# AML/CFT Policy

Last updated: 10.01.2025

This Anti-Money Laundering and Combating the Financing of Terrorism Policy (AML/CFT Policy) (the "Policy") has been adopted by Paypilot (hereinafter referred to as “Paypilot“, “we“, “Company”) to prevent the use of its products and services for money laundering and terrorist financing activities. The Company is committed to complying with all applicable laws, regulations, and guidance regarding AML and Combating the Financing of Terrorism (CFT). This AML/CFT Policy is an essential part of our Terms of Use.

## 1. Purpose

This Policy is intended to protect the Company from being used as a tool for illegal activities such as money laundering or terrorist financing by establishing guidelines for identifying and mitigating the risks of such activities in its interactions with External Parties. The Policy sets out specific procedures that the Company will follow to achieve this goal, including the implementation of robust client and business partner identification processes, ongoing Transaction Monitoring to detect Suspicious Activity, and mandatory Reporting of any Suspicious Activity to the relevant authorities. By taking these steps, the Company will be better equipped to safeguard its Reputation, protect its assets, and avoid any implication in Financial Crime.

The Policy also set out the specific responsibilities of employees, senior management and the Board of Directors in ensuring that the company's AML/CFT Compliance program is effective and up to date. Additionally, it also provides the company's internal controls and procedures for ensuring Compliance with applicable laws, regulations, and standards. It also includes the requirement for the Company to conduct regular internal audits, Risk Assessments, and Training Programs for employees to ensure that they are aware of their responsibilities and the company's AML/CFT Compliance program.

Overall, the goal of this Policy is to ensure that the Company is able to identify and prevent any illegal activities from taking place within its operations and to maintain the integrity of its Financial Systems by adhering to the best practices for Anti-Money Laundering and Combating the Financing of Terrorism.

## 2. Scope

This Policy is designed to ensure that the Company is compliant with laws and regulations related to money laundering and terrorist financing, and that it is not unknowingly involved in any illegal activities. To achieve this, the Company will conduct Due Diligence on all External Parties with which it has relationships. This will involve evaluating potential risks and assessing the Reputation and past behavior of these parties to ensure that they are not involved in any illegal activities.

The Company will also establish procedures for identifying and Reporting Suspicious Activity, and for verifying the identity of Users and other External Parties. This includes implementing know-your-customer/know-your-business (KYC/KYB) procedures and Anti-Money Laundering (AML) protocols. Additionally, the Company will ensure that its employees are trained to recognize and report Suspicious Activity, and that they are aware of the company's policies and procedures in this regard.

The Policy outlines the steps and procedures the Company will take to evaluate and manage the risks associated with External Parties, including conducting Due Diligence, implementing KYC/KYB and AML protocols, and training employees to recognize and report Suspicious Activity. The goal is to ensure that

the Company is not unknowingly involved in any illegal activities and is in Compliance with all laws and regulations related to money laundering and terrorist financing.

3. Definitions

- AML/CFT laws and regulations: The laws, regulations and guidance related to Anti-Money Laundering and Combating the Financing of Terrorism that the Company is committed to comply with.
- Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Compliance Program: The Company's internal program for ensuring Compliance with AML and CFT laws and regulations.
- Audits and Assessments: Regular internal Audits and Risk Assessments to ensure the effectiveness of the company's AML/CFT Compliance program.
- Company reference to Pilot Innovation Sp. z.o.o., Company number: 540171166, POLAND, WARSAW, 02-697, Wincentego Rzymowskiego 30, office 424, which registered as Deposit Virtual Currency Wallet Operator and Virtual Currency Exchange Operator.
- Compliance Department: A Department within the Company responsible for reviewing and investigating reports of Suspicious Activity and determining whether the reported activity is indicative of money laundering or terrorist financing. They also take necessary steps to report Suspicious Activity to the appropriate authorities.
- User Due Diligence (CDD): A thorough process of identifying and assessing the risks associated with new relationships, which includes a variety of steps to verify the identity of the User or business partner, assess the risk of money laundering or terrorist financing, and obtain information about the User's or business partner's Source of Funds and intended use of the company's products or services.
- Due Diligence: A process of evaluating potential risks and assessing the Reputation and past behavior of External Parties to ensure that they are not involved in any illegal activities, such as money laundering or terrorist financing.
- External Parties: Users, business partners, suppliers, and other third parties with whom the Company has relationships.
- Financial Crime: Illegal activities that involve financial transactions, such as money laundering and terrorist financing.
- Financial Systems: The processes and infrastructure that enable financial transactions, such as banking and payment systems.
- Ongoing Monitoring: Regularly reviewing and assessing the activities of External Parties and transactions to detect Suspicious Activity and ensure Compliance with AML/CFT policies and procedures.
- Purpose: This Policy is intended to protect the Company from being used as a tool for illegal activities such as money laundering or terrorist financing by establishing guidelines for identifying and mitigating the risks of such activities in its interactions with External Parties.
- Reputation: The perception of a Company held by the public, Users and other stakeholders.
- Risk Assessment: A process of evaluating the potential risks of money laundering and terrorist financing associated with the company's external relationships, by considering a range of factors, including the nature of the relationship, the products or services provided, the location of the User or business partner, and the User's or business partner's industry or sector.

