin of these funds.

5.9.8.1.5. For situations where a crypto wallet has an indirect connection with a high-risk wallet and the exposure percentage does not exceed 20% of the total transaction sum, CryptoWallet. applies a red flag for further scrutiny.

5.9.8.1.6. In all situations related sanctioned regions, PEP, sanctioned entities, sanctioned individuals, and triggers as described in article 5.9.6, CryptoWallet. implements the measures specified in article5.9.7.

6. UNUSUAL ACTIVITY REPORT

6.1. CryptoWallet. is obliged to notify the Financial Intelligence Unit and interested 3rd parties of (i) activities or (ii) circumstances identified in the course of economic activity:

6.1.1. which have characteristics that indicate the use of proceeds from criminal activity or the commission of related criminal offences (primarily related to reporting of suspicious and unusual transactions or activities).

6.1.2. which give rise to suspicion, or which are known to be money laundering or the commission of related crimes, or the characteristics of which point to money laundering or the commission of related crimes (primarily related to reporting a suspected money laundering transaction or activity);

6.1.3. which give rise to suspicion, or which are known to be terrorist financing or the commission of related crimes, or the characteristics of which point to terrorist financing or the commission of related crimes (primarily related to reporting a suspected terrorist financing transaction or activity);

6.1.4. in the event of which there is a suspicion or knowledge of the need to apply an international financial sanction

6.2. The Financial Intelligence Unit and interested 3rd parties must also be notified of the following:

6.2.1. the circumstances of refusing to establish a business relationship or an occasional transaction, if the basis for the refusal is suspicion of money laundering or terrorist financing, or if CryptoWallet. is unable to apply the due diligence that must be applied when establishing a business relationship, because the client does not or refuses to provide the relevant data, or the data provided is not sufficient to ensure the adequacy of collected data;

6.2.2. the extraordinary termination of the business relationship, if the business relationship is terminated because it is not possible to apply the due diligence again as after a reasonable period of time CryptoWallet. has still not been able to apply sufficient due diligence to exhaustively collect data, verify the accuracy of data or eliminate money laundering or terrorist financing suspicion, or because the client does not provide or refuses to provide the relevant data, or the data provided is not sufficient to ensure the adequacy of collected data (primarily reporting a suspicious and unusual transaction or activity).

6.3. The notifications specified in clauses 6.1 and 6.2 must be made before making a transaction, which gives rise to suspicion, or which is known to be money laundering or terrorist financing or the commission of related crimes and if such circumstances are detected before making the transaction. Given the speed with which money laundering and terrorist financing crimes are committed, fulfilling this pre-transaction notification obligation may be appropriate in other cases as well. If postponing the transaction may cause significant damage, not making the transaction is not possible, or may prevent the capture of a potential perpetrator of money laundering or terrorist financing, the transaction is executed and then a report is submitted to the Financial Intelligence Unit. To identify such circumstances, the obliged person is in contact with the Financial Intelligence Unit.

7. IMPOSING INTERNATIONAL SANCTIONS

7.1. The objective of the national imposition of international sanctions and the implementation thereof is, in compliance with the United Nations Charter, to maintain or restore peace, prevent conflicts, and reinforce international security, support and reinforce democracy, follow the rule of law, human rights and international law and achieve other objectives of the common foreign and security policy.
of the European Union. An international sanction within the meaning of this code of conduct is a measure that is not related to the use of armed forces, and which has been decided to be imposed by the European Union, the United Nations, another international organization or the relevant state in order to achieve the aforementioned goal.

7.2. Subject to international sanctions means a natural or legal person, entity or body which is directly specified in the act on the imposition or implementation of international sanctions and with regard to whom the measures prescribed therein are taken.

7.3. A person with special obligations, to whom the special obligations of the International Sanctions Act apply is, among other things, a virtual currency service provider within the meaning of the Money Laundering and Terrorist Financing Prevention Act.

7.4. CryptoWallet. (hereinafter also person with special obligations) takes measures to fulfil the resulting obligations upon the entry into force of the legislation establishing or implementing an international financial sanction and demonstrates the diligence necessary to ensure the achievement of the goal of the international financial sanction and to avoid breach of the sanction. A natural or legal person who has a suspicion or who knows that a person with whom they have a business relationship or are making a transaction or operation with, as well as a person with whom they are planning to establish a business relationship or make a transaction or operation, is subject to an international financial sanction, immediately notifies the Financial Intelligence Unit of the identification of the subject of the international financial sanction, the relevant suspicion and the measures taken.

7.5. CryptoWallet. places significant emphasis on the conduct of individuals and entities involved in its economic activities, including those with whom it maintains business relations, conducts transactions, or engages in any form of business. The company also considers individuals who intend to establish business relations, conduct transactions, or engage in any business-related activities. Additionally, CryptoWallet. considers circumstances that suggest the possibility that a person may be subject to international financial sanctions. The company actively strives to mitigate any potential legal consequences and reputational risks associated with its interactions with sanctioned individuals. In line with its commitment to compliance, CryptoWallet. promptly terminates relationships and initiates further investigations upon the confirmation of any suspicions. The company strictly adheres to the policy of not engaging in any dealings with sanctioned individuals.

7.6. CryptoWallet. periodically monitors the website of the Financial Intelligence Unit and immediately takes the measures provided for in the legislation establishing or implementing the international financial sanction in order to ensure the achievement of the goal of the international financial sanction and to prevent breaches of the international financial sanction.

7.7. Upon entry into force, amendment, invalidation or expiration of an international financial sanction legislation, CryptoWallet., as a person with special obligations, immediately checks whether the person with whom it is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, is the subject of the international financial sanction imposed, amended or lifted.

7.8. If the legal act establishing or implementing an international financial sanction is declared invalid, it expires, or it is changed in such a way that the application of the international financial sanction to the subject of the international financial sanction is lifted in whole or in part, CryptoWallet., as a person with special obligations, immediately ceases the implementation of the measure to the extent provided for in the act on the imposition or application of the international financial sanction.

7.9. CryptoWallet. establishes in writing or in a format which can be reproduced in writing procedural rules for the implementation of an international financial sanction and the fulfilment of the obligations arising from the respective law and procedure for checking the compliance with these procedural rules and appoints the person responsible for the implementation of the international financial sanction, whose contact details he forwards to the supervisory authority.

7.10. According to the International Sanctions Act, persons with special obligations must carry out additional due diligence to identify situations when international financial sanctions must be applied. To this end, the named persons must:

7.10.1. exercise extra diligence with respect to the client and the circumstances of the transaction (including the other party to the transaction) when establishing a business relationship and conducting transactions;

7.10.2. credit and financial institutions pay attention to all parties and circumstances of the transaction (including goods) in trade finance transactions to ensure enforcement of international sanctions;

7.10.3. monitor the information on sanctions in their activities and the corresponding lists on the website of the Financial Intelligence Unit;

7.10.4. notify the Financial Intelligence Unit of the identification of a subject of the financial sanction and the implementation of a financial sanction on the basis of such information;

7.10.5. collect additional information (including from the Client) if there is a suspicion that a person is subject to financial sanctions;

7.10.6. in the event of there still being a suspicion of financial transaction regarding the person or the circumstances of the transaction and the other party after collecting additional information, notify the Financial Intelligence Unit of the suspicion (also if additional information cannot be collected), while refusing to make further transactions and/or establish a business relationship;

7.10.6.1. notify the Financial Intelligence Unit of the refusal to establish a business relationship;

7.10.6.2. inform the Financial Intelligence Unit of a suspicion that a person is under the direct or indirect control of a subject to international sanctions;

7.10.6.3. have the procedural rules and MLRO necessary for the implementation of the financial sanction;

7.10.6.4. carry out checks to identify financial sanctions;

7.10.6.5. store data related to financial sanction suspicions, implementations and corresponding controls.

7.10.7. Upon identification of the subject of international financial sanctions, it is necessary to identify the measures established to sanction this person. The measures to be taken are described in the legislation establishing the sanction, so the exact sanction imposed on the person must be identified in order to ensure the legal and correct implementation of the measures.

7.10.8. All other persons must show due diligence in the course of their activities in order to identify the need for the implementation of an international financial sanction. A natural who has a suspicion or who knows that the person with whom it is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, immediately notifies the Financial Intelligence Unit of the identification of the subject of the international financial sanction, the relevant suspicion and the measures taken.

