Plac Bankowy str., 2, room 1309, post office code 00-095, Warsaw, Poland. National Economy Register number: 389934132, tax identification number: 7123424132. Bank details: PL16160014621807188470000001 PLN, PL86160014621807188470000002 EUR
+38050 46 46 46 2; bizz0777@gmail.com

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy

COMFORT LIFE TECH Sp. z o.o.
Company Registry (KRS): 0000921491
Tax ID (NIP): 7123424132
REGON: 389934132
Registered Address: Plac Bankowy 2, 1309, 00-095 Warsaw, Poland
Email: bizz0777@gmail.com

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy

Effective Date: April, 01, 2025

1. General Provisions

1.1. This Anti-Money Laundering and Counter-Terrorist Financing Policy (hereinafter the “Policy”) is adopted by **Comfort Life Tech Sp. z o.o.** (the “Company”) in accordance with:

- The Polish Act of 1 March 2018 on Counteracting Money Laundering and Financing of Terrorism (as amended);
- Regulation (EU) 2015/847 and successive AML Directives of the European Parliament and of the Council;
- Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA);
- The recommendations and best practices of the Financial Action Task Force (FATF);
- Any other binding legal acts of the Republic of Poland and the European Union concerning AML/CFT;
- Provisions on personal data protection under the EU General Data Protection Regulation (GDPR) and relevant Polish data protection laws.

1.2. The objective of this Policy is to establish internal procedures, rules, and controls enabling the Company to:

- Identify and verify its customers (“Clients”) on the Company’s platform or services (the “Platform”);
- Detect, prevent, and report activities related to money laundering (“ML”) and terrorist financing (“TF”);
- Comply with all obligations to inform competent Polish authorities (particularly the General Inspector of Financial Information—GIIF) about suspicious activities or transactions;
- Ensure that all Company employees and associates understand and fulfill these AML/CFT obligations.

1.3. This Policy covers the Company’s business in dealing with crypto-assets and fiat transactions, including:

- Cryptocurrency exchange;
- Custodial or brokerage services (if provided);
- Any additional operations involving crypto-assets that may pose AML/CFT risks.

1.4. This Policy is reviewed and, if necessary, updated at least annually or whenever relevant laws or guidelines change.

2. Organizational Basis for AML/CTF Control Methods

2.1. **Approval and Oversight**

• The Company's Management Board approves this Policy and oversees compliance.
• A dedicated Compliance Officer (or AML Specialist) is appointed to implement this Policy and manage day-to-day AML/CTF tasks.

2.2. **Internal Controls**
• The Company has established know-your-customer (KYC), know-your-business (KYB), and know-your-transaction (KYT) procedures in accordance with Polish and EU AML law, FATF recommendations, and MiCA requirements.
• These internal controls apply to all staff members and service providers who may, in the course of their duties, affect the Company's AML/CTF obligations.

2.3. **Legal Framework Alignment**
• Primary reference is made to the Polish Act on Counteracting Money Laundering and Terrorist Financing.
• MiCA (EU Regulation 2023/1114) is also integrated for aspects specifically regulating crypto-assets.
• Where relevant, the Company may also consider guidelines or interpretive notes from Polish regulators (e.g., the Ministry of Finance, the Polish Financial Supervision Authority), as well as from the European Banking Authority (EBA) and European Securities and Markets Authority (ESMA).

3. Implementation of AML/CTF Controls

3.1. **Scope of Methods**
• This Policy and supporting internal procedures constitute the Control Methods for AML/CTF compliance.
• They guide employee obligations for KYC, suspicious transaction reporting, recordkeeping, and risk assessment.

3.2. **Purpose of Control Methods**
• Identify and verify Clients and relevant transactions at the onboarding stage, and continuously afterward, based on risk.
• Prevent and detect possible ML/TF-related transactions or patterns.

3.3. **Risk-Based Approach**
• The Company applies a risk-based approach in line with Polish and EU AML legislation.
• Clients are assigned a risk category (e.g., standard, medium, high) based on indicators like country of origin, transaction volume, type of activity, presence on sanctions lists, or PEP (politically exposed person) status.
• The depth of due diligence (simplified, standard, or enhanced) correlates with these risk levels.

3.4. **Data Protection**
• The Company collects and processes personal information solely for AML/CTF compliance and in accordance with the GDPR.
• Data will not be disclosed to third parties except as required by law, regulation, or with Client's explicit consent.

4. Client Verification Procedures (KYC)

4.1. **Initial Verification**
• **Individuals** must provide valid proof of identity (e.g., ID card, passport) and any additional documents required under Polish AML law.
• **Legal entities** must submit documentation (e.g., company registration certificate, details of ownership structure, KRS excerpt, beneficial owners), showing authorization for their representatives to act on behalf of the entity.

4.2. **Verification Methods**

• The Company may utilize official government databases (e.g., CEIDG, KRS), external verification services, or public registers.

• Documents may require notarization or an apostille if authenticity cannot be verified through electronic means.

4.3. **Beneficial Owner and Authorized Representative**

• Only authorized individuals may open accounts for legal entities.

• The beneficial owner must be identified and verified in line with the Polish Act on Counteracting Money Laundering and Terrorist Financing.

