Information on Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Principles

1. General Information

The Anti-Money Laundering and Counter-Terrorist Financing Policy (hereinafter – the "Policy") aims to prevent and mitigate potential risks that **Pilot Innovation** (hereinafter – the "Company") may be involved in any illegal activities.

To comply with both international and domestic regulations, the Company 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, as well as to respond to any form of suspicious activity from its Users.

"**Money Laundering** (legalisation of proceeds of crime)" shall be understood in line with Article 299 of the Polish Penal Code of 6 June 1997.
"**Terrorist Financing**" shall be understood in line with Article 165a of the Polish Penal Code of 6 June 1997.

This Policy should not be interpreted as a comprehensive set of all policies, procedures, and control measures applied by the Company in preventing money laundering, terrorist financing, and other unlawful activities.

2. Company's Obligations

2.1 Obliged Entity in Poland

PILOT INNOVATION SP. Z O.O. is an obliged entity under the provisions of the **Polish Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing** (Journal of Laws 2018, item 723, as amended), as well as other applicable legal acts.

Supervisory Authority

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

Company's Duties

- **Customer Identification and Financial Security Measures (KYC/CDD):**
    - Implementation of "Know Your Customer" (KYC) procedures;
    - Client risk assessment in accordance with the Risk-Based Approach (RBA);
    - Enhanced Due Diligence (EDD) for higher-risk clients.
- **Reporting Obligations towards GIIF:**
    - Reporting transactions with a value of EUR 15,000 or more;
    - Mandatory reporting of suspicious transactions potentially related to money laundering or terrorist financing;

- Maintaining proper records and documentation for no less than **5 years**.

Compliance with International AML/CTF Standards
The Company ensures compliance with international anti-money laundering and counter-terrorist financing standards, including:

- **Directive (EU) 2015/849** (4th AML Directive);
- **Regulation (EU) 2023/1113** of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets, and amending Directive (EU) 2015/849 (the "Transfer Regulation");
- **FATF Recommendations** (Financial Action Task Force) on countering financial crime.

3. Customer Due Diligence Obligations
Comprehensive verification of customer identity (**Customer Due Diligence – CDD**) is a mandatory measure under the Polish **Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing** (Journal of Laws 2023, item 1124). The Company is required to collect, verify, and update customer information at all stages of cooperation.

Depending on the client's assessed risk level, different levels of CDD apply:

- **Standard Due Diligence (SDD)** – applied to low-risk customers;
- **Enhanced Due Diligence (EDD)** – applied where higher risk is identified, requiring additional data.

3.1 Standard Due Diligence (SDD)
For **individual clients**, the following documents and checks are required:

- Passport or national identity card;
- Proof of residential address (e.g., bank statement, utility bill);
- Biometric verification (liveness check) in case of remote verification.

For **corporate clients**, the following are required:

- Incorporation documents;
- Identification documents of the Ultimate Beneficial Owner (UBO) and members of the management board;
- Proof of company address;
- Extract from the National Court Register (KRS);

- Proof of source of funds;
- List of top 5 business partners and contracts with them;
- Information about the company's website and proof of domain ownership.

3.2 Enhanced Due Diligence (EDD)
The Company applies EDD measures in the following cases:

- Where the client's data raises doubts about its credibility;
- Where the client is a financial institution from a third country;
- Where the client is a Politically Exposed Person (PEP) or a close associate/family member;
- Where the client resides in or operates from a high-risk jurisdiction.

In such cases, the Company may:

- Request additional identity verification documents;
- Verify the source of the client's funds and wealth;
- Increase the frequency of transaction monitoring;

Conduct deeper analysis of the client's business activity

3.3 Verification of Source of Funds
The Company is required to ensure that the funds used by a client originate from a legitimate source. For this purpose, the following may be requested:

- Bank statements;
- Documents confirming income and investments;
- Evidence of asset sales or other lawful transactions.

4. Politically Exposed Persons (PEPs)
The Company determines whether a client or its beneficial owner is a Politically Exposed Person (PEP), a family member, or a close associate. If a client is identified as a PEP, enhanced due diligence (EDD) measures are automatically applied.

5. Ongoing Monitoring and Data Updates
The Company implements transaction monitoring systems in accordance with the Polish **Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing** (Journal of Laws 2018, item 723). The purpose of monitoring is to detect and prevent

suspicious financial operations that may be linked to money laundering (AML) or terrorist financing (CTF).

5.1 Monitoring Procedures
Transaction monitoring is continuous and includes:

- Analysis of customer transaction activity patterns;
- Automated transaction screening using data analysis systems;
- Manual review of transactions meeting suspicious criteria;
- Transaction screening against sanctions lists and high-risk jurisdiction lists;
- Ongoing risk assessment of the client and their transactional activity.