- Risk-Based Approach: A methodology in which the Company applies more stringent measures for higher-risk relationships and less stringent measures for lower-risk relationships.
- Sanctions Compliance: Procedures for screening Users, business partners and transactions against Sanctions Lists to ensure that the Company is not doing business with individuals or entities that are prohibited by sanctions laws.
- Sanctions Lists: Lists of individuals or entities that have been designated by government agencies as being subject to sanctions, embargoes, or other restrictions on trade or financial transactions.
- Sanctions Screening: Procedures implemented by the Company to check the names of individuals and entities against lists of individuals and entities that have been designated by government agencies as being subject to sanctions, embargoes, or other restrictions on trade or financial transactions.
- Source of Funds: The origin of the money or assets that a User or business partner uses to conduct transactions or activities.
- Suspicious Activity: Any unusual or suspicious financial transactions or activities that may indicate money laundering or terrorist financing.
- Third-Party Service Providers: External companies or individuals that provide services to the company, such as accounting, legal, or IT services.
- Training Programs: Programs for educating employees on how to recognize and report Suspicious Activity and their responsibilities under the company's AML/CFT Compliance program.
- Transaction Monitoring: The process of reviewing and analyzing financial transactions to detect Suspicious Activity and ensure Compliance with AML/CFT policies and procedures.
- Verification of Identity: The process of confirming the identity of a User or business partner through government-issued identification documents or by checking their creditworthiness.

## 4. Risk Assessment

The Company recognizes that different external relationships present varying levels of risk for money laundering or terrorist financing activities. Therefore, it will conduct a comprehensive Risk Assessment of all its external relationships to identify and evaluate any potential risks. This Risk Assessment will consider a range of factors, including the nature of the relationship, the products or services provided, the location of the User or business partner, and the User's or business partner's industry or sector.

Based on the results of the Risk Assessment, the Company will take appropriate measures to mitigate any risks identified. These measures include enhanced Due Diligence procedures, such as additional Verification of the User's or business partner's Identity or the source of their funds. The Company also implements Ongoing Monitoring procedures to detect any Suspicious Activity or changes in the risk profile of the external relationship.

Additionally, the Company implements a Risk-Based Approach for its AML/CFT Compliance program, which means the Company will apply more stringent measures for higher-risk relationships and less stringent measures for lower-risk relationships.

## 5. Requirements for Users

The Company has established rules to prevent illegal operations in all Applications created by the User. The person making and receiving payment must be the same individual, and transfers to third parties are strictly prohibited. Contact information and personal data provided by the User must be accurate and up-to-date. Additionally, the use of anonymous proxy servers or anonymous Internet connections to create Applications is strictly prohibited.

## 6. User Due Diligence (CDD)

The Company is committed to conducting thorough User Due Diligence (CDD) on all new Users and business partners to ensure that it is not unknowingly facilitating money laundering or terrorist financing activities. CDD is a critical process for identifying and assessing the risks associated with new relationships, and it includes a variety of steps to verify the identity of the User or business partner, assess the risk of money laundering or terrorist financing, and obtain information about the User's or business partner's Source of Funds and intended use of the company's products or services.

To conduct CDD, the Company takes several steps such as verifying the User's identity through government-issued identification documents.

The Company may also request additional documents for the User's identification such as a bank statement or utility bill from the past three months showing the User's full name and current address. The Company reserves the right to request photo/video verification of the User if there are suspicions of false information being provided. In turn, the Company verifies the authenticity of documents and information provided by the User.

If the User's identification information has been altered or their activity appears suspicious, the Company has the right to request updated documents from the User, even if they have already been verified.

Additionally the Company might also assesses the risk of money laundering or terrorist financing by researching the User's or business partner's background, including their financial history, and by evaluating their industry or sector, obtains information about the User's or business partner's Source of Funds and intended use of the company's products or services to understand their business activities.

The Company also recognizes the importance of Ongoing Monitoring to ensure that its Users and business partners do not pose a risk of money laundering or terrorist financing. Therefore, it will conduct Ongoing Monitoring of its Users and business partners to ensure that their activities do not change and become a higher risk. This includes monitoring transactions for Suspicious Activity, reviewing User information for any changes, and conducting additional CDD when necessary.

Overall, the company's CDD process and Ongoing Monitoring are essential tools for identifying and managing the risks associated with its external relationships and for ensuring that it is complying with applicable laws and regulations related to Anti-Money Laundering and Combating the Financing of Terrorism.

## 7. Sanctions Screening

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

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

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

## 8. Reporting Suspicious Activities

The Company recognizes the importance of having a process in place for employees to report any suspicious activities or transactions that indicate money laundering or terrorist financing. To achieve this, the Company will establish a process for employees to confidentially report any suspicious activities or transactions that they encounter in the course of their work. This process will be clearly communicated to all employees, and they will be encouraged to report any suspicious activities or transactions as soon as they become aware of them.