• The Company will consult the Central Register of Beneficial Owners (CRBR) to verify or confirm beneficial ownership whenever possible.

4.4. **Ongoing Monitoring**

• The Company reserves the right to request updated documents periodically or when suspicious activity is detected.

• Clients are obliged to cooperate fully with these re-verifications.

5. Risk Evaluation

5.1. **Risk Factors**

• Jurisdictions subject to sanctions or identified as high-risk by FATF or the EU.

• Politically exposed persons (PEPs).

• Large or unusual transactions that do not match the Client's stated business profile.

• Complex ownership structures that cannot be easily verified.

5.2. **High-Risk Clients or Transactions**

• The Company conducts enhanced due diligence (EDD) for higher-risk Clients, including deeper background checks, source-of-funds confirmations, and additional approvals.

• If risk remains unacceptably high, the Company may refuse to onboard or may terminate an existing relationship.

5.3. **Client Notification**

• The Company may inform Clients about additional checks or clarifications required due to risk-based triggers, unless prohibited by law.

6. Establishing and Maintaining the Business Relationship

6.1. **Client Acceptance**

• A new Client relationship begins only once the AML checks (including KYC) are complete.

• The Client must confirm acceptance of this AML Policy, as well as any Terms of Use the Company publishes.

6.2. **Enhanced Due Diligence (EDD)**

• EDD applies particularly for Clients from high-risk countries, PEPs, or when other risk indicators arise.

• Additional measures may include obtaining detailed information on the Client's source of wealth, beneficial owners, or business activities.

6.3. **Refusal or Discontinuation**

• The Company may refuse a relationship or transaction if the Client does not cooperate with AML/CTF procedures or if suspicion of ML/TF activities arises.

7. Actions Upon Suspicion of ML/TF

7.1. **Freezing or Blocking**

• If the Company suspects that certain activities are linked to money laundering or terrorist financing, it may suspend or block transactions and freeze the Client's account.

7.2. **Reporting Obligations**

• In compliance with Polish law, the Company must report suspicious activity to the General Inspector of Financial Information (GIIF) without informing the Client (tipping off is prohibited).

• Additional reporting to law enforcement or the public prosecutor's office may be required.

8. Correspondence Exchange for Verification

8.1. **Communication with Financial Institutions**

• When necessary, the Company may contact other financial or credit institutions to confirm or refine the data regarding a Client or a transaction, as allowed by law.

8.2. **Liaison with Regulators**

• The Company complies with requests or orders from national regulators, courts, or law enforcement regarding ongoing investigations or AML/CTF checks.

9. Transaction Monitoring Program

9.1. **Monitoring Tools**

• The Company employs both automated and manual monitoring techniques to detect anomalies (e.g., sudden spikes in transaction volume, transactions to/from high-risk jurisdictions).

9.2. **Documentation Requests**

• If anomalies or red flags appear, the Client may be asked to provide supporting documents or detailed explanations for certain transactions.

9.3. **Refusal of Suspicious Transactions**

• Should a Client fail to provide satisfactory explanations or documents, the Company may refuse the transaction, freeze assets, or close the account, consistent with applicable AML/CTF laws.

10. Termination of the Business Relationship

10.1. **Risk Thresholds**

• Each Client is assigned a risk score upon onboarding and is subject to periodic or event-driven reevaluations.

• If the risk score surpasses the Company's acceptable threshold, the business relationship may be terminated.

10.2. **Non-Disclosure**

• If the termination relates to ML/TF suspicions, the Company is not required to disclose the reasons.

• The Company adheres to the prohibition on tipping off the Client about any suspicious activity reporting.

11. Record-Keeping

11.1. **Data Retention Period**

• The Company keeps all AML-related records (identification documents, verification details, transaction logs, communications) for at least five (5) years after the end of the business relationship, or longer if required by law or official order.

11.2. **GDPR Compliance**

• Personal data is collected and processed strictly for AML/CTF and legal compliance purposes, in accordance with the GDPR and Polish data protection law.

• Clients may exercise their data protection rights unless superseded by AML/CTF obligations.

12. Training of Employees

12.1. **AML/CTF Staff Training**

• All relevant personnel undergo regular AML/CTF training on current legal requirements, internal procedures, and red-flag identification.

• New hires must complete initial AML training prior to handling Client onboarding or transactions.

12.2. **Confidentiality**

• Employees are required to maintain strict confidentiality of AML investigations, suspicious transaction reports, and other sensitive information, per the law and internal policy.

13. Final Provisions

13.1. **Policy Updates**

• This Policy will be updated periodically to reflect changes in Polish law, EU regulations (including MiCA), and relevant AML/CTF best practices.

13.2. **Management Responsibility**

• The Management Board of Comfort Life Tech Sp. z o.o. bears ultimate responsibility for effective implementation and oversight of the AML/CTF framework.

13.3. **Entry into Force**

• This Policy enters into force on the date approved by the Company's Management Board and is binding on all employees, officers, and agents of the Company.

SIGNATURES

Approved by:
Name/Title: president of the Management Board

Date: April, 01, 2025

Signature:
Oleg Goncharuk _____