The Company applies a **Risk-Based Approach (RBA)**, under which clients are classified into different risk levels (low, medium, high, and unacceptable), and their transactions are reviewed with appropriate detail depending on their risk classification.

5.2 Identification of Suspicious Transactions
The Company is required to maintain a register of suspicious transactions and report them to the **General Inspector of Financial Information (GIIF)**.

5.3 Risk Assessment
The Company conducts an **internal risk assessment annually**, taking into account:

- **Geographical factors** (countries with high levels of corruption or weak financial supervision);
- **Customer type** (PEPs, financial institutions);
- **Payment instruments used** (cash, anonymous payments);
- **Nature of the client's business** (companies operating in sectors with elevated AML/CTF risk).

Based on this assessment, corrective actions are developed to minimize risks and improve monitoring processes.

5.4 Use of Technology in Monitoring
The Company employs advanced technologies for the analysis of transactional data, including:

- Automated monitoring systems with machine learning algorithms;
- Blockchain analytics to trace cryptocurrency operations;

- Databases of sanctions lists, Politically Exposed Persons (PEPs), and adverse media;

- Tools for behavioral data analysis of clients.

These technologies enhance the accuracy of detecting suspicious transactions and reduce the number of false positives.

6. Responsible Officer (RO)

The Company's Responsible Officer (RO) oversees compliance with the AML/CTF Policy and ensures adherence to the legal requirements of the Republic of Poland and international standards.

Key responsibilities include:

- Supervising the application of AML/CTF procedures and transaction monitoring;

- Cooperating with GIIF and submitting suspicious transaction reports;

- Developing and updating internal AML/CTF procedures;

- Training employees and conducting internal audits;

- Assessing risks and implementing corrective measures.

The Responsible Officer acts as the primary contact with regulators and ensures the effectiveness of the Company's internal control framework.

7. Refusal of Service

Unacceptable Clients

The Company does not enter into business relationships with clients who:

- Refuse to provide the required information and documents for verification;

- Are "Shell Banks" (banks without a physical presence in a regulated jurisdiction);

- Reside or operate in countries subject to international sanctions or prohibited by the Company's internal policy;

- Raise justified suspicions of potential involvement in money laundering, terrorist financing, or other illegal activities.

Prohibited Countries and Territories

The Company does not onboard clients from the following countries and territories:

Afghanistan; American Samoa; Belarus; Burundi; Cambodia; Cameroon; Central African Republic; Chad; Cuba; Democratic People's Republic of Korea (North Korea); Democratic Republic of the Congo; Eritrea; Ethiopia; Haiti; Iran; Iraq; Kazakhstan;

Kyrgyzstan; Lebanon; Libya; Mali; Mozambique; Myanmar (Burma); Nicaragua; Pakistan; Palestine; Russia; Senegal; Sierra Leone; Somalia; South Sudan; Sudan; Syria; Tajikistan; Transnistria; Turkmenistan; Uganda; Ukraine – Non-government controlled territories (Crimea, Donetsk, Kherson, Luhansk, Zaporizhzhia oblasts); Uzbekistan; Venezuela; Yemen; Zimbabwe.

Clients or beneficial owners linked to these countries are automatically classified as **"Rejected / Prohibited."**

High-risk third countries:

The following jurisdictions are classified as high-risk according to the EU Delegated Regulation (EU) 2024/594, FATF public statements, and the Polish AML Act (Art. 2 (2) (13)). Clients or counterparties connected with these countries may be accepted only under Enhanced Due Diligence (EDD), MLRO approval, and documented SoF/SoW verification.

Albania; Barbados; Burkina Faso; Cameroon; Cayman Islands; Gibraltar; Jamaica; Jordan; Nigeria; Panama; Philippines; South Africa; Tanzania; Trinidad and Tobago; Uganda; United Arab Emirates (UAE); Vietnam; and any other jurisdiction designated as high-risk by **FATF** or the **European Commission** at the time of onboarding or periodic review.

Medium-Risk Countries

Jurisdictions with partially effective AML/CFT supervision, elevated corruption or tax-transparency concerns, but generally cooperative frameworks. EDD recommended for large-volume transactions or crypto-exposure.