7.10.9. The Financial Intelligence Unit will check the application of the financial sanction within 10 working days from the receipt of the notification, including whether the subject of the financial sanction has been correctly identified and whether the measures have been taken legally, and then inform the person that submitted the notification about the result of the inspection within 2 working days.

7.10.10. A person with special obligations collects and preserves for five years the following information:

7.10.10.1. inspection time;

7.10.10.2. the name of the inspecting person;

7.10.10.3. results of the inspection;

7.10.10.4. measures taken.

7.11. If a person with special obligations or a person authorized by them doubts whether a person with whom it is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, is the subject of an international financial sanction, they ask additional information from that person for the identification of said fact. If a person who is in business relations or is making transactions or is carrying out acts with the person having specific obligations, as well as a person who intends to create business relations, make a transaction or carry out an act, refuses to provide additional information or it is impossible to identify by means thereof if the person is a subject of international financial sanction, the person having specific obligations or a person authorized by them refuses to make a transaction or act, takes measures provided for in the act on the imposition or implementation of international financial sanction and notifies immediately the Financial Intelligence Unit of their doubts and of the measures taken.

7.12. Upon entry into force of an act on the imposition or implementation of international financial sanctions the employees of CryptoWallet. take measures to fulfil the obligations arising therefrom and demonstrate due diligence to ensure the achievement of the objective of the international financial sanction and avoid breach of the sanction.

7.13. An employee of CryptoWallet. who has doubts or who knows that a person with whom CryptoWallet. is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, is a subject of international financial sanction, immediately notifies the Financial Intelligence Unit of the identification of the subject of international financial sanction, of the doubt thereof and of the measures taken.

7.14. In the economic activity of CryptoWallet., an employee of CryptoWallet. pays special attention to the activities of the person with whom CryptoWallet. is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, and to the circumstances which refer to the possibility that the person is a subject of an international financial sanction.

7.15. If an employee of CryptoWallet. doubts whether a person with whom CryptoWallet. is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, is the subject of an international financial sanction, they inform the board of with CryptoWallet. of this suspicion, which in turn asks the said person for additional information in order to determine whether these suspicions are correct.

7.16. If a person with whom CryptoWallet. is in business relations or is making a transaction or carrying out an act, as well as a person intending to create business relations, make a transaction or carry out an act, refuses to provide additional information or it is impossible to identify by means thereof if the person is a subject of international financial sanction, CryptoWallet. refuses to make a transaction or act, takes measures provided for in the act on the imposition or implementation of international financial sanction and notifies immediately the Financial Intelligence Unit of their doubts and of the measures taken.

7.17. If an act on the imposition or implementation of international financial sanction is repealed, expires, or is amended in such a manner that the implementation of the international financial sanction with regard to the subject of the international financial sanction is terminated wholly or partially, CryptoWallet. ceases the implementation of the measure to the extent provided for in the act on the imposition or application of the international financial sanction.

7.18. European Union sanctions against countries can be checked online on the website at https://www.sanctionsmap.eu/#/main; it is possible to check the sanctions of the European Union and the United Nations against subjects

7.19. Additionally, CryptoWallet. leverages a KYC provider that offers client monitoring services and conducts checks against a comprehensive range of sanction lists, including but not limited to the following.:

7.19.1. DFAT Australia Consolidated Sanctions List
7.19.2. DFATD Canada Special Economic Measures Act Designations
7.19.3. EU External Action Service - Consolidated list of Sanctions
7.19.4. European Council List of Designated Vessels
7.19.5. European Council Restrictive Measures on Russian entities destabilizing the situation in Ukraine.
7.19.6. Finland National Bureau of Investigation Asset Freeze List
7.19.7. Indonesia PPATK List of Suspected Terrorists and Terrorist Organizations DTTOT Sanctions
7.19.8. Iran March and May 2017 Sanctions against US entities
7.19.9. Ireland Organizations Sanction Laws
7.19.10. Israel Division of Sanctions Headquarters Prevention of Distribution and Financing of Weapons of Mass Destruction sanctions
7.19.11. Israel National Bureau for Counter Terror Financing Designated associations and terrorist's organisations
7.19.12. Luxembourg Liste des Sanctions Financières Internationales
7.19.13. Ministry of Finance Japan Economic Sanctions List
7.19.14. Monaco Economic Sanctions
7.19.15. New Zealand Police Designated Terrorists
7.19.16. Norway Sanctions and Restrictive Measures
7.19.17. OFAC Consolidated List
7.19.18. OFAC SDN List
7.19.19. Serbia Government Decisions on Terrorism related Sanctions Designations
7.19.20. Singapore First Schedule of the Terrorism (Suppression of Financing) Act
7.19.21. Sri Lanka Ministry of Defence Sanctions Designations under UN Regulation concerning the proliferation of WMD
7.19.22. Switzerland Federal Council Freezing of Foreign Illicit Assets
7.19.23. Switzerland SECO List
7.19.24. Taiwan Ministry of Justice Investigation Bureau Sanctions under Anti-terrorism Law
7.19.25. Thailand Designated Persons Sanctions List

7.19.26. Thailand Designated Persons Thai Version
7.19.27. Tunisia Sancti
7.19.28. HM treasury's office for financial sanctions consolidated list
7.19.29. FinCEN Sanctions List
7.19.30. United Nations Consolidated List
7.19.31. United Nations Security Council List of Designated Vessels
7.19.32. United States Bureau of Industry and Security Entity List
7.19.33. United States Bureau of Industry and Security Military End Client List
7.19.34. United States Bureau of Industry and Security The Denied Persons List
7.19.35. United States Bureau of Industry and Security Unverified List
7.19.36. Israel National Bureau for Counter Terror Financing Seizure of Cryptocurrencies
7.19.37. Sri Lanka Government Notifications Under The Preventions of Terrorism Act No. 48 of 1979
7.19.38. Qatar National Counter Terrorism Committee International Sanctions
7.19.39. United States Department of State Counter Terrorism Rewards Program Organisations

7.20. The responsible person or the person appointed by him checks the entry into force, amendment and termination of sanctions using automated technological solutions and public databases of the key partners of CryptoWallet. (Sumsub). Sanctions are monitored automatically and in the event of receipt of inaccurate or incomplete data, the responsible person may organize an additional manual check. Also, the automated control is structured in such a way that it monitors the existing Client base in real-time and when sanctions come into force against a specific client, it immediately transmits the information via e-mail to the responsible person. In addition, if the automated system detects a contradiction with the information in the databases, it immediately sends the message via e-mail to the responsible person. The designated person monitors on an ongoing basis the performance of the automated system and promptly reports any issues that arise to the responsible person for further investigation. CryptoWallet. conducts Sanction status screening for Clients during onboarding and during the year on an ongoing basis after initial check was completed. Ongoing screening will be restarted after client annual recheck. Screening is calibrated with a default fuzzy logic accuracy (threshold 90% and bi-gram jaccard similarity is used for comparison) provided by the service provider.

8. POLITICALLY EXPOSED PERSON AND NEGATIVE NEWS

8.1. Politically exposed person means 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:

8.1.1. local politically exposed person means a person specified in clause 8.1 who is or who has been

8.1.2. entrusted with prominent public functions in European Economic Area country or

8.1.3. an institution of the European Union;

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

8.1.5. person known to be close associate' means a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person or a local politically exposed person; 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 or local politically exposed person.

8.2. In instances where the client or the beneficial owner holds a politically exposed status, is related to a politically exposed person as a family member or is associated with them as a known close associate, CryptoWallet. will decline to establish the relationship. If such a status is verified subsequent to the commencement of the relationship, it will result in the termination of the relationships.

8.3. CryptoWallet. conducts PEP status screening for Clients during onboarding and during the year on an ongoing basis after initial check was completed. Ongoing screening will be restarted after client annual recheck. Screening is calibrated with a default fuzzy logic accuracy (bi-gram jaccard similarity is used for comparison, threshold 90%) provided by the service provider and performed daily. Clients will be screened for negative news during onboarding and ongoing basis.

8.4. CryptoWallet. conducts a name check of a client daily and consider, based on a risk approach, extending the check to the client's beneficial owners against the latest sanction lists before the establishment of a business relationship with that client, regardless of what service is to be provided and perform ongoing screening of our client base regularly thereafter.

