Policy on Anti-Money Laundering, Counter-Terrorist Financing, and "Know Your Customer" Policy

1. General Information

The Policy on Anti-Money Laundering, Counter-Terrorist Financing, and the "Know Your Customer" Policy (hereinafter referred to as the "Policy") is designed to prevent and mitigate potential risks of **PILOT INNOVATION SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ**, Reg.number:540171166, ALEJA STANOW ZJEDNOCZONYCH, №32, office 8, WARSAW, POLAND, (hereinafter referred to as the "Company", "**Paypilot**") being involved in any illegal activities.

To comply with international and local regulations, **Paypilot** implements effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, the proliferation of weapons of mass destruction, corruption, and bribery, and to respond in case of any form of suspicious activity by its Users.

"Money Laundering" is understood as "the conversion or transfer of property, knowing that such property is derived from criminal activity or from participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or assisting any person involved in committing such activity in avoiding the legal consequences of their actions."

"Terrorist Financing" is understood as "the intentional provision or collection of funds by any means, directly or indirectly, with the intention that they should be used or knowing that they will be used to carry out terrorist acts."

This Policy should not be interpreted as an exhaustive set of all policies, procedures, and control measures implemented by the Company to prevent money laundering, terrorist financing, and other forms of illegal activity.

2. Company Obligations

2.1 Obliged Entity in Poland

The Company **Paypilot** is subject to regulation in accordance with the **Polish Act on Counteracting Money Laundering and Terrorist Financing of March 1, 2018 (Dz.U. 2018 poz. 723)** and other applicable legal acts.

Regulatory Authorities

The Company is supervised by the **General Inspector of Financial Information (GIIF)**, which is the competent authority in Poland responsible for monitoring and preventing financial crimes.

Company Responsibilities

Client Identification and Due Diligence Measures (KYC/CDD):

- Implementation of "Know Your Customer" (KYC) procedures;
- Customer risk assessment based on the **Risk-Based Approach (RBA)**;
- Enhanced Due Diligence (EDD) for high-risk clients.

Reporting Obligations to GIIF:

- Reporting transactions amounting to **€15,000 and above**;
- Mandatory reporting of **suspicious transactions** potentially related to money laundering or terrorist financing;
- Maintaining relevant documentation for at least **5 years**.

Compliance with International AML/CTF Standards:

- **Directive (EU) 2015/849 (4th AML Directive)**;
- **Directive (EU) 2018/843 (5th AML Directive)**;
- **Regulation (EU) 2015/847 on the provision of information accompanying transfers of funds**;
- **Financial Action Task Force (FATF) recommendations** on combating financial crimes.

3. Customer Due Diligence (CDD)

Comprehensive **Customer Due Diligence (CDD)** is a mandatory measure under the **Polish Act on Counteracting Money Laundering and Terrorist Financing of March 1, 2018 (Dz.U. 2018 poz. 723)**. The Company is obliged to collect, verify, and update customer information at all stages of cooperation.

Depending on the level of risk assigned to a client, different levels of **CDD** apply:

- **Standard Due Diligence (SDD)** – for low-risk customers;

- **Enhanced Due Diligence (EDD)** – for customers identified as high-risk, requiring additional data.

3.1. Standard Due Diligence Measures

For individual clients, the following documents are required:

- Passport or national **ID card**;
- Proof of address (bank statement, utility bill);
- **Liveness check**.

For legal entities, the following documents are required:

- **Corporate documents** (Articles of Association);
- Passport of the **beneficial owner** and **director**;
- Proof of **company address**;
- **Register of directors and shareholders**;
- **Source of funds confirmation**;
- **Top-5 business partners and contracts with them**;
- **Website information and domain ownership confirmation**.

3.2. Enhanced Due Diligence (EDD)

The Company applies **EDD** when:

- The **customer's data raises doubts** about its authenticity;
- The customer is a **financial institution from a third country**;
- The customer is a **Politically Exposed Person (PEP)** or a close associate;
- The customer resides in or operates in a **high-risk jurisdiction**.

Under **EDD**, the Company may:

- Request **additional identity verification documents**;
- Conduct **source of wealth and funds checks**;
- Increase **transaction monitoring frequency**;
- Analyze **customer business activities**.

3.3. Source of Funds Verification

The Company is required to ensure that the funds used by the client have a **legitimate origin**. For this purpose, the following documents may be requested:

PayPilot
Your private payments jet

- **Bank statements**;
- **Income and investment documents**;
- **Proof of property sales or other legal transactions**.