Medium-Risk List:
Andorra; Angola; Argentina; Armenia; Azerbaijan; Bahamas; Bahrain; Bangladesh; Bosnia and Herzegovina; Botswana; Brazil; Brunei; Chile; China (PRC); Colombia; Costa Rica; Croatia; Czech Republic; Dominican Republic; Ecuador; Egypt; El Salvador; Georgia; Ghana; Greece; Guatemala; Honduras; Hong Kong SAR; Hungary; India; Indonesia; Israel; Kenya; Kuwait; Laos; Latvia; Lithuania; Malaysia; Maldives; Malta; Mauritius; Mexico; Moldova; Mongolia; Montenegro; Morocco; Namibia; Nepal; North Macedonia; Oman; Papua New Guinea; Paraguay; Peru; Poland; Qatar; Romania; Saudi Arabia; Serbia; Singapore; Slovakia; Slovenia; Sri Lanka; Suriname; Taiwan; Thailand; Tunisia; Turkey; Ukraine (government-controlled territory); Uruguay.

Low-Risk Countries

Countries with robust AML/CFT regimes, strong governance, low corruption perception, and EU/OECD/FATF full compliance. SDD may apply where legally permitted.

Low-Risk List:
Austria; Australia; Belgium; Bulgaria; Canada; Croatia; Cyprus; Denmark; Estonia; Finland; France; Germany; Iceland; Ireland; Italy; Japan; Liechtenstein; Luxembourg; Monaco; Netherlands; New Zealand; Norway; Portugal; San Marino; South Korea; Spain; Sweden; Switzerland; United Kingdom;

The Company will not knowingly enter into or maintain a business relationship with individuals or entities involved in or connected to:

● Illegal gambling or unlicensed betting activities;
● Weapons or defense-related trade (including intermediaries, dual-use goods, ammunition, chemical or biological weapons, cluster munitions);
● Narcotics, precursors, or illegal pharmaceuticals;
● Human trafficking, modern slavery, or child exploitation;
● Shell banks or institutions with no physical presence or effective supervision; ● Adult content (pornography, webcam services, live adult streaming, child or bestiality content, rape or violence-related material);
● Intellectual property or copyright infringement, counterfeit goods;
● Unlicensed financial institutions, money transmitters, or virtual asset providers; ● Privacy coins or anonymity-enhanced cryptocurrencies (e.g., Monero, Zcash, Dash);
● Ponzi, pyramid, or high-yield investment schemes; Binary options, unregulated trading platforms, or ICO/ITO token placements;
● Clients issuing or holding bearer shares or equivalent untraceable ownership instruments.

Bearer shares refer to negotiable instruments representing ownership in a legal entity, where control rests solely with the physical holder and cannot be verified by the Company. Registered or dematerialised shares are acceptable.

The Company reserves the right to reject, suspend, or terminate any business relationship or transaction that falls outside its risk appetite or presents unmanageable AML/CFT risk.

Based on EBA Guidelines EBA/GL/2022/05 of 14 June 2022 and the KNF Position on AMLRO of 1 December 2022, the Company indicates that, within the necessary scope of periodic (or ad hoc) management information and the annual activity report compiled by the Designated Employee (AMLRO), the following data and information are, in particular, considered required:

● ML/TF risks and the Company's compliance with AML/CFT provisions;
● the Company's cooperation with competent state authorities and related correspondence;
● all findings and actions of the financial intelligence and supervisory authorities (including analytical and inspection activities) addressed to the Company, including information on measures applied or penalties imposed, correspondence with the Company, reports submitted, breaches found and penalties imposed, as well as the manner and stage of implementing recommendations;
● any serious or material problems and breaches in the AML/CFT area, recommendations issued in this respect, and remedial actions taken;
● a summary of the main findings of the institution-wide ML/TF risk assessment;
● a description of any changes to the method used by the Company to assess the individual customer risk profile;
● the classification of customers by risk categories, including changes compared to the previous reporting period and the main reasons for changes in customer risk categories;
● the number of customer files (by risk category), including those for which no review and update of the customer risk assessment has yet been carried out; ● the

application of customer due diligence measures, including for occasional transactions and for customers classified in higher ML risk categories; ● information and statistics on the number of:

- ○ unusual transactions analysed and detected,
  reports of suspicious transactions or other actions submitted to the financial intelligence unit and the public prosecutor's office,
- ○ relationships with customers rejected or terminated due to inability to apply due diligence measures,
- ○ requests received from the financial intelligence unit, courts, or law-enforcement authorities;

● a description of the organisational structure in the AML/CFT area and any material changes together with their justification;
● a description of the human and technical resources available to the AML/CFT unit; in cases of outsourcing — a list of AML/CFT processes outsourced to the service provider together with a description of the results of monitoring performed by the supervised entity;
● in the area of risk assessment — implemented risk-mitigation mechanisms and adopted procedures, together with a description of problems, deficiencies, and irregularities, as well as conclusions, recommendations, and changes introduced;
● a description of compliance monitoring activities undertaken to assess the implementation of AML/CFT policies (strategies), internal controls, and procedures,
together with an assessment of the adequacy of all monitoring tools used by the supervised entity;
● the performance of the training obligation;
● planned activities of the Designated Employee;
● findings of internal control and the implementation status of issued recommendations;
● a description of changes in the supervised entity's legal environment and the impact of those changes on its AML/CFT process.

