Introduction.

The purpose of CoinFlip Exchange Sp. z o.o.'s Anti-Money Laundering and Counter-Terrorist Financing and Know Your Customer Policy *(hereinafter — the **'AML/CTF Policy')*** is to identify, prevent, and mitigate possible risks of involvement of the Cryptocurrency Exchange Platform CoinFlip Exchange Sp. z o.o.com ***('CoinFlip Exchange Sp. z o.o.')*** in any illegal, fraudulent, or any other prohibited activities across the applicable jurisdictions.

CoinFlip Exchange Sp. z o.o. commits to strict adherence to Know Your Customer ***(KYC)*** and AML/CTF laws and regulations, affirming our pledge to avoid willful violations of KYC and AML policies. Within reasonable control, CoinFlip Exchange Sp. z o.o. shall implement requisite measures and technology to furnish services that are inherently safe and secure, thereby maximizing protection against financial loss due to money laundering.

Our Know Your Customer (KYC) and AML/CTF policies constitute an extensive framework comprising international standards, encompassing the specific KYC and AML regulations applicable to respective jurisdictions.

Through our robust compliance infrastructure, CoinFlip Exchange Sp. z o.o. diligently upholds regulatory requisites and standards, both at local and global levels, thereby ensuring the sustained operational integrity of our Platform, namely:

- a Know Your Customer (**KYC)** and Know Your Business (**KYB**) verification obligations, that include identification of the customer *(natural person or legal entity)*, beneficial owners (if any), and the nature and purpose of the business relationship; and
- an obligation of constant vigilance of the transactions initiated by the User to detect fraudulent behavior and/or criminal activity of the User. The legislation requires that the intensity of the vigilance be adapted according to the risk profile of the User or the transaction. A Suspicious Activity Report (SAR) must be filed with the competent authorities when any operation of the User is suspected to be criminal activity, fraudulent behavior, etc.

CoinFlip Exchange Sp. z o.o. has implemented effective internal procedures following international and local regulations in different jurisdictions where CoinFlip Exchange Sp. z o.o. is legally operating to prevent money laundering, terrorist financing, drug, and human trafficking, the proliferation of weapons of mass destruction, corruption, and bribery and to react correspondingly in case of any form of criminal activity from the users of CoinFlip Exchange Sp. z o.o. platform *(hereinafter the – **'Customers', 'Users'**).*

Money Laundering.

Money Laundering, as defined by international regulations and legislation aimed at preventing money laundering and terrorist financing, encompasses the following:

1. Altering the legal status of Digital assets or transferring them, with the knowledge that these assets stem from criminal activity or by engaging in such activity, intending to conceal or obscure their illicit origins or to aid any individual involved in criminal activity in evading legal repercussions. Additionally, engaging in or being involved in an arrangement, knowing or reasonably suspecting,

or having reason to suspect, that the arrangement facilitates the acquisition, retention, use, or control of criminally obtained assets.
2. Concealing or disguising the true nature, origin, source, location, disposition, movement, ownership, or other rights on the property, while being aware that said property is derived from criminal activity or by participating in such activity.
3. Acquiring, managing, or utilizing property while knowing, at the time of acquisition or transfer, that the said property originates from a criminal act or by participating in such activity constitutes an offense. Regardless of attempts made to conceal or disguise the criminal origin of the property, it remains unlawful to acquire, use, or possess such criminally derived property. Importantly, this offense does not necessitate active engagement in the laundering process.
4. Engaging in preparatory actions, attempting to commit, or being complicit in any of the actions outlined in clauses *1.*, 2., and *3.* of this section is also considered an offense.

Money laundering necessitates distinct criminalization apart from predicate offenses. This entails that the acts involving the concealment of the origins of Digital assets derived from illegal activities constitute an independent crime, mandating prosecution regardless of the preceding criminal activity.

AML/CTF Policy outlines three fundamental stages of money laundering:

- **Placement**: involves the introduction of unlawfully acquired funds into the financial system;
- **Layering**: focuses on distancing illicit funds from their source through intricate financial transactions by blurring the lines of communication, moving money through multiple accounts, financial operations, or jurisdictions to obscure its origin.
- **Integration**: reintroduction of laundered funds into the legal economy without being linked to its illegal origin, achieved through investments or purchases that create the appearance of lawfully obtained wealth.