8.5. Negative news check

8.5.1. The negative news screening aims to ensure that CryptoWallet. effectively identifies and mitigates any reputational risks associated with its clients by conducting regular screening for negative news provided by service provider.

8.5.2. CryptoWallet. utilizes the services of Sumsub for negative news screening of its clients. Sumsub's screening system is implemented to identify negative news and adverse media associated with Clients. Negative news screening is conducted during the Client onboarding process and on an ongoing basis.

8.5.3. If potential or true negative news matches are identified by Sumsub, CryptoWallet. takes charge of the escalation process, which may involve conducting enhanced due diligence or terminating Client relationships as deemed necessary.

8.5.4. CryptoWallet. reserves the right to disclose the received monitoring information or results to relevant and interested third parties for further investigation or approval, if it is not restricted by law or other applicable regulations.

9. OUTSOURCING

9.1. CryptoWallet. acknowledges the significance of adhering to outsourcing requirements as outlined in the financial crime framework and undertakes the following steps to ensure compliance with regulatory obligations:

9.1.1. maintains a comprehensive procedures document that encompasses the recording, evaluation, and monitoring of critical or important outsourced functions. These rules are regularly reviewed and updated to align with the Regulatory Guidelines on Outsourcing.

9.1.2. conducts thorough assessments to determine the importance or criticality of each function that is considered for outsourcing. The assessments include evaluating whether the function would typically be carried out by CryptoWallet.. Additionally, CryptoWallet. conducts due diligence on potential service providers, including assessing their financial stability. Risk assessments are performed, considering Contractual Risk, Strategic Risk, Reputation Risk, Compliance Risk, Operational Risk, Exit Strategy Risk, Access Risk, Concentration and Systemic Risk (including risks associated with dominant service providers or multiple arrangements with closely connected providers), and Credit Risk.

9.1.3. assigns responsibilities for documenting, managing, and controlling outsourcing arrangements. The designated personnel ensure that all legal and regulatory requirements, including the provided guidelines, are met. Adequate resources are allocated to ensure compliance, including the documentation, and monitoring of all outsourcing arrangements. An Outsourcing Register is maintained to track and record relevant information.

9.1.4. establishes an outsourcing function within the organization or designates a senior staff member who is directly accountable to the management body or Board. This individual is responsible for overseeing and managing the risks associated with outsourcing arrangements, ensuring compliance with the established guidelines.

9.1.5. maintains comprehensive documentation to demonstrate compliance with its outsourcing policy and procedures. This includes documentation at the Board level. A register of current outsourcing arrangements is maintained, and internal audits are conducted to ensure ongoing compliance with the policy and regulatory requirements.

9.1.6. maintains contingency plans, including a plan for disaster recovery and periodic testing of backup facilities.

9.1.7. ensures that its agreements with outsource providers contain clauses that align with the outlined requirements, including:

9.1.7.1. clear description of the outsourced function;

9.1.7.2. start and end dates with relevant notice periods;

9.1.7.3. governing law;

9.1.7.4. parties' financial obligations;

9.1.7.5. identification of critical or important functions;

9.1.7.6. locations from which the critical or important function will be provided or where relevant data will be kept and processed;

9.1.7.7. provisions regarding availability, integrity, privacy, and safety of the data;

9.1.7.8. right to monitor and audit the service provider's performance;

9.1.7.9. agreed service levels, including "exact quantitative and qualitative performance targets" if applicable;

9.1.7.10. reporting obligations;

9.1.7.11. mandatory insurance requirements;

9.1.7.12. requirements regarding business contingency plans;

9.1.7.13. provisions ensuring data accessibility in the case of insolvency, resolution, or discontinuation of the service provider's business;

9.1.7.14. obligation for the service provider to cooperate with relevant regulators;

9.1.7.15. unrestricted right for CryptoWallet., to inspect and audit the service provider;

9.1.7.16. termination rights

9.2. Occasionally, we may encounter issues or breaches in our outsourced activities, and it is expected that we address and resolve these matters promptly. The utmost priority in resolving such disputes or breaches is to ensure that they do not result in:

9.2.1. failure of the business to provide fair, efficient, and professional services to clients

9.2.2. failure of the business to comply with legislative and code requirements,

9.2.3. significant financial or operational losses for the business.

9.2.4. If a dispute or breach of contract arises with an outsourced supplier, it should be immediately referred to a Senior Manager for resolution.

9.2.5. The Senior Manager will utilize their business skills and expertise to rectify the matter with the supplier.

9.3. If the Senior Manager is unable to satisfactorily rectify the matter with the supplier within 14 days, they will consider one or more of the following options, based on the nature and severity of the situation:

9.3.1. accept the failure or breach by the supplier;

9.3.2. seek assistance from relevant alternative dispute resolution facilitators;

9.3.3. consult our legal advisers regarding the matter;

9.3.4. recommend to the Board the termination of the supply contract or agreement for their consideration;

9.3.5. suggest to the Board the engagement of an alternative supplier to provide replacement services.

10. EXIT MANAGEMENT

10.1. CryptoWallet. keep the right to terminate relationships with a client at the sole discretion and the Client will not be entitled to a remedy or alternative for discontinued services. CryptoWallet. has defined roles, responsibilities, and governance for the exit strategy, including compliance personnel trained to handle the process efficiently and in compliance.

10.2. CryptoWallet. has identified specific red flags that may indicate potential financial crime risks or compliance breaches. For example, if a Client consistently engages in large, unexplained transactions or exhibits unusual transaction patterns inconsistent with their known business activities, it may trigger a review and consideration for exiting the Client relationship. Among other reasons not listed, CryptoWallet. may also suspend or terminate your account for any or all the following reasons:

10.2.1. Any client found to be in violation of applicable AML regulations, such as engaging in money laundering activities or knowingly facilitating transactions involving illicit funds, will be subject to immediate termination of their account and associated privileges.

10.2.2. Clients who fail to comply with CryptoWallet.'s AML policy, including providing requested identification documents, suspicious activity reports, or any other relevant information, may have their account suspended or terminated.

10.2.3. Clients engaged in high-risk activities, as determined by CryptoWallet.'s risk assessment procedures,

10.2.4. including but not limited to engaging in frequent large-scale transactions, transferring funds to/from high-risk jurisdictions, or involvement in known illicit activities, may face termination of their account.

10.2.5. Clients providing false, misleading, or fraudulent information during the onboarding process, such as incorrect identification details or purpose of transactions, will have their account terminated.

10.2.6. Clients who refuse to cooperate with CryptoWallet.'s AML compliance measures, including blocking or delaying the investigation of suspicious transactions or providing false explanations for their activities, may be subject to termination.

10.2.7. Clients who have previously been warned or suspended for AML policy violations and continue to engage in non-compliant activities may face permanent termination of their account.

10.2.8. In cases where a client is found to be connected with a sanction regime, sanctioned individuals, or sanctioned companies, an exit management process will be initiated.

10.3. CryptoWallet. has established a clear communication approach when interacting with Clients during the exit process. For instance, if the decision to exit a Client is made, CryptoWallet. ensures that any communication or engagement with the Client is conducted in a manner that maintains confidentiality and complies with the tipping-off rule. This ensures that the Client is not alerted to the fact that they are being exited due to suspicions of financial crime.

10.4. CryptoWallet. has implemented a robust tracking and recording process for Client exits. For example, when a decision is made to exit a Client, CryptoWallet. records essential information such as the Client's name, the reason for exit consideration, the dates of review and final decision, the sign-off authority, and the actual date of Client exit. This documentation ensures a transparent and auditable record of the exit process.

10.5. CryptoWallet. maintains a watch list monitor Clients flagged for potential exit. This list allows CryptoWallet. to focus on Clients who require ongoing scrutiny, ensuring that they are not inadvertently overlooked during the exit process. Continuous monitoring helps detect any suspicious activities that may require further investigation.

11. RECRUITMENT

11.1. CryptoWallet. recognizes the importance of recruiting appropriately trained and experienced staff, including contractors and third parties, to ensure a risk-based approach to combating financial crime. The following measures ensure that CryptoWallet. recruits qualified individuals who contribute to our efforts in combating financial crime and adhering to AML regulations: Clients flagged for potential exit. This list allows CryptoWallet. to focus on Clients who require ongoing scrutiny, ensuring that they are not inadvertently overlooked during the exit process. Continuous monitoring helps detect any suspicious activities that may require further investigation.

