Anti-Money Laundering (AML) and Know Your Client (KYC) Policy

Introduction

APZONE LIMITED and/or **Chainroll Limited** ("we", "our", or "us") is committed to preventing money laundering and complying with relevant laws and regulations aimed at combating financial crimes. This Anti-Money Laundering (AML) and Know Your Client (KYC) Policy ("AML/KYC Policy") outlines our approach to identifying and mitigating the risks associated with money laundering, terrorist financing, and other illicit activities. Please read this Policy carefully before using https://remozo.com website and our services.

Compliance with Laws and Regulations

This AML/KYC Policy is an excerpt of our internal Anti-money laundering and counter terrorist financing compliance guidelines. We adhere to all applicable laws, regulations, and guidelines related to AML and KYC, including but not limited to:

- The Financial Action Task Force (FATF) Recommendations
- The European Union's Anti-Money Laundering Directives
- The Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 up to 2023.
- Other relevant regulatory requirements in jurisdictions where we operate.

Client Due Diligence (CDD)

We conduct thorough Client Due Diligence (CDD) processes to verify the identity of our customers and assess the risks associated with their activities. Our CDD procedures may include:

- Identifying the Client and verifying its identity using reliable, independent sources, documents or data, including e-identifying;
- Identifying and verifying of the representative of the Client and the right of representation;
- Identifying the Client's Beneficial Owner;
- Assessing and obtaining information on the purpose of the Business Relationship;
- Conducting ongoing DD on the Client's business to ensure the Provider of service's knowledge of the Client and its source of funds is correct;
- Obtaining information whether the Client is a PEP or PEP's family member or PEP's close associate;
- Obtaining information whether International Sanctions are imposed against the Client, Beneficial Owner, representative, director and other persons that may be relevant.

Identification of a person Upon implementing DD measures the following person shall be identified:

- Client – a natural person or a legal entity.

- Representative of the Client – an individual who is authorized to act on behalf of the Client.
- Beneficial Owner of the Client.
- The Politically Exposed Person (PEP) – if the PEP is the Client or a person connected with the Client.

Upon establishing the relationship with the Client we shall identify and verify the Client by using information technology means, and follow technical requirements for the customer identification process for remote identification authentication via electronic devices for direct video transmission. Consequences of insufficient identification of a Client:

- Promptly apply the enhanced DD measures pursuant to the guidelines;
- Notify the Money Laundering Reporting Officer (MLRO) of the failure to implement normal CDD in a timely manner;
- Assess the risk profile of the Client and notify MLRO;
- Suspicious activity should be monitored and assessed postnote.

To comply with the CDD obligation, we have the right and obligation to:

- request documents and information regarding the activities of the Client and legal origin of funds;
- request appropriate identity documents to identify the Client and its representatives;
- request information about Beneficial Owners of a Client;
- screen the risk profile of the Client, select the appropriate CDD measures, assess the risk whether the Client is or may become involved in money laundering (ML) or terrorist financing (TF);
- re-identify the Client or the representative of the Client, if there are any doubts regarding the correctness of the information received in the course of initial identification;
- refuse to participate in or carry out the activity on our platform if there is any suspicion that the activity on our platform is linked with ML or TF, or that the Client or another person linked with the activity on our platform is or could be involved in ML or TF.

The objective of the continuously applied CDD measures is to ensure on-going monitoring of Clients and their activity on our platform.

We update the data of a Client, i.e. takes appropriate CDD measures, every time when:

- upon identification and verification of the information;
- based on data renewal terms which may vary depending on the risk group to which particular Client is assigned to;
- we has learned through third persons or the media that the activities or data of the Client have changed significantly;
- the data pertaining to the activity of Client reveal significant changes in the Client's area of activity or business volumes, which warrants amending the Client's risk profile.

Enhanced Due Diligence (EDD)

In cases where higher risks are identified, we may implement Enhanced Due Diligence (EDD)

measures to gather additional information about customers and their activity on our platform. This may include obtaining more extensive documentation, conducting background checks, and obtaining approval from senior management before establishing or continuing the business relationship.

Activity Monitoring and Reporting

We monitor customer activity on our platform for unusual or suspicious activities that may indicate potential money laundering or terrorist financing. If such activities are detected, we promptly report them to the relevant authorities as required by law.