COINFLIP EXCHANGE SP. Z O.O. MAINTAINS A STRICT ZERO-TOLERANCE APPROACH TOWARDS MONEY LAUNDERING, TERRORIST FINANCING, CORRUPTION AND BRIBERY, TAX EVASION, INDEPENDENT OF ANY PREDICATE OFFENSE.

CoinFlip Exchange Sp. z o.o. is obligated to notify the designated Regulatory Authorities as stipulated by relevant international Anti-Money Laundering (AML) frameworks *(such as FNTT; NCA; AUSTRAC; FINTRAC; FAU, etc.)* no later than one working day upon becoming aware or harboring concerns. This obligation applies when there is knowledge or concern that assets, regardless of their value, have been acquired directly or indirectly from a criminal act or involvement in such activities. Similarly, it applies if there is knowledge, or we suspect that these assets are linked to the financing of terrorist activities, in adherence to international AML standards.

Terrorist Financing.

Terrorist Financing, refers to the deliberate provision or collection, by any means, directly or indirectly, of funds intended or knowingly used to facilitate terrorist acts. It involves legitimate entities or individuals providing funds to support terrorist activities or organizations for ideological, political, or other motivations.

Terrorist financing is the process of legitimate businesses and individuals that may choose to provide funding to resource terrorist activities or organizations for ideological, political or other reasons.

CoinFlip Exchange Sp. z o.o. is obliged to ensure that its Users:

- *are not designated as terrorist organizations;*
- *not facilitating the funding of terrorist organizations.*

Tax evasion, Tax Fraud

Tax evasion and Tax fraud represent intentional efforts to avoid paying the full amount of taxes owed to the government. They encompass deceitful actions aimed at sidestepping tax obligations, whether entirely or partially. Tax fraud involves a purposeful intent to deceive and involves identifiable material components.

The offense of tax fraud can be constituted:

- *voluntary omission or deliberate error in declarations;*
- *concealment of taxable amounts;*
- *organizing insolvency to evade Tax payment; or*
- *employing other tactics to hinder Tax collection.*

Bribery and Corruption.

Bribery and Corruption encompass actions wherein an individual improperly offers, promises, or provides an undue advantage to influence another person's conduct of their duties. This undue advantage may be in the form of monetary or non-monetary benefits and is intended to induce the recipient to perform, delay, or neglect their duties, thereby acting in a manner contrary to principles of honesty and integrity. Conversely, it constitutes a corrupt practice for an individual to accept or seek such an advantage in the context of their responsibilities.

Special attention should be directed towards individuals susceptible to engaging in corrupt practices. Notably, those leveraging their influence for personal gain perpetrate acts of money laundering when they Deposit or utilize funds received improperly or convert advantages acquired through their authoritative positions into monetary assets.

AML/CTF Regulation.

Internation legislation that regulates AML/CTF Policy of CoinFlip Exchange Sp. z o.o.:

- ***International Convention for the Suppression of Terrorist Bombings*** – Adopted by the United Nations General Assembly on December 15, 1997.
- ***United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*** – Held in Vienna on December 20, 1988.

- ***United Nations Convention against Transnational Organized Crime*** – Adopted by the United Nations General Assembly resolution 55/25 on November 15, 2000.
- ***The Basel Declaration*** – Approved on December 28, 1988, by the Basel Committee on Banking Regulation and Supervision.
- ***Financial Action Task Force (FATF) 40 Recommendations*** – Established in a report by FATF on February 6, 1990, in Paris. These recommendations, last updated in February 2023, focus on preventing money laundering and countering terrorist financing.
- ***Commission Delegated Regulation (EU) 2016/1675*** – July 14, 2016, supplementing Directive (EU) 2015/849 of the European Parliament and of the Council. It identifies high-risk third countries with strategic deficiencies.
- ***Fourth Anti-Money Laundering Directive (Directive 2015/849/EU)*** – Enacted on May 20, 2015, aimed at preventing the use of the financial system for money laundering or terrorist financing. It amends Regulation (EU) No 648/2012 of the European Parliament and of the Council and repeals Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJEU 5 June 2015, No. L 141/73).
- ***Fifth Anti-Money Laundering Directive (Directive 2018/843/EU)*** – Enacted on May 30, 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or terrorist financing, and Directives 2009/138/EC and 2013/36/EU.