Politically Exposed Persons (PEPs)

The Company classifies the following categories of individuals as Politically Exposed Persons (PEPs):

Domestic PEPs (Poland / local jurisdiction)

Individuals who are or have been entrusted with *prominent public functions* at the national level, including:

- ● Head of State or Head of Government
- ● Ministers, Deputy Ministers, Secretaries of State
- ● Members of Parliament (Sejm and Senate)
- ● Members of governing bodies of political parties
- ● Members of the Supreme Court, Constitutional Tribunal, or other high-level judicial bodies whose decisions are not subject to further appeal
- ● Members of the Court of Auditors or the Board of the National Bank of Poland
- ● Ambassadors, Chargés d'Affaires
- ● High-ranking officers of the armed forces (general/admiral level)
- ● Members of the management, supervisory, or administrative bodies of state-

owned enterprises
- Directors, deputy directors, and members of management bodies of international organizations

Note:
Individuals holding *local or regional functions* (e.g., mayors, city or municipal council deputies, local government representatives) are not considered PEPs, unless they have influence on national-level decisions or public resources.

Foreign PEPs

Individuals entrusted with prominent public functions by a foreign country, including:

- Heads of State or Government
- Ministers, Deputy Ministers, or Assistant Ministers
- Members of national parliaments
- Members of governing bodies of political parties
- Members of supreme courts or constitutional courts
- Members of courts of auditors or central bank boards
- Ambassadors, Chargés d'Affaires, or high-ranking officers in the armed forces
- Senior executives of state-owned enterprises
- Directors, deputy directors, and members of the management of international organizations

International Organization PEPs
Individuals who hold or have held senior management positions in international organizations, including:

- Directors, Deputy Directors, or Members of the Board
- Senior executives equivalent to the above levels
  Examples: UN, IMF, World Bank, EU institutions, NATO, OSCE, etc.

Family Members of PEPs
The following are also considered related to a PEP:

- Spouse or person recognized as equivalent to a spouse
- Children and their spouses or partners
- Parents of the PEP

Close Associates of PEPs
Any individual known to:

- Have joint beneficial ownership of legal entities or arrangements with a PEP
- Have close business relations with a PEP
- Be the sole beneficial owner of a legal entity or arrangement known to have been established for the benefit of a PEP

Exclusion Clause
The following categories **are not classified as PEPs**, unless otherwise demonstrated:

- Deputies or council members of local/municipal authorities (e.g., city or regional councils)
- Civil servants and employees of local administrations without decision-making powers at national level
- Persons employed in state institutions in technical or advisory roles

Accepted Identification Documents

1. Purpose and Scope

This Annex establishes the list of identification documents accepted by Pilot Innovation Sp. z o.o. (“the Company”) for the purposes of Customer Due Diligence (“CDD”) and Know Your Customer (“KYC”) procedures in accordance with:

- the Polish Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (“AML Act”);
- EU Directive (EU) 2015/849 (AMLD IV) as amended;
- FATF Recommendations; and
- EBA Guidelines EBA/GL/2022/05.

The list applies to onboarding and ongoing verification of natural persons, legal entities, and beneficial owners, whether identified directly by the Company or through the automated KYCAid system.

2. General Rules

1. All documents must be valid, legible, and issued by a competent public

authority.

2. Documents must contain at least:

    - full name,
    - date of birth or incorporation,
    - nationality or registered jurisdiction,
    - identification number (personal or company),
    - photograph (for natural persons),
    - issue and expiry dates (where applicable).

3. Copies or scans of documents must be in colour and of sufficient quality for authenticity verification.

4. Documents in a language other than Polish or English must be accompanied by a certified translation.

5. Documents issued by prohibited or high-risk jurisdictions (as defined in *Annex No. 1*) are not accepted.
6. The Company reserves the right to request additional documents or verification where risk indicators require Enhanced Due Diligence (EDD).

8. Cooperation and Information Exchange

The Company actively cooperates with regulatory bodies and law enforcement authorities to prevent money laundering and terrorist financing. Paypilot provides necessary information upon official request in accordance with applicable laws and international obligations.

For matters concerning cooperation and information exchange, the Company may be contacted at: **aml@paypilot.org**