11.1.1. CryptoWallet. employs a risk-based approach to recruit appropriately trained and experienced individuals, considering the nature of roles and potential financial crime risks.

11.1.2. CryptoWallet. established a comprehensive employment screening system to assess suitability and integrity, which includes:

11.1.2.1. identity Verification

11.1.2.2. employment History Checks

11.1.2.3. criminal Record Checks d. Regulatory Checks

11.1.2.4. reference Checks f. Ongoing Monitoring

11.2. CryptoWallet. screening process follows principles of fairness, consistency, and compliance with applicable laws and regulations, while respecting privacy rights

11.3. CryptoWallet. conducts comprehensive training and orientation programs for all new employees, ensuring a smooth integration into the organisation.

12. TRAINING

12.1. CryptoWallet. recognizes the importance of providing regular and up-to-date training on Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) to its employees. The frequency and content of the training program will be adjusted to reflect changes in legal and regulatory requirements, employees' duties, and business model changes. These training sessions will be conducted no less than once a year to ensure compliance and keep employees well-informed. The training program aims to educate employees on the latest developments in preventing money laundering and terrorist financing, including practical methods and emerging trends.

12.2. The MLRO is responsible for implementing and overseeing the AML/CTF training program to ensure employees are aware of their legal obligations. The MLRO should collaborate with relevant stakeholders to develop and deliver comprehensive training sessions.

12.3. The frequency of AML/CTF training sessions will be determined based on the following factors:

12.3.1. Amendments to legal and regulatory requirements: Training should be updated to reflect any changes in AML/CTF regulations.

12.3.2. Employees' duties: Training frequency may be adjusted based on employees' roles and responsibilities within the organization.

12.3.3. Changes in the business model: If there are significant changes in the business model that impact AML/CTF risks, additional training may be conducted.

12.3.4. On an annual basis, unless otherwise triggered by above mentioned factors.

12.4. The AML/CTF training program should cover the following key areas:

12.4.1. Understanding AML/CTF regulations: Employees should be educated on the legal and regulatory requirements related to money laundering and terrorist financing prevention.

12.4.2. Latest developments and trends: Training should focus on the most recent developments in AML/CTF practices, including emerging methods and trends used for money laundering and terrorist financing.

12.4.3. Practical methods and tools: Employees should be provided with practical knowledge, tools, and techniques to identify, prevent, and report suspicious activities related to money laundering and terrorist financing.

12.5. Training sessions may be conducted through various methods, including workshops, seminars, online modules, or a combination of these approaches. The most suitable delivery method will be chosen based on effectiveness, accessibility, and cost considerations.

12.6. Failure to comply with the training requirements may lead to disciplinary actions, which can include verbal warnings, written warnings, suspension, or termination of employment, depending on the severity and frequency of non-compliance.

12.7. In cases where an employee fails to successfully complete the required AML/CTF training, they may

12.8. be provided with additional retraining opportunities. The employee will be required to participate in the retraining session(s) and successfully complete the assessment to meet the training completion requirement.

12.9. CryptoWallet. maintains accurate records of employees' participation and completion of AML/CTF training. These records will serve as evidence of compliance and may be used for auditing purposes or reporting to relevant authorities, if necessary.

12.10. After a new employee has signed their employment contract, the MLRO must instruct them in accordance with the established procedure within at least one week after the new employee starts work and introduce this code of conduct to the new employee against a signature.

12.11. The MLRO has the right to submit proposals to the management board of the undertaking regarding training providers. If the obligation to enforce the code of conduct is assigned to another person on the basis of an authorization agreement, they must follow the code of conduct in full.

13. AUDIT AND PROCEDURES FOR ENSURING COMPLIANCE WITH THE RULES OF PROCEDURE AND INTERNAL CONTROL STANDARDS

13.1. Supervision over the compliance of the management board of CryptoWallet. with the requirements of the Money Laundering and Terrorist Financing Prevention Act and the legislation established on the basis thereof is carried out by the Financial Intelligence Unit and/or other competent authorities and institutions designated by relevant laws.

13.2. Compliance of the employees of CryptoWallet., its structural units and MLRO with the requirements of the Money Laundering and Terrorist Financing Prevention Act and the legislation established on the basis thereof is monitored and controlled by the management board of the undertaking, senior manager or MLRO.

13.3. The competence of the employees of CryptoWallet. to comply with the requirements of the Money Laundering and Terrorist Financing Prevention Act and the legislation established on the basis thereof:

13.3.1. only those employees who have been authorized to do so by the management board or the senior manager and who have thoroughly familiarised themselves with the relevant legislation, information issued by the competent authorities, with these rules of procedure and have exhaustive knowledge in the field of AML/KYC may handle operations related to the fulfilment of requirements and obligations arising from the Money Laundering and Terrorist Financing Prevention Act and of the legislation established on the basis thereof, including the implementation of due diligence, whereby only those employees also have the right to decide on the initiation, creation and continuation of business relationships;

13.3.2. in matters related to the fulfilment of requirements and obligations arising from the Money Laundering and Terrorist Financing Prevention Act and of the legislation established on the basis thereof, the employees and heads of structural units of CryptoWallet. primarily consult with the MLRO and, in the absence of such person, with the responsible member of the management board. The senior manager always has the right to control the activities of the employees, heads of structural units and MLRO of CryptoWallet..

13.4. The employees and heads of structural units of CryptoWallet. undertake to strictly comply with:

13.4.1. International Sanctions Act;

13.4.2. Money Laundering and Terrorist Financing Prevention Act;

13.4.3. Directive (EU) 2015/849 of the European Parliament and of the Council;

13.4.4. relevant instructions and orders of the Financial Intelligence Unit and other competent authorities;

13.4.5. procedural rules and internal control rules established by the management board of CryptoWallet.;

13.4.6. relevant and legal orders and instructions of the management board, senior manager and MLRO of CryptoWallet..

13.5. If an employee (or the manager of a structural unit) has a doubt as to whether a due diligence measure or other related criterion has been met (or the execution of a transaction or the establishment of business relations is permitted) - the employee (or the head of a structural unit) must immediately contact their immediate superior (head of a structural unit, MLRO, senior manager) and suspend the transaction or business relationship until they receive an answer to their request and an order on how to behave.

13.6. CryptoWallet. implements the following system of internal control over compliance with 14.6.2. Money Laundering and Terrorist Financing Prevention Act and the legislation established on the basis thereof and the requirements of these procedural rules and internal control standards:

13.6.1. The activities of the employees of CryptoWallet. are monitored and controlled by:

13.6.2. the head of the structural unit of the employee;

13.6.3. in the absence of the head of the structural unit of the employee, the senior manager and/or MLRO.

13.7. The employee must transmit to the head of the structural unit or, in the absence thereof, to the senior manager and/or to the MLRO all relevant data concerning the identities of the clients of CryptoWallet. and the nature of the business relations established with them, including the client's personal data, data of the transaction carried out with the client, the results of the implementation of due diligence measures and other important information at the latest on the next working day after the completion of data collection and implementation of due diligence.

13.8. The activities of the head of a structural unit of CryptoWallet. are monitored and controlled by the senior manager of CryptoWallet. and/or to the MLRO.

13.9. The head of the structural unit of CryptoWallet. must transmit to the MLRO or the responsible member of the board at least once a month all relevant data collected by them or the employees of their structural unit on the identities of the clients of CryptoWallet. and the nature of the business relations established with them, together with relevant reports.

13.10. The activities of the MLRO of CryptoWallet. are monitored and controlled by the senior manager or management board.

13.11. The MLRO checks the relevant data provided by the employees and heads of structural units of CryptoWallet. on the identities of the clients of CryptoWallet. and the nature of the business relationships established with them and organizes the storage of this data in accordance with the provisions of the Money Laundering and Terrorist Financing Prevention Act and this code of conduct. The MLRO submits relevant reports to the management board of CryptoWallet. once per quarter.

13.12. The activities of the senior manager of CryptoWallet. are monitored and controlled by other board members or, in exceptional cases, by the general meeting of shareholders.