Risk-Based Approach.

CoinFlip Exchange Sp. z o.o. employs a risk-based approach in its AML/CTF strategy to manage risks inherent in its operations, utilizing a standardized risk rating model for assessing money laundering exposure across User relationships. This approach is tailored following the nature, scale, and complexity of its business activities.

Through this risk-based methodology, CoinFlip Exchange Sp. z o.o. consistently identifies and evaluates AML/CTF risks inherent in its operations. By comprehensively understanding these risks, CoinFlip Exchange Sp. z o.o. can discern vulnerable areas within its operations and implement appropriate AML/CTF measures to effectively mitigate these identified risks.

When applying a risk-based approach, CoinFlip Exchange Sp. z o.o. will:

- *identify the money laundering risks that are relevant to the business activities;*
- *carry out a detailed risk assessment of the business, focusing on the risk factors as described by the money laundering regulations;*
- *carry out a risk assessment of both existing and prospective Users;*
- *design and put in place controls to manage and reduce the impact of the real and emerging risks;*
- *monitor the controls and improve their efficiency;*
- *keep records of what we did, including the reasons behind our actions.*

Customer Due Diligence (CDD).

Customer Due Diligence (CDD) is key to understanding the AML/CTF compliance procedures on CoinFlip Exchange Sp. z o.o.

Customer Due Diligence (CDD) aims to fortify the financial services sector against exploitation for money laundering or terrorist financing. Acquiring comprehensive information about Users and effectively utilizing this data stands as the primary defense mechanism to prevent the facilitation of illicit funds laundering.

CoinFlip Exchange Sp. z o.o. is mandated to conduct thorough CDD and ongoing monitoring to ascertain User identities, determine any third-party involvement, ensure compliance with legal requirements for service provisions, and facilitate cooperation with law enforcement by providing available information on Users or activities under investigation.

Overview of CDD measures:

- **Identifying the User and Verifying Identity:** This involves collecting pertinent information to establish the User's identity through reliable and independent sources. It includes obtaining details such as name, address, date of birth, and official identification documents;
- **Identifying the Beneficial Owner and Verifying Identity, where relevant:** If applicable, determining and verifying the identity of the beneficial owner(s) who ultimately own or control the User. This measure ensures transparency regarding ownership and control structures;
- **Obtaining Information on the Purpose and Intended Nature of the Business Relationship:** Gaining a clear understanding of the purpose, intended nature, and expected regularity of the business relationship. This includes understanding the types of transactions or activities anticipated to be conducted within the business relationship;
- **Monitoring and Ongoing Due Diligence:** Continuous monitoring of User transactions and activities to detect any Abnormal activity, Unusual behavior or Questionable conduct. This involves setting up systems to observe transactions regularly and implementing mechanisms to trigger further investigation if activities appear irregular;
- **Risk Assessment, Risk Profiling, and Risk-Based Approach:** Conduct risk assessments to evaluate and categorize Users based on the level of risk they pose, based on factors like industry sector, geographical location, and the nature of transactions undertaken. Applying a risk-based approach ensures that resources are allocated appropriately to manage higher-risk Users more vigilantly while reducing unnecessary burdens on lower-risk ones;
- **Legal and Regulatory Compliance:** Ensuring that the User complies with all relevant legal and regulatory frameworks, including industry-specific regulations and anti-money laundering laws.
- **Enhanced Due Diligence (EDD):** Implementing additional checks and measures for higher-risk Users or transactions. This might include seeking additional documentation, obtaining senior management approval for business relationships, or conducting more frequent reviews of high-risk activities;
- **Record-Keeping and Documentation:** Maintaining comprehensive records of all customers' due diligence processes, including User information, identity verification documents, risk assessments, and transaction records. This documentation is crucial for regulatory compliance and audit purposes;
- **Training and Awareness Programs:** Providing regular training to staff members involved in CDD processes to ensure they are equipped with the knowledge and tools to effectively carry out due diligence procedures. This helps in maintaining a culture of compliance and vigilance throughout the organization;
- **Transaction Monitoring Systems:** Implementing automated AML/CTF systems, software and services that continuously analyze and monitor transactions for Abnormal activity, Unusual behavior or Questionable conduct. These systems employ algorithms and thresholds to detect anomalies that might indicate potential money laundering activities;