Prohibited activity

The Client shall use our services solely in compliance with its Terms of Use, including this KYC/AML Policy, solely for his or her own account. The Client shall not sell, lease or otherwise provide access to the services to any third party.

The following conduct and activity are prohibited:

- The Client does not have sufficient authorizations to carry out the activity on our platform, or the authorizations are unclear;
- The Client's need to carry out the activity on our platform has not been reasonably justified;
- The Client is a fictitious person;
- The Client or the representative of the Client refuses to provide information for the purposes of establishing the substance of the activity on our platform and assessment of the risks;
- The Client has not presented sufficient data or documents to prove legal origin of the assets and funds, after having been asked to do so;
- Based on the information received from recognized and reliable sources (e.g. state authorities, international organizations, media) the Client, the Beneficial Owner of a Client, or another person associated with the Client (e.g. director, representative) is or has been linked with organized crime, ML or TF, tax evasion, bribery or corruption;
- The Client, the Beneficial Owner of a Client, or another person associated with the Client is or has been linked with sources of income of organized crime, i.e. illicit traffic of excise goods or narcotic substances, illegal trafficking of arms or human trafficking, mediation of prostitution, unlicensed international transfers of e-money;
- International Sanctions are being applied against the Client, the representative or the Beneficial Owner;
- The Client advocates, promotes or assists any violence or any unlawful act.

Implementation of International Sanctions.

We conduct screenings and draw special attention to all its Clients (existing and new), to their activities and to the facts and indicators which refer to the possibility that the Client is a subject to International Sanctions in force including but not limited to European Union sanctions, U.S. Office of Foreign Assets Control sanctions and other sanctions that we determine necessary to implement.

Restricted Jurisdictions

Albania, Afghanistan, The Bahamas, Barbados, Botswana, Burkina Faso, Cambodia, Cayman Islands, Cuba, Democratic Republic of Korea (DPRK), Haiti, Ghana, Jamaica, Iran, Iraq, Gibraltar, Mauritius, Morocco, Myanmar, Nicaragua, Pakistan, Panama, Philippines, Senegal, South Sudan, Syria, Trinidad and Tobago, Uganda, Vanuatu, Yemen, Angola, Burundi, Central African Republic, Congo, Congo (Democratic Republicof the), Guinea-Bissau, Liberia, Libya, Mali, Sierra Leone, Somalia, Côte d'Ivoire, Zimbabwe.

We reserve the right to choose markets and jurisdictions in which it operates, and may also restrict or refuse provision of its services in other countries, territories or regions if deemed necessary by its own risk appetite or required by laws, competent authorities or sanctions programs. You should inform us immediately if you become a resident in any of the Restricted jurisdiction. You understand and acknowledge that if it is determined that you have given false representations of your location or place of residence, we reserve the right to take any appropriate actions with compliance to the local jurisdiction, including termination of your access to our services.

Risk Assessment

We conduct risk-assessment of its activities and Clients, and establish a risk profile of a Client based on information gathered under the guidelines and apply relevant level of due diligence measures accordingly.

Data Security and Confidentiality

We maintain strict controls over customer data to ensure confidentiality and prevent unauthorized access. Client's information is only shared with authorized personnel on a need-to-know basis and is protected by appropriate security measures. For more information please refer to our Privacy Policy.

The originals or copies of the documents, which serve as the basis for identification of a person, and of the documents serving as the basis for establishing a business relationship, shall be stored for at least eight (8) years after the expiry of the business relationship or the completion transaction. Information regarding reported activity shall be stored by the MLRO.

Compliance Monitoring and Review

We conduct regular reviews and assessments of our AML and KYC policies, procedures, and controls to ensure they remain effective and compliant with applicable laws and regulations. We update our policies and procedures as necessary to address emerging risks and changes in the regulatory environment.

Reporting Violations

We encourage employees, customers, and other stakeholders to report any concerns or suspected violations of our AML/KYC Policy and procedures. Reports can be made anonymously, and we prohibit retaliation against individuals who report concerns in good faith.

Contact Us

If you have any questions or concerns about our AML/KYC Policy, please contact us at info@remozo.com .

Effective Date.

This AML/KYC Policy is effective as of 01/08/2024.