13.13. In the event of a temporary absence of the MLRO, the senior manager or the person temporarily appointed by them checks the relevant data provided by the employees and heads of structural units of CryptoWallet. on the identities the clients of CryptoWallet. and the nature of the business relationships established with them, and organizes the storage of this data in accordance with the provisions of the Money Laundering and Terrorist Financing Prevention Act and this code of conduct.

13.14. The senior manager and the management board of CryptoWallet. undertake to inform the employees of the undertaking on an ongoing basis about changes in legislation and new positions of supervisory institutions, the activities of CryptoWallet., changes in its risk assessments and criteria arising from clients or certain client groups, changes in the long- and short-term business approach of the undertaking and separate positions and guidelines (according to the market situation, political and economic situation, orders of supervisory bodies, etc.) to fulfil the obligations arising from the Money Laundering and Terrorist Financing Prevention Act. Said information and notices do not necessarily have to be formalized as appendices to this manual and may be delivered at meetings, through individual managers, by e-mail, but they must be complied with and followed regardless of the delivery method.

13.15. Breach of the duty of care arising from the Money Laundering and Terrorist Financing Prevention Act, failure to comply with the order of the senior manager, management board or MLRO, or failure to inform the senior manager, management board, MLRO or the Financial Intelligence Unit in case of suspicion of money laundering or terrorist financing, either directly or through the head of the structural unit, is sufficient grounds for initiating disciplinary proceedings against the employee and/or head of structural unit and to terminate the employment relationship.

13.16. The management board of CryptoWallet. ensures that the resources allocated for ensuring compliance with the Money Laundering and Terrorist Financing Prevention Act and the requirements of this code of conduct are sufficient and that the employees directly involved in fulfilling the requirements of the Money Laundering and Terrorist Financing Prevention Act operate in conditions where they are fully aware of the requirements of the Money Laundering and Terrorist Financing Prevention Act and this code of conduct.

13.17. CryptoWallet. must carry out an internal audit. During the internal audit, adherence to procedural rules, compliance with internal control standards and the functioning of systems are also checked. The internal auditor is subject to the requirements and legal bases of the activity provided for the certified internal auditor in the Auditors Activities Act. The internal auditor checks the compliance of the activities of CryptoWallet. and its managers and employees with legislation, regulations of the Financial Intelligence Unit, decisions of management bodies, internal regulations, contracts signed by the virtual currency service provider and good practice.

13.18. The virtual currency service provider guarantees the internal auditor all the rights and working conditions necessary for the performance of their duties, including the right to receive explanations and information from the managers and employees of the virtual currency service provider and to monitor the elimination of discovered deficiencies and the implementation of suggestions made.

13.19. The internal auditor is obliged to immediately forward in writing to the managers of the virtual currency service provider and the Financial Intelligence Unit any information that has become known to them about the virtual currency service provider and which points to violations of the law or damage to the interests of clients.

14. RECORD KEEPING

14.1. In line with the regulations CryptoWallet. has developed this record keeping rules that highlights an approach to record keeping. This approach is applicable to all Clients and Clients' activity. All employees are expected to adhere to the principles highlighted in this policy

14.1.1. client Verification information;

14.1.2. CDD/ EDD checks;

14.1.3. details of beneficial ownership;

14.1.4. transactional data and evidence;

14.1.5. records of suspicious activity;

14.1.6. internal reports to the MLRO;

14.1.7. external reports to FIU or relevant authority;

14.1.8. the practice's risk assessment;

14.1.9. the practice's compliance checks;

14.1.10. policies and Procedures change data;

14.1.11. other required information in accordance with Anti-Money laundering regulations

14.2. In addition to the data specified in this code of conduct, the employee of CryptoWallet. records the following data about the transaction to be performed:

14.2.1. transaction type; unique transaction identifier; transaction price; transaction period; sending or recipient account number; other special transaction conditions.

14.3. All mention records will be retained for at least five years from the end of the business relationship or the date of the transaction as applicable. CryptoWallet. is storing the mentioned information with the following 3rd party service providers:

14.3.1. SumSub - data related to customer KYC, CDD, EDD, screening against sanctions, domestic and international PEPs, adverse media, data related to Crypto monitoring and screening

14.3.2. PKO Bank Polski - data related to fiat transactions

14.3.3. Fireblocks - data related to the crypto transactions and risk flags

14.3.4. Zendesk - data related to the conversions with clients

14.3.5. Only responsible management and a person designated by responsible management have access to the stored data.

15. FINAL PROVISIONS

15.1. This Anti-Money Laundering (AML) policy may be amended or updated from time to time as required by changes in laws, regulations, or best practices. Any amendments made will be communicated to all relevant parties and will take effect immediately upon publication.

15.2. All employees and relevant stakeholders of CryptoWallet. are expected to comply with this AML policy and its provisions. Non-compliance may result in disciplinary action, including termination of employment or business relationships.

15.3. All information obtained and records maintained in accordance with this AML policy will be treated with the utmost confidentiality. Access to such information will be restricted to authorised personnel on a need-to-know basis, and appropriate safeguards will be implemented to protect against unauthorised access or disclosure.

15.4. CryptoWallet. fully cooperates with relevant regulatory authorities and law enforcement agencies in any investigations or inquiries related to money laundering or terrorist financing activities. This includes providing requested information, reporting suspicious transactions, and implementing necessary measures to assist in the prevention and detection of financial crimes. At the first request of an employee of the Financial Intelligence Unit, all documents necessary for the inspection must be submitted to the inspectors.

15.5. If any provision of this AML policy is found to be invalid, illegal, or unenforceable, the remaining provisions shall remain in full force and effect

Confirmed by the management board of CryptoWallet on 10th February 2024: Aleksei Arno, MLRO.

Signature:

APPENDIX 1 TO AML POLICY
SUPPORTED CRYPTOCURRENCIES

Token name	Abbreviature	Official information	SUMSUB KYT monitoring support
Tether USDt	USDT	https://coinmarketcap.com/currencies/tether/	yes
Tether EURt	EURT	https://coinmarketcap.com/currencies/tether-eurt/	yes
TrueUSD	TUSD	https://coinmarketcap.com/currencies/trueusd/	yes
USDD	USDD	https://coinmarketcap.com/currencies/usdd/	yes
DAI	DAI	https://coinmarketcap.com/currencies/multi-collateral-dai/	yes
BITCOIN	BTC	https://coinmarketcap.com/currencies/bitcoin/	yes
LITECOIN	LTC	https://coinmarketcap.com/currencies/litecoin/	yes
ETHEREUM	ETH	https://coinmarketcap.com/currencies/ethereum/	yes
CARDANO	ADA	https://coinmarketcap.com/currencies/cardano/	yes
XRP	XRP	https://coinmarketcap.com/currencies/xrp/	yes
NEAR PROTOCOL	NEAR	https://coinmarketcap.com/currencies/near-protocol/	yes
SPEND	SPEND	TOKEN https://cryptowallet.com/	yes
BNB	BNB	https://coinmarketcap.com/currencies/bnb/	yes
AVALANCHE	AVAX	https://coinmarketcap.com/currencies/avalanche/	yes
TRON	TRX	https://coinmarketcap.com/currencies/tron/	yes
POLYGON	MATIC	https://coinmarketcap.com/currencies/polygon/	yes
POLKADOT	DOT	https://coinmarketcap.com/currencies/polkadot-new/	yes
ALGORAND	ALGO	https://coinmarketcap.com/currencies/algorand/	yes
DOGECOIN	DOGE	https://coinmarketcap.com/currencies/dogecoin/	yes
SOLANA	SOL	https://coinmarketcap.com/currencies/solana/	yes

APPENDIX 2 TO AML/KYC POLICY
CUSTOMER RISK ASSESSMENT

1. INTRODUCTION

CryptoWallet evaluates AML/CTF risk by implementing the risk-based approach and considering national and supranational risk assessments, as well as recommendations and guidelines of the Financial Action Task Force (FATF), European Banking Authority (EBA), and other international and local Laws and regulations.
CryptoWallet has created this CRA to explain how it assesses inherent risks across its individual customers. Individual Customer risk assessment is updated where necessary based on the guidelines issued by European supervisory authorities, FATF as well as the published results of the European Commission's supranational risk assessment, National risk assessment, guidelines, and reports issued by the FIU. The risks inevitably vary from customer to customer, but the risks considered by CryptoWallet follow the risks set out in the legislation of the EU :

- Customer Risk;
- Country and/or Geographical Risk;
- Transaction Risk;
- Delivery channel Risk.