- **Adverse Media Screening:** Conducting searches across various media sources to identify any negative or adverse information related to Users or beneficial owners. This helps in assessing potential risks associated with the individuals or entities involved;
- **Politically Exposed Persons (PEPs) Screening:** Screening Users to identify whether they are Politically Exposed Persons, individuals entrusted with prominent public functions. This additional scrutiny helps in assessing the associated risks and applying appropriate due diligence measures;
- **Geographic Risk Assessment:** Evaluating risks associated with specific geographic locations or jurisdictions. Some regions might pose higher risks due to weak AML/CTF regulations or higher prevalence of financial crime, necessitating tailored due diligence measures;
- **Collaboration and Information Sharing:** Engaging in collaborations or partnerships with other financial institutions or authorities to share insights and intelligence on emerging risks or criminal activities, enabling a collective effort in combatting financial crimes.

CoinFlip Exchange Sp. z o.o. often requires more than just the User's identity; it necessitates a deeper understanding of the User's business activities. This knowledge is essential to accurately assess the alignment between the transactions and activities conducted with or through the company and the nature of the User's business. Evaluating the consistency of these transactions with the User's declared business activities is fundamental in ensuring robust risk assessment and compliance measures.

Know Your Customer (KYC) and Know Your Business (KYB).

Upon establishing a business relationship, it is essential for CoinFlip Exchange Sp. z o.o. to discern the expected nature of a User's business activities to define normal operational patterns. As the relationship progresses, any routine transactions conducted by the User are evaluated against the anticipated activity. Any deviations or unexplained activities are scrutinized to ascertain potential indications of money laundering or terrorist financing.

At the initiation of the relationship, personal information including nationality, date of birth, and residential address is collected. These data points are pivotal in evaluating the risk of financial crimes, including Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CTF). In cases involving high-risk transactions, it may be necessary to verify the information provided by the User.

In the case when the User is a legal entity (company), the Know Your Business (KYB) compliance procedure becomes more stringent and is contingent upon factors such as the company's structure, location, and other relevant aspects. The identification of the company's ownership, authorized representatives, domicile, and nature of business is required.

Due to variations in governmental documentation standards for legal entities across different jurisdictions, the verification process for such Users is conducted through Enhanced Due Diligence (EDD) procedures, significantly increasing time consumption.

Source of Funds.

Verification of the source of funds, including how the payment is made, its origin, and the entity making the payment, is a fundamental aspect of every transaction in terms of CoinFlip Exchange Sp. z o.o. adhering to AML/CTF laws and regulations. Compliance procedures of CoinFlip Exchange Sp. z o.o. maintain a stringent practice of ensuring complete knowledge regarding the source of funds at the onset of any User relationship.

Users are expected to substantiate the accumulation of funds through documentation, such as statements or evidence of specific transactions, such as inheritances or insurance payouts.

Moreover, CoinFlip Exchange Sp. z o.o. actively requests clarification on the source of funds due to compliance reasons regarding its legal nature. Legitimate sources of funds encompass various lawful origins, including:

- ***Employment-related Income:*** *Such as wages, bonuses, dividends, and other earnings arising from employment activities.*
- ***Retirement Benefits:*** *Including pension payments and similar retirement-related income.*
- ***Savings and Investments:*** *Comprising interest earned from personal savings accounts and returns from various investments.*
- ***Proceeds from Asset Transactions:*** *Such as money from property sales or other legitimate asset disposals.*
- ***Genuine Windfalls:*** *Including legitimately won money from betting, lottery wins, or similar forms of luck-based winnings.*
- ***Inheritances and Gifts:*** *Lawfully acquired funds received through inheritance or as gifts*

Illegitimate sources of funds, on the other hand, include money gained through terrorism, fraud, bribery, laundered money, and so on.