To aid employees in recognizing and Reporting suspicious activities, the Company will provide training on the various red flags that indicate money laundering or terrorist financing. This training will include information on how to recognize patterns of behavior or transactions that are indicative of illegal activities, as well as the procedures for Reporting such activities.

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

The Company will establish a process for employees to report suspicious activities or transactions, and provide them with training to recognize red flags that indicate money laundering or terrorist financing. The Compliance Department will review and investigate these reports and take necessary steps to report Suspicious Activity to the appropriate authorities.

## 9. Third-Party Service Providers

The Company will take steps to ensure that all Third-Party Service Providers comply with its Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) policies and procedures. This will involve conducting thorough Due Diligence on these providers, reviewing their Reputation and past behavior, and evaluating their own AML and CFT policies and procedures. To ensure Sanctions Compliance, the Company will include specific provisions related to AML and CFT in contracts with Third-Party Service Providers. Additionally, the Company will conduct regular monitoring of these providers to confirm they are adhering to the AML and CFT policies and procedures set forth in the contract.

## 10. Training

The Company will provide training to its employees on the policies and procedures, and best practices for preventing money laundering and terrorist financing in its external relationships. The training will be conducted on a regular basis, at least once a year, and will be tailored to the specific roles and

responsibilities of each employee. The Company will also keep its employees updated on any changes in regulations or guidance related to AML and CFT.

11. Restricted jurisdictions

The Company do not serve Clients from: Afghanistan, Albania, Algeria, Andorra, Anguilla, Antigua and Barbuda, Argentina, Bahamas, Bahrain, Bangladesh, Barbados, Benin, Bermuda, Bolivia, Botswana, Brazil, Brunei, Burkina Faso, Burundi, Cambodia, Cameroon, Cape Verde, Cayman Islands, Central African Republic (CAR), Ceuta, Chad, Chile, China, Colombia, Comoros, Congo, Cook Islands, Costa Rica, Cuba, Democratic People's Republic of Korea (DPRK), Democratic Republic of Congo, Djibouti, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, French Guiana, Gabon, Gambia, Ghana, Grenada, Guadeloupe, Guatemala, Guinea, Guinea-Bissau, Haiti, Honduras, Iceland, India, Iran, Iraq, Ivory Coast, Jamaica, Japan, Jordan, Kenya, Korea, Kuwait, Laos, Lebanon, Lesotho, Liberia, Libya, Macao, Madagascar, Maldives, Mali (Melilla), Marshall Islands, Martinique, Mauritania, Mexico, Mongolia, Morocco, Mozambique, Myanmar, Namibia, Nepal, Nicaragua, Niger, Nigeria, Pakistan, Palestine, Panama, Paraguay, Peru, Puerto Rico, Qatar, Republic of Congo, Republic of Kosovo, Republic of Liberia, Reunion, Russia, Rwanda, Sahara Arab Democratic Republic, Samoa, Sao Tome and Principe, Sark, Saudi Arabia, Senegal, Serbia, Sierra Leone, Somalia, South Africa, South Sudan, Sri Lanka, St. Barth, Senegal, St. Maarten, State of Palestine, Sudan, Switzerland, Syria, Taiwan, Tanzania, (temporarily occupied territories of Ukraine: Crimean Peninsula, Donetsk Oblast, Kharkiv oblast, Kherson oblast, Luhansk Oblast, Zaporizhzhya oblast), Togo, Transnistrian Moldavian Republic, Trinidad and Tobago, Tunisia, Turkey, Turkmenistan, Uganda, United Arab Emirates (UAE), United States of America (USA), Uruguay, Vanuatu, Venezuela, Western Sahara, Yemen, Zambia, Zimbabwe.

12. Specific restrictive measures

Monitoring of the User's transactions and analysis of the received data is one of the tools for assessing the risk and detecting suspicious transactions. In case of suspicion of money laundering, the Company controls all transactions and reserves the right to:

• suspend or terminate the User's account;

• suspend the exchange and freeze assets until the circumstances are clarified;

• return the User's funds by canceling the Order;

• if during the transaction/wallet check for cleanliness of cryptocurrency assets, it is found that the coins are marked with the SCAM, STOLEN, RANSOMWARE label or a risk analysis of 50% or more, the transaction is not eligible for exchange and refund.

The Company may freezes assets owned, held, or controlled directly or indirectly by individuals and entities and any benefits derived from these assets, as per Due Diligence. This freeze applies to individuals and entities listed:

1. In the lists published by the Inspector General based on United Nations Security Council resolutions issued under Chapter VII of the United Nations Charter, regarding threats to international peace and security caused by terrorism, particularly in Resolution 2253 (2015) and Resolution 1988 (2011).

2. In the list of individuals and entities subject to specific restrictive measures kept by the Inspector General and published in the Public Information Bulletin on the website of the minister responsible for public finance.

The Company must provide information about the frozen assets to the General Inspector within 2 business days by submitting it electronically.

## 13. Conclusion

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

## 14. Contact Us

If You have any questions about this Agreement, You can contact us:

- By email: compliance@paypilot.org