CryptoWallet must conduct appropriate due diligence prior to establishing a business relationship with a client. In order for the Company to determine an appropriate level of due diligence it must conduct an inherent risk rating of the client and determine the level of ongoing monitoring.

2. CRA METODOLOGY

CryptoWallet considers that every client presents a certain degree of risk, which will be apparent on the assessment criteria set out below. To identify, assess and prevent the potential ML/TF or Sanctions risks of a client a granular and objective risk assessment should be performed.
Section 4 below sets out how inherent risk should be calculated for all clients based on:

- Customer Risk;
- Country and/or Geographical Risk;
- Transaction Risk;
- Delivery Channel Risk.

To determine the inherent risk level of the individual Customer and have adequate control measures to mitigate the risk, CryptoWallet applies individual risk assessment. The company performs an individual risk assessment of the Customer ML/TF risk in the following cases:

- Before the establishment of the business relationship with the customer;
- On an ongoing basis according to the initially assigned risk level to the customer.

The inherent individual risk assessment of the customer and the risk level attributed should be periodically reviewed and updated. Unless there is a specific change of circumstance, risk level assigned should be updated on a risk-based approach as follows:

Inherent Risk Assessment	Inherent Risk Update
Low Risk	Every 3 Years
Moderate Risk	Every 2 Years
High Risk	Every 1 Year

A change of circumstances for the purposes of the above will include, but is not limited to:

- A possible match related to PEP, relevant Adverse Media or Sanctions;

- A new service/product is provided to the customer which usage might lead to increase of the risk of the customer;
- There is a significant deviation in the customer's behaviour from the information that the company obtained during the customer's onboarding;
- The unusual transaction pattern is detected during ongoing monitoring of the customer.

The inherent risk level of the customer can be changed (increased or decreased) because of the re-assessment of the risk, based on the results of the ongoing monitoring of the business relationship and/or new factors relating to the customer. If the recalculation of customer's inherent risk results in a change of risk from low or moderate to high, approval to continue the relationship will be required from the AML Officer and subsequently EDD will be performed.

3. CRA SCORING METHODOLOGY

The score of all risk factors in the CryptoWallet CRA is derived from the combination of (i) the risk level, which is attributed to the selected option (multiple choices within the risk factors), and (ii) the impact level, which is attributed to the risk factor.
For each question that has a "prohibited", "high risk", "moderate risk" or "low risk" score, the following numerical scores are given by the CRA:

- Prohibited (the client is deemed prohibited / outside of company's risk appetite);
- High (score of 9);
- Medium (score of 3);
- Low (score of 1).

In addition, every risk factor has an attributed impact level, which depends on the importance of the risk factor in the evaluation of the inherent customer's risk based on the type of risk being assessed, as follows:

- Customer risk (the risk factor score multiplied by 40%);
- Screening risk (the risk factor score multiplied by 30%);
- Transaction risk (the risk factor score multiplied by 15%); and
- Delivery channel risk (the risk factor score multiplied by 15%).

The sum of all evaluated risk factors equals to the inherent customer's risk score.
The Inherent customer's risk score as set out in the CRA is described by the formula (and explained more in detail) below.

$Z = Sum(a + b + c + d)$, where

- a – sum of score of questions 1.1-1.3
- b – sum of score of questions 2.1-2.3
- c – score of the question 3.1
- d - score of the question 4.1
- Z =Inherent Customer's Risk Score

The Inherent customer's risk score as well as customer's inherent risk level is calculated based on the information provided in the CRA and presented on the right side of the CRA.
If there are any concerns related to ML/TF risks associated with the customer and there are additional criteria not listed in the Customer risk assessment tool, Compliance department employees, as well as AML Officer, has a right to overrule the recommendation of the risk assessment tool in case there is a motivated opinion that the customer's risk level is higher than it is recommended by the risk scoring. Such decisions should be approved by AML Officer and recorded in the internal log of the company.
Each risk factor has more than one option to select. A number of options has been assigned to one of the three risk levels (from Low to High or Prohibited) for example:

2.1 Country of residence	Use 'x' to select
What is the risk level of the country where customer resides?	
Low	
Medium	
High	
Prohibited	

Figure 1 Low, Moderate, High, Prohibited Risk Options

Alternatively, three risk levels (from Low to High):

2.3 Customer type	Use 'x' to select
What is the employment status?	
Employed	
Student	
Unemployed	

Figure 2 Low, Moderate or High-Risk Options

In addition, each risk factor has a different impact on the risk (either 40%, 30% or 15%). The impact level (assigned to the risk factor) depends on the importance of the risk factor in the overall evaluation of the customer's risk. The impact has been decided based on the guidance set out in Wolfsberg Guidance for calculating risk assessments for the purposes of AML assessments[1].

Furthermore, and as indicated above, in line with the CryptoWallet AML Policy there are number of prohibitions assigned to each risk factor which returns an automatic prohibition of the customer and a rejection of the business relationship.

1.3 Match in the sanctions list	Prohibited
Have any true matches in the sanctions lists been detected?	
Yes	x
No	

Figure 3 Prohibited.

In order to aid objectivity, the majority of the questions have been designed to be answered by placing an "x" next to pre-defined answers. If the analyst attempts to answer a question with two answers, an error message stating "Select only one" pops up.

2. Customer Information	Fill in the Form
2.1 Country of residence	Select only one
What is the risk level of the country where customer resides?	
Low	x
Medium	x
High	
Prohibited	

Figure 4 Select only one error.

1

4. CLIENT RISK ASSESSMENT- CONSIDERATIONS AND METHODOLOGY

CryptoWallet enters into business relationships with individual customers. An AML Officer is responsible for the individual risk assessment process. A risk assessment together with the risks posed by the customer must be presented to the senior management who decides on the acceptance of high-risk customers and provides the written approval for onboarding the customer or continuing the business relationships with the customer. The approval should be documented and added to the customer's file.
If the customer is considered High Risk based on the inherent risk assessment, Enhanced Due Diligence ('EDD') measures must be applied. Prohibited countries are outlined in Appendix 4

Individual clients and users of CryptoWallet Services will be screened against sanctions lists through a third-party provider. CryptoWallet uses AML service provider – Sum&Sub for customers' screening against sanctions lists to ensure that we are compliant with international financial sanctions regulations. All the customers will be automatically screened against the relevant sanctions lists of designated persons after client details are introduced in the CryptoWallet 's internal IT systems. The clients would be deemed as Prohibited if they will:

- have matches in the sanctions lists;
- will reside in the prohibited country;
- will fail to be verified by CryptoWallet.

CryptoWallet uses the AML service providers – SumSub as identification and verification tools for individual clients. In case a third-party provider fails to verify the documents provided by the client, the compliance team of CryptoWallet will perform a manual check. Therefore, a couple of verification methods with different risk levels were introduced to the Risk Assessment tool. CDD and EDD processes are described in detail in the CryptoWallet AML Policy.

5. INHERENT RISK CALCULATION

Once the client is assessed by CryptoWallet through the CRA, the score is calculated automatically in the CRA Excel and the final risk score is presented to ascertain the inherent risk score of the client. There are no exceptional circumstances and no manual override on the CRA process other than requesting exemptions from the AML Officer at CryptoWallet and Moorwand in relation to prohibited criteria. Based on the result from the CRA, CryptoWallet takes the decision whether to onboard the client or not. Scores of customer Risk Rating for CryptoWallet clients is indicated below:

Customer Risk Rating		From	To
Risk Rating	Low	2.55	4
	Moderate	4.05	7
	High	7.05	15.2
	Prohibited	Prohibited	Prohibited

Figure 5 Individual CRA Scoring

6. RISK APPETITE

In conjunction with the risk mitigation system established in the provisions of the model for identifying the client's risk level, the management board of CryptoWallet determines the risk level of CryptoWallet to be moderate. CryptoWallet does not establish business relationships with persons against whom prohibitions are stipulated by this guide of conduct and its appendices or by law and/or with respect to whom there is a suspicion that the client will use the services of CryptoWallet in money laundering, tax evasion, terrorist financing or criminal activity schemes or to facilitate them but does not create additional obstacles in regards to the use of their services by clients with respect to whom there are no such doubts. CryptoWallet primarily avoids client relations if:

6.1. a client cannot be identified;

6.2. due diligence resulting from the Money Laundering and Terrorist Financing Prevention Act cannot be applied to the client for any reason
6.3. the client is located in a prohibited country
6.4. the client is subject to European Union or UN sanctions;
6.5. the client has Politically exposed person history
6.6. the client has previously been punished pursuant to criminal procedure for money laundering, tax evasion, terrorist financing or criminal activities that can be directly or indirectly associated with credit fraud or virtual currencies or is facing criminal proceedings and the obliged person has Information about this;
6.7. also, CryptoWallet intends to minimize the number of high-risk clients by avoiding creating business relationships with people who might be politically exposed persons and persons aged 65 years and over.
6.8. In relation to the remaining clients with whom the obliged person does not exclude the establishment of business relationship, the obliged person shall establish due diligence measures resulting from the Money Laundering and Terrorist Financing Prevention Act and the procedural rules and internal according to the client's risk level to mitigate risks, by assessing the overall risk level of the client using the risk assessment and management model set out in this appendix and paying heightened attention to each risk level category of the client

ATTACHMENT 3 TO AML/KYC POLICY
INDIVIDUAL CRA EXPLAINING THE EVALUATION CRITERIA

1. SCREENING RISK

Initially each client is assigned a risk score depending on the risk factors listed below:

Risk Factor	Explanation	Prohibited	Low	Moderate	High
Adverse Media	Have any true adverse media (negative news) matches concerning financial crime been detected relating to the customer?	n/a	No	Yes, but unverifiable	Yes, verifiable
Match in the PEP list	Have any true matches in the PEP lists been detected?	Yes	No	n/a	n/a
Match in the sanctions list	Have any true matches in the sanction's lists been detected?	Yes	No	n/a	n/a

In order to answer the questions of the Screening Risk Factor part of the Individual CRA, the following should be used as a guide:

1.1. CryptoWallet uses a third-party screening tool to check all the customers – when customers register in the system, the information is transmitted to the provider and checked for negative adverse media, PEP matches and matches in the sanctions lists. CryptoWallet is prohibited from working with PEPs and Sanctioned individuals.

1.2. In case there is a positive match in sanctions lists the result will be prohibited which should result in the CRA being halted. If any question is unanswered or answered in an incorrect manner (i.e. wrong input – only 'x/X' letter will return the score; two boxes are checked, etc.), then it will not be possible to proceed with the inherent risk calculation.

2. CUSTOMER RISK

Risk Factor	Explanation	Prohibited	Low	Moderate	High
Country of residence	What is the risk level of the country where customer resides? (according to Geo and IP checks performed)	Prohibited	Low	Moderate	High
Relationships with the client	How long has the client been registered with the company?	N/A	Less than 1 year	From 1 to 3 years	More than 3 years
Customer type	What is the employment status?	N/A	Employed	Student	Unemployed

In order to answer the questions of the Customer Risk Factor part of the Individual CRA, the following should be used as a guide:

2.1. CryptoWallet has agreed to follow Moorwand Guide on Countries, which has the list of countries divided by risk rating based on the information obtained from different reliable sources. In addition, CryptoWallet performs the following checks of geo-location for its individual customers:

- IP address;
- Device identifiers;
- Virtual accounts wallet addresses.

2.2. The longer the customer has relationships with CryptoWallet, the lower risk will be assigned.

2.3. CryptoWallet will evaluate customers with different employment positions. Furthermore, there are no prohibited statuses.

If any questions is unanswered or answered in an incorrect manner (i.e. wrong input – only 'x/X' letter will return the score; two boxes are checked, etc.), then it will not be possible to proceed with the inherent risk calculation.

3. TRANSACTION RISK

Risk Factor	Explanation	Prohibited	Low	Moderate	High

Transaction risk	What is the estimated value of the transactions performed during 1 month?	N/A	X < 5,000 EUR	5,000 EUR< X < 10,000 EUR	10, 000 EUR < X < 20,000 EUR

In order to answer the questions of the Transaction Risk Section of the CRA, the following should be used as a guide:

3.1. CryptoWallet decided to categorize the customers according to their monthly transaction volume within CryptoWallet's limits. There are no prohibited limits; however, customers should provide an explanation for any necessary limit adjustments.

3.2. If the question is unanswered or answered in an incorrect manner (i.e. wrong input – only 'x/X' letter will return the score; two boxes are checked, etc.), then it will not be possible to proceed with the inherent risk calculation.

4. VERIFICATION RISK/DELIVERY CHANNEL

Verification Risk, for the purpose of CryptoWallet's business, the Company takes into account how the customers were verified during the onboarding stage. If CryptoWallet employees are unable to complete the CDD measures on the customer it will not be possible to carry out an accurate CRA, onboarding should cease, and business relationships cannot be established. The following question and answers were created to assess the delivery risk related to customer:

Risk Factor	Explanation	Prohibited	Low	Moderate	High
Verification of the customer's identity	How was the customer's identity verified?	Not verified	Via eKYC tool	n/a	Via manual verification

In order to answer the question of the Verification Risk Factor part of the Individual CRA, the following should be used as a guide:

4.1. As CryptoWallet has contracted a third-party provider to complete identification and verification of the customers, it is important to receive the information from the provider on the ongoing basis. In case the provider failed to verify the identity of the customer, manual checks should be applied by CryptoWallet dedicated team. Therefore, manual verification of the documents was assigned High Risk. In case the verification by both methods fails, the customer should be assigned "Prohibited" risk rating and all the business relationships should be ended.

4.2. If the question is unanswered or answered in an incorrect manner (i.e. wrong input – only 'x/X' letter will return the score; two boxes are checked, etc.), then it will not be possible to proceed with the inherent risk calculation.

APPENDIX 4 TO AML POLICY
SUPPORTED COUNTRIES AND ADDITIONAL AML/KYC PROCEDURES.

To ensure the highest standards of security, legality, and regulatory compliance, CryptoWallet has implemented additional Anti-Money Laundering (AML) and Know Your Customer (KYC) procedures. These measures are specifically designed to mitigate the risks associated with client jurisdiction and planned activities with CryptoWallet. Their purpose is to prevent fraud, money laundering, and other illicit activities connected with specific regions and countries

1. REGULATORY SOURCES

1.1. EU – High risk third countries and the International context content of anti-money laundering and countering the financing of terrorism (https://finance.ec.europa.eu/financial-crime/high-risk-third-countries-and-internationalcontext-content-anti-money-laundering-and-countering_en)

1.2. UN – Restrictive measures (https://www.sanctionsmap.eu/#/main)

1.3. FATF – FATF – Jurisdictions under Increased Monitoring – June 2023 (https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-othermonitored-jurisdictions/Increased-monitoring-june-2023.html)

1.4. Internal decision on high-risk and prohibited countries by CryptoWallet.

2. SUPPORTED COUNTRIES

CryptoWallet services are available to customers in specific jurisdictions. The following list outlines the supported countries where our services can be used and accessed. This list is subject to change and will be updated as necessary.