Prohibited activities.

CoinFlip Exchange Sp. z o.o. regularly reviews the list of activities defined as prohibited. CoinFlip Exchange Sp. z o.o. prohibits any operations related to the following activities:

- *Drugs and drug paraphernalia (e.g., narcotics, controlled substances, and any equipment designed for making or using drugs);*
- *Marijuana/cannabis dispensaries and related products and businesses;*
- *Weapons, munitions, gunpowder, and other explosives (including fireworks);*
- *Toxic, flammable, and radioactive materials;*
- *Pseudo-pharmaceuticals, Substances designed to mimic illegal drugs;*
- *Sexually explicit content, Sexually-related services;*
- *Pyramid and investment schemes, multi-level marketing schemes, and other unfair, predatory or deceptive practices;*
- *Items used for speculation or hedging purposes (such as derivatives);*
- *Credit and collection services;*
- *Items that infringe or violate any intellectual property rights such as copyrights, trademarks, trade secrets, or patents, including counterfeit or unauthorized goods;*
- *Products and services with varying legal status from state to state;*
- *Transactions that disclose the personal information of third parties in violation of applicable law;*

- *Transactions related to cloud-mining;*
- *Transactions involving sanctioned entities;*
- *Any other business activity which, in our sole discretion, is outside our risk appetite.*

Enhanced Due Diligence (EDD).

CoinFlip Exchange Sp. z o.o. must apply EDD measures on a risk-sensitive basis in any situation that by its nature can present a higher risk of money laundering or terrorist financing. As part of this, CoinFlip Exchange Sp. z o.o. may conclude, under its risk-based approach, that the standard evidence of identity is insufficient concerning the money laundering or terrorist financing risk, and that it must obtain additional information about a particular User.

The extent of additional information sought, and of any ongoing monitoring carried out in respect of any particular User, or category of the User, will depend on the money laundering or terrorist financing risk that the User, or category of User, is assessed to present to CoinFlip Exchange Sp. z o.o..

CoinFlip Exchange Sp. z o.o. has a policy of doing EDD on all Users due to the business being non-face-to-face. This includes monitoring all transactions, monitoring IP addresses, and reviewing all crypto wallets that CoinFlip Exchange Sp. z o.o. interacts with both Deposits and Withdrawals. CoinFlip Exchange Sp. z o.o. reviews the EDD process on an ongoing basis, and the CCO completes a quarterly report for the board to assess any issues and update on any potential improvements.

CoinFlip Exchange Sp. z o.o. also completes further due diligence when:

- Dealing with natural persons or legal entities established in the countries identified as high-risk countries;
- The background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions which have no apparent economic or lawful purpose.
- Any account that has large transactional activity.
- Dealing with Users who may be Politically Exposed Persons, on Sanctions lists, or have Adverse Media.

The monitoring of the degree and nature of the business relationship shall be increased in order to determine whether those activities or transactions appear unusual or questionably criminal.

Politically Exposed Persons (PEP's) Screening

To ensure that CoinFlip Exchange Sp. z o.o. is aware of any Users who would be designated as PEP or be on a sanctions list, CoinFlip Exchange Sp. z o.o. has decided to have all Users checked by independent external screening tools.

A Politically Exposed Person (PEP), is a natural person who is or who has been entrusted with prominent public functions and includes the following:

(a) *heads of State, heads of government, ministers, and deputy or assistant ministers;*

(b) *members of parliament or of similar legislative bodies;*

(c) *members of the governing bodies of political parties;*

(d) *members of supreme courts, of constitutional courts, or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;*

(e) *members of courts of auditors or the boards of central banks;*

(f) *ambassadors, chargés d'affaires, and high-ranking officers in the armed forces;*

(g) *members of the administrative, management, or supervisory bodies of State-owned enterprises;*

(h) *directors, deputy directors, and members of the board or equivalent function of an international organization.*

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials.