4. Politically Exposed Persons (PEPs)

The Company determines whether a client or their beneficial owner is a **Politically Exposed Person (PEP)**, a **family member**, or a **close associate**. If a client is classified as a PEP, they are subject to **enhanced verification and monitoring measures**.

5. Ongoing Monitoring and Data Updates

The Company implements **transaction monitoring systems** in accordance with the **Polish Act on Counteracting Money Laundering and Terrorist Financing of March 1, 2018 (Dz.U. 2018 poz. 723)**. The purpose of monitoring is to **detect and prevent** suspicious financial transactions related to money laundering (AML) or terrorist financing (CTF).

5.1. Monitoring Procedures

- Analyzing **customer transaction activity patterns**;
- **Automated transaction screening** using data analysis systems;
- **Manual review of suspicious transactions**;
- **Checking transactions against sanctions lists** and high-risk jurisdictions;
- **Assessing customer risk levels** and transaction behavior.

5.2. Identifying Suspicious Transactions

Suspicious transactions include those that:

- **Do not match the customer's typical behavior**;
- Are **unusually large or frequent**;
- **Involve high-risk or sanctioned jurisdictions**;
- Show signs of **structuring** (splitting transactions to avoid reporting thresholds);
- Involve **rapid fund movements** without economic justification.

5.3. Risk Assessment

The Company conducts an **annual internal risk assessment** related to:

- **Geographical factors** (countries with high levels of corruption and weak financial regulation);

- **Customer types** (Politically Exposed Persons (PEPs), financial institutions);
- **Payment instruments used** (cash, cryptocurrency, anonymous payments);
- **Nature of the client's business** (companies operating in high-risk AML/CTF sectors).

As part of the assessment, **corrective measures** are developed to **minimize risks** and **enhance monitoring processes**.

5.4. Response to Suspicious Transactions

If suspicious transactions are detected, the Company takes the following steps:

- **Initial review** – an internal analysis of the transaction to identify potential AML/CTF violations.
- **Request for additional information from the client** – clarifications regarding the source of funds and the economic rationale of the transaction.
- **Transaction suspension** – if there are serious grounds for suspicion.
- **Reporting to GIIF** – submitting a report on suspicious activity to the regulatory authority.
- **Account closure** – if the client fails to provide convincing evidence of the legitimacy of their actions.

5.5. Use of Technology in Monitoring

The Company utilizes advanced technologies for transaction data analysis, including:

- **Automated monitoring systems with machine learning algorithms**;
- **Blockchain analytics to track cryptocurrency transactions**;
- **Databases of sanctions lists, Politically Exposed Persons (PEPs), and adverse media**;
- **Customer behavioral data analysis tools**.

These technologies improve the accuracy of **detecting suspicious transactions** and reduce the **rate of false positives**.

6. MLRO

The **MLRO** at **Paypilot** ensures AML/CTF policy compliance and adherence to Polish regulations and international standards.

Main Responsibilities:

PayPilot
Your private payments jet

- **Supervising KYC, CDD, EDD, and transaction monitoring** procedures;
- **Interacting with GIIF** and submitting reports on suspicious transactions;
- **Developing and updating internal AML/CTF procedures**;
- **Conducting employee training and internal audits**;
- **Risk assessment and implementation of corrective measures**.

7. Refusal to Provide Services

The Company **does not establish business relationships** with clients who:

- **Refuse to provide** requested information and verification documents;
- Are **Shell Banks** (banks without a physical presence in a regulated jurisdiction);
- Reside or operate in **sanctioned or high-risk jurisdictions**;
- Raise **reasonable suspicions** of potential involvement in money laundering, terrorist financing, or other illegal activities.

The Company **does not accept** clients from certain high-risk countries and territories, including but not limited to Afghanistan, Albania, Algeria, Andorra, Angola, Anguilla, Antigua, Argentina, Barbuda, Bahamas, Bahrain, Bangladesh, Barbados, Benin, Bermuda, Bolivia, Botswana, Brazil, Brunei, Bulgaria, 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, Croatia, 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, Monaco, Mongolia, Morocco, Mozambique, Myanmar, Namibia, Nepal, Nicaragua, Niger, Nigeria, Pakistan, Palestine, Panama, Paraguay, Peru, Philippines, 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, Vietnam, Western Sahara, Yemen, Zambia, Zimbabwe

PayPilot
Your private payments jet

8. Cooperation and Information Exchange

The Company actively **collaborates** with regulatory authorities and law enforcement agencies to combat money laundering and terrorist financing. **Paypilot** provides the necessary information upon official requests in accordance with applicable laws and international obligations.

For inquiries regarding cooperation and information exchange, please contact the Company at: **support@paypilot.org**.