LOW RISK			MEDIUM RISK			HIGH RISK		
Austria	AT	AUT	Albania	AL	ALB	United Arab Emirates	AE	ARE
Belgium	BE	BEL	Argentina	AR	ARG	Bulgaria	BG	BGR
Cyprus	CY	CYP	Canada	CA	CAN	Croatia	HR	HRV
Czech Republic	CZ	CZE	Australia	AU	AUS	Indonesia	ID	IDN
Denmark	DK	DNK	Brazil	BR	BRA	Mexico	MX	MEX
Estonia	EE	EST	Armenia	AM	ARM	Montenegro	ME	MNE
Finland	FI	FIN	Azerbaijan	AZ	AZE	Philippines	PH	PHL
Malta	MT	MLT	Bhutan	BT	BTN	Qatar	QA	QAT
Portugal	PT	PRT	Chile	CL	CHL	South Africa	ZA	ZAF
France	FR	FRA	Costa Rica	CR	CRI	Sri Lanka	LK	LKA
Germany	DE	DEU	Kenya	KE	KEN	Turkey	TR	TUR
Greece	GR	GRC	Ecuador	EC	ECU	Serbia	RS	SRB
Hungary	HU	HUN	El Salvador	SV	SLV	Botswana	BW	BWA
Iceland	IS	ISL	Columbia	CO	COL	Macedonia	MK	MKD

Ireland	IE	IRL	Faroe Islands	FO	FRO	Monaco	MC	MCO
Italy	IT	ITA	Georgia	GE	GEO			
Latvia	LV	LVA	India	IN	IND			
Romania	RO	ROM, ROU	Israel	IL	ISR			
Lithuania	LT	LTU	Malawi	MW	MWI			
Luxembourg	LU	LUX	Malaysia	MY	MYS			
Netherlands	NL	NLD	Malta	MT	MLT			
Norway	NO	NOR	Moldova	MD	MDA			
Poland	PL	POL	Namibia	NA	NAM			
Slovakia	SK	SVK	Nepal	NP	NPL			
Slovenia	SI	SVN	New Zealand	NZ	NZL			
Spain	ES	ESP	Peru	PE	PER			
Sweden	SE	SWE	Singapore	SG	SGP			
Liechtenstein	LI	LIE	Thailand	TH	THA			
Switzerland	CH	CHE	Ukraine	UA	UKR			
			Zambia	ZM	ZMB			
			Japan	JP	JPN			
			Mauritius	MU	MUS			
			Uruguai	UY	URY			
			Åland Islands	AX	ALA			
			Brunei darussalam	BN	BRN			
			South Korea	KR	KOR			

3. TYPES OF VERIFICATION PROCEDURES FOR SUPPORTED COUNTRIES

3.1. CryptoWallet applies the following measures for low-and medium-risk countries:

3.1.1. Basic Customer Due Diligence:

3.1.1.1. Identity verification

3.1.1.2. Liveness check

3.1.1.3. Residence address collection

3.1.1.4. Sanction/PEP/Adverse Media initial and ongoing screening

3.1.1.5. Additional measure: Customer Due Diligence questionnaire

3.1.2. CryptoWallet may apply Enhanced Due Diligence measures at any time for clients from low- and medium-risk countries at its sole discretion. Alternatively, if a client from a low- or medium-risk country is determined to have a high-risk level based on the results of a risk assessment, they may be granted a high-risk status

3.2. CryptoWallet applies the following measures for High risk countries:

3.2.1. Enhanced Customer Due Diligence:
3.2.1.1. Identity verification
3.2.1.2. Liveness check
3.2.1.3. Sanction/PEP/Adverse Media initial and ongoing screening
3.2.1.4. Residence address collection and verification with Proof of address
3.2.1.5. Additional measure : Enhanced Due Diligence questionnaire
3.2.1.6. Additional measure : Source of Funds or Source of wealth based on clients expected turnover

4. ADDITIONAL VERIFICATION MEASURES

4.1. In addition to undergoing the Customer Due Diligence process for low- and medium-risk countries and Enhanced Due Diligence for High-Risk Countries during the initial account registration and establishment of the client relationship, clients are required to complete a comprehensive questionnaire. This questionnaire is specifically designed to gather detailed information regarding the client's planned activities in connection with CryptoWallet Services. The purpose of this thorough inquiry is to ensure a precise understanding of the client's needs, objectives, and the intended use of our services

4.2. For low- and medium-risk countries, CryptoWallet applies a questionnaire to collect from client the following information:
4.2.1. The client should indicate what his main purpose is for using CryptoWallet services;
4.2.2. The client should indicate his expected monthly turnover with CryptoWallet services.
4.2.3. The client should indicate his current occupation and annual income.
4.2.4. The client should indicate his source of funds (cryptocurrency /fiat currency).

4.3. For high-risk countries, CryptoWallet applies as part of Enhanced Due Diligence Procedure a questionnaire to collect from client the following information and documentation:
4.3.1. The client should indicate what their main purpose is for using CryptoWallet services;
4.3.2. The client should indicate his expected monthly turnover with CryptoWallet services.
4.3.3. The client should indicate his current occupation and annual income.
4.3.4. The client should indicate his source of funds (cryptocurrency /fiat currency).
4.3.5. The client should provide documentation that confirms his source of funds or source of wealth
4.3.6. The client should indicate whether he is a Politically Exposed Person (PEP), a family member of a PEP, or a close associate of a PEP.
4.3.6.1. If the answer is yes, the client should clarify what type of PEP he is.
4.3.7. The client should indicate whether he currently performs or has previously performed business activities.
4.3.7.1. If the answer is yes, the client should clarify the type of activity and the company involved

5. RESTRICTED COUNTRIES

5.1. The use of CryptoWallet services in certain jurisdictions is restricted or prohibited due to legal and regulatory considerations. Currently prohibited country list:

Algeria	DZ	DZA
Cayman Islands	KY	CYM
Afghanistan	AF	AFG
Belarus	BY	BLR
Bouvet Island	BV	BVT
Central African Republic	CF	CAF
Congo	CG	COG

Congo democratic republic	CD	COD
Ethiopia	ET	ETH
French Guiana	GF	GUF
French Southern territories	TF	ATF
Iran	IR	IRN
Democratic people's republic of Korea	KP	PRK
Libya	LY	LBY
Nicaragua	NI	NIC
Palestine	PS	PSE
Russia	RU	RUS
Sint Eustatius	BQ	BES
South Sudan	SS	SSD
Syria	SY	SYR
Bahamas	BS	BHS
Bonaire	BQ	BES
Christmas Island	CX	CXR
Cuba	CU	CUB
Falkland Islands	FK	FLK
French Polynesia	PF	PYF
Guinea-Bissau	GY	GUY
Iraq	IQ	IRQ
Lebanon	LB	LBN
Myanmar	MM	MMR
Pakistan	PK	PAK
Panama	PA	PAN
Saba=Bonaire and Sint Eustatius	BQ	BES
Somalia	SO	SOM
Sudan	SS	SSD
Trinidad and tobago	TT	TTO
Yemen	YE	YEM
Jordan	JO	JOR
China	CN	CHN
puerto rico	PR	PRI
United States	US	USA
Venezuela	VE	VEN
Western Sahara	EH	ESH
Kosovo	QZ	QZZ
Mali	ML	MLI
Zimbabwe	ZW	ZWE
Egypt	EG	EGY
Guam	GU	GUM
Guinea Bissau	GW	GNB
Haiti	HT	HTI

Honduras	HN	HND
Virgin Islands, British	VG	VGB
Bangladesh	BD	BGD
Crimean Peninsula		
Donetsk Region		
Luhansk Region		
Zaporizhzhia		
Kherson		
Hong Kong	HK	HKG
Kerch		
Transnistria region		
Tunisia	TN	TUN
Saudi Arabia	SA	SAU
Tonga	TO	TON
Vanuatu	VU	VUT
Guyana	GY	GUY
Wallis and Futuna	WF	WLF
Tuvalu	TV	TUV
Mozambique	MZ	MOZ
Saint vincent and the grenadines	VC	VCT
Senegal	SN	SEN
Bosnia and Herzegovina	BA	BIH
Burundi	BI	BDI
Darfur = western Sudan	SD	SDN
Ghana	GH	GHA
Laos	LA	LAO
Antarctica	AQ	ATA
Bouvet islands	BV	BVT
Eritrea	ER	ERI
South georgia and the south sandwich islands	GS	SGS
Heard island and mcdonald islands	HM	HMD
United Kingdom	GB	GBR
Barbados	BB	BRB
Burkina Faso	BF	BFA
Cameroon	CM	CMR
Gibraltar	GI	GIB
Jamaica	JM	JAM
Niger	NE	NER
Nigeria	NG	NGA
Tanzania	TZ	TZA
Uzbekistan	UZ	UZB
Vietnam	VN	VNM
Uganda	UG	UGA

Morocco	MA	MAR
Swaziland=Eswatini	SZ	SWZ
British indian ocean territory	IO	IOT
American Samoa	AS	ASM

6. COUNTRY RISK REVIEW:

6.1. Periodic review:

6.1.1. The country risk list will be subject to regular reviews at least every 6 months to assess the current geopolitical and economic landscape.

6.2. Emerging Risks:

6.2.1. The list will be updated promptly in the event of emerging risks or significant changes in the political, economic, or security conditions of a country.

6.3. Regulatory Changes:

6.3.1. Any changes in international regulations or sanctions that impact the risk profile of a country will prompt an immediate review and update of the list.