Politically Exposed Person's (PEP) Family members include the following:

(a) *the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;*

(b) *the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;*

(c) *the parents of a politically exposed person. 'Persons are known to be close associates' means*

(d) *natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;*

(e) *natural persons who have 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.*

CoinFlip Exchange Sp. z o.o. has decided that Politically Exposed Persons (PEPs), their Family members, and known close associates of PEPs **do not fall within the risk appetite**, and as such, CoinFlip Exchange Sp. z o.o. **does not allow these types of Users** to have access to CoinFlip Exchange Sp. z o.o. products/services.

Sanctions Policy.

In alignment with our commitment to maintaining robust Anti-Money Laundering and Counter-Terrorist Financing practices and compliance with applicable laws and regulations, as well as international financial Sanctions, CoinFlip Exchange Sp. z o.o. enforces a stringent Sanctions Policy regarding the freezing of transactions involving sanctioned entities or suspected violations of sanctions, as well as the suspension/terminations of use of our services by the Users, involved in such activities.

CoinFlip Exchange Sp. z o.o. takes all required steps to ensure that all Users with whom a business relationship is established are screened against relevant notices published by: **United Nations Sanctions (UN); US Consolidated Sanctions; OFAC – Specially Designated Nationals (SDN); EU Financial Sanctions; UK Financial Sanctions (HMT); Australian Sanctions; Switzerland Sanction List – SECO; INTERPOL Wanted List; Consolidated Canadian Autonomous Sanctions List; Office of the Superintendent of Financial Institutions (Canada); Bureau of Industry and Security (US); Department of State, AECA Debarred List (US); Department of State, Nonproliferation Sanctions (US)**, and others.

CoinFlip Exchange Sp. z o.o. ensures the maintaining of compliance with all regulatory, legislative, economic, and financial sanction requirements, and the performing sanctions screening on all Users and third parties before commencing business relationships and, on an ongoing basis during the life-cycle of the relationship.

CoinFlip Exchange Sp. z o.o. Sanctions Policy strictly prohibits any engagement with Users involved in money laundering or terrorist financing. This applies when the CoinFlip Exchange Sp. z o.o. becomes aware of or suspects potential involvement in such activities or when the User relationship poses an unacceptable level of sanctions risk.

If CoinFlip Exchange Sp. z o.o. harbors uncertainty regarding a User's potential status under financial sanctions or suspects a specific transaction by the User violates financial sanctions, CoinFlip Exchange Sp. z o.o. will initiate a suspension procedure and implement Due Diligence measures, including:

- gather additional information to ascertain the User's potential involvement in financial sanctions or the potential violation of financial sanctions in a transaction or activity. This involves verifying data, documents, or information from a credible and independent source.
- acquiring further details about the nature and purpose of the business relationship, transaction, or activity. CoinFlip Exchange Sp. z o.o. may request additional documentation from the User, such as Proof/Source of Funds or Proof of Transaction Origin, identity documents, request Photo/Video-verification materials, liveness check and validate these materials using credible and independent sources.
- in cases where there's a risk or suspicion of a violation of this Sanctions Policy, CoinFlip Exchange Sp. z o.o. will rigorously apply Enhanced Due Diligence measures.
- freeze the funds and economic resources of the subject of international financial sanctions and suspend or terminate the User access to CoinFlip Exchange Sp. z o.o. products and services.

If, after implementing Due Diligence measures, CoinFlip Exchange Sp. z o.o. confirms that a User is indeed subject to financial sanctions or that the transaction or activity of such User violates financial sanctions, or if additional information obtained through Enhanced Due Diligence fails to conclusively determine this, or in the event of suspected financial sanction violations, CoinFlip Exchange Sp. z o.o. will freeze funds involved in such transaction and suspend the User, promptly reporting such findings or suspicions to the relevant regulatory authorities.

Additionally, if during the Due Diligence procedure, CoinFlip Exchange Sp. z o.o. identifies that a transaction or operation of the User involves a sanctioned entity or another third party associated with sanctions — such as a Deposit from such a sanctioned entity or its associated third party — the User bears full responsibility for this transaction and/or operation, assumes complete accountability

for its execution, subsequent Due Diligence procedures concerning the operation, potential freezing of funds involved in said transaction, and further suspension of the User.

High-Risk Countries.

Government and international agencies issue details of countries whose financial or social systems are such that they are likely to pose a high risk of money laundering. The rules require additional 'due diligence' checks to be carried out when dealing with individuals or money hailing from these countries. In addition, they require these checks to pay regard to the specific shortcomings or concerns highlighted by the national or international bodies.

The usage of the CoinFlip Exchange Sp. z o.o. products/services is prohibited for citizens and/or residents of the following countries (territories) and jurisdictions*: **Afghanistan, American Samoa, U.S. Virgin Islands, Territory of Guam, Iran, Yemen, Libya, State of Palestine, Puerto Rico, Somalia, the Democratic People's Republic of Korea, The Northern Mariana Islands, USA, Syria, Russian Federation, Republic of Belarus, Republic of Sudan, Transnistria, temporarily occupied territories of Georgia, Turkish Republic of Northern Cyprus, Western Sahara, Federal Republic of Ambazonia, Kosovo, South Sudan, Canada, United Kingdom, Nicaragua, Trinidad and Tobago, Venezuela, Myanmar, and temporarily occupied territories of Ukraine.**

**Please be advised that the above list of prohibited and high-risk jurisdictions is subject to continual revision by CoinFlip Exchange Sp. z o.o. per current laws and regulations, and consequently, it is your responsibility to verify the latest version available on our Website.*

Customer Transaction Monitoring.

After a User's onboarding, CoinFlip Exchange Sp. z o.o. conducts comprehensive transaction monitoring procedures. Utilizing internally developed automated fraud prevention and risk management systems, CoinFlip Exchange Sp. z o.o. employs vigilance measures throughout the business relationship.

The vigilance measures encompass:

- **Transaction Monitoring:** Constantly monitoring customer-initiated transactions to identify any that appear unusual, fraudulent, or otherwise criminal, or deviate from typical patterns based on our understanding of the User and the business relationship's risk profile. This vigilance involves automated and manual transaction monitoring tools using predefined criteria, parameters, and thresholds;
- **Sanctions Compliance:** Monitoring and assessing transactions involving sanctioned individuals or entities in alignment with recognized Sanctioned Lists;
- **Regular Customer File Updates:** Periodically updating User files following the established KYC/AML risk periodicity for each User;
- **Risk Rating Updates:** Updating the User's risk rating during each review or following a triggering event, such as significant changes in the business relationship *(e.g., a User becoming a Politically Exposed Person (PEP)*, Adverse Media and third-party alerts or as necessitated for handling alerts or enhanced reviews;

- **Validation of High-Risk Operations:** Seeking appropriate validation for high-risk operations in terms of AML/CTF compliance procedures.

Continuous vigilance during the relationship may prompt modifications to the assigned rating and the implementation of heightened surveillance when transactions are Red-flagged as atypical (e.g., STRs, alerts, and multiple enhanced reviews).

Furthermore, CoinFlip Exchange Sp. z o.o. **reserves the right to prohibit both incoming and/or outgoing questionable or sanctioned transactions *(or transactions executed from/to/by sanctioned entities)***. This includes freezing funds involved in such transactions and suspending and/or terminating access to CoinFlip Exchange Sp. z o.o.'s products/services.

Red-flags, Abnormal activity, Unusual behavior, or Questionable conduct

A transaction that may trigger Red-flags, Abnormal activity, Unusual behavior, or Questionable conduct often deviates from the User's established legitimate business or personal activities, or from the customary transactions typical for that particular User profile. Thus, the primary element in identification is possessing adequate knowledge about the User's business to discern any unusual or irregular transaction or a series of transactions.

CoinFlip Exchange Sp. z o.o. gathers proof of the destination of funds and the beneficiary's identity from Users. Additionally, the origin of funds and the transaction's purpose are obtained.

While a document *(e.g., bank statement, cash declaration)* aiding in establishing the funds' origin *(e.g., inheritance, real estate sale)* might be provided, it alone may not suffice to justify the source of funds. Declarations or attestations provided by the User within the business relationship may not be considered conclusively adequate.

If CoinFlip Exchange Sp. z o.o. encounters User opposition, refusing to disclose relevant evidence citing business or professional secrecy, CoinFlip Exchange Sp. z o.o. treats this as grounds for questions. In this scenario, doubts persist, establishing concerns due to the unremoved doubt.

In the field of AML/CTF international laws and regulations mandate our adherence to all aforementioned compliance procedures, including the collection of all necessary additional documents and information from Users, as a part of our AML/CTF policies.

AML Compliance Officer (Money Laundering Reporting Officer (MLRO).

The responsibility of the AML Compliance Officer (Money Laundering Reporting Officer (MLRO), duly authorized by CoinFlip Exchange Sp. z o.o., is to oversee and ensure the effective implementation of Anti-Money Laundering/Counter-Terrorist Financing (AML/CTF) measures. This includes the obligation to report any breaches of AML/CTF protocols and manage the collection and submission of Suspicious Activity Reports (SARs).

The AML Compliance Officer's duties encompass comprehensive supervision of all facets related to CoinFlip Exchange Sp. z o.o.'s AML/CTF efforts. These responsibilities extend to, but are not restricted to:

- Establishing and regularly updating internal policies and procedures in adherence to relevant laws and regulations. This involves managing the completion, review, submission, and retention of mandated reports and records.
- Collecting Users' identification information, verifying provided data, and implementing a record management system for proper document storage and retrieval.
- Gathering and analyzing information concerning unusual transactions or suspected criminal activity, money laundering, or terrorist financing activities.
- Conducting investigations into any unusual or criminal activity identified.
- Promptly reporting of money laundering or terrorist financing to the appropriate authorities and providing necessary information in compliance with regulations.
- Periodically providing written statements to the management board, affirming compliance with legal requirements.
- Organizing specialists' training programs to ensure awareness and compliance.
- Fulfilling other duties and obligations pertinent to legal compliance requirements.
- Regularly updating the risk assessment to align with evolving circumstances and regulatory changes.

The Compliance Officer is entitled and authorized to interact with the competent Law Enforcement and Regulatory authorities, which are involved in the prevention of money laundering, terrorist financing, and other illegal activity.

AML/CTF Training.

CoinFlip Exchange Sp. z o.o. specialists undergo comprehensive AML/CTF training coupled with job-specific guidance. This training is conducted at least once every six (6) months to ensure specialists are well-informed and adhere to all pertinent laws and regulations. Additional training is administered as needed, such as in the event of new laws or regulations, or as mandated by legal requirements.

The AML/CTF Training Program undergoes regular updates to align with the latest laws and regulations, ensuring its relevance and compliance with current standards.

Record-Keeping and Documentation.

CoinFlip Exchange Sp. z o.o. will retain the following records for a 5 (five) consecutive years after the termination of the User relationship:

- *Copies of or references to evidence obtained regarding a User's identity and details of User trading activities for 5 (five) years from the date of the relevant transaction.*
- *All User communications, including emails or recorded calls.*

Additionally, CoinFlip Exchange Sp. z o.o. will maintain internal records for 5 (five) years, which include:

- *Records documenting all AML/CTF Training sessions delivered.*
- *Details outlining actions taken concerning both internal and external reports.*
- *Information reviewed by the AML Compliance Officer or their nominee in relation to an internal report where no external report is filed.*

CoinFlip Exchange Sp. z o.o. will ensure strict adherence to these requirements, ensuring that the documents can be furnished upon request.

Amendments and Final provisions.

This AML/CTF Policy is effective as of the date of publishing on our Website and will remain in effect except concerning any changes in its provisions in the future, that come into force and will be applied immediately after they are published on the website.

We may update and/or change the terms of this AML/CTF Policy, and it is your responsibility to monitor all relevant updates to this document.

If you disagree with this AML/CTF Policy, then you should refrain from using our Website, mobile application, and/or Services or opening an Account. This AML/CTF Policy is an integral part of our User Agreement.

If you have any questions regarding this AML/CTF Policy, please contact our AML Department at