

Real Estate and Service AP GmbH carries out activities related to digital assets secured by real assets (real estate and agricultural infrastructure). All token-related transactions are subject to mandatory AML/KYC procedures in accordance with Swiss law.

Real Estate and Service AP GmbH

Registered in Zug, Switzerland

Last Updated: ____ March 25th, 2025 ____

1. Introduction

Real Estate and Service AP GmbH (hereinafter “the Company”) is committed to implementing robust Anti-Money Laundering (AML) and Know Your Customer (KYC) measures in compliance with Swiss Financial Market Supervisory Authority (FINMA) regulations, FATF recommendations, European AML Directives, and Swiss Money Laundering Act (GwG).

The Company operates globally, including serving EU-based clients and partners. While adhering primarily to Swiss regulations (GwG, FINMA), this policy incorporates EU AML Directives (e.g., AMLD6) to ensure compliance with cross-border transactions and international best practices.

This policy outlines the procedures for preventing financial crimes, detecting suspicious activities, and ensuring full regulatory compliance.

2. Regulatory Compliance

Real Estate and Service AP GmbH is committed to full compliance with **Swiss, EU, and international anti-money laundering (AML) and counter-terrorism financing (CTF) regulations**. The Company ensures adherence to the following regulatory frameworks:

- **Swiss AML Law (GwG) and FINMA Circular 2017/1**, governing AML/CTF compliance for financial intermediaries and blockchain-related activities.
 - **EU’s 6th Anti-Money Laundering Directive (AMLD6)** – applied to cross-border transactions involving EU-based clients, participants, or counterparties.
 - **Financial Action Task Force (FATF) Standards** – ensuring compliance with global best practices for AML/CTF and digital asset regulation.
 - **Money Laundering Reporting Office Switzerland (MROS) Guidelines** – ensuring **suspicious activity reporting (SARs) and transaction monitoring**.
 - **OFAC, UN, EU, and Swiss Sanctions Lists** – screening all clients, transactions, and business partners to prevent interactions with sanctioned individuals or entities.
-

2.1 Scope of Regulatory Alignment

While **Real Estate and Service AP GmbH** is headquartered in **Switzerland**, its AML/CTF policies incorporate elements of **EU AML Directives (e.g., AMLD6)** and **FATF** to ensure seamless compliance in **cross-border transactions**. The policy extends beyond Swiss regulations due to:

- **International Transactions** – The Company engages with participants, token holders, and partners from multiple jurisdictions, requiring alignment with EU AML standards to facilitate global compliance.
 - **Financial Institution Requirements** – Many banking and payment partners impose **EU AMLD6 and FATF compliance requirements** for transactions, regardless of Switzerland's non-EU status.
 - **Proactive Regulatory Alignment** – As AML regulations evolve, the Company ensures **voluntary compliance with EU AML Directives** and emerging **Swiss FINMA/FATF guidance** on virtual assets and tokenization.
-

2.2 Mandatory KYC & AML Screening

To ensure regulatory compliance, all participants, token holders, participants, and business counterparties must undergo mandatory KYC verification and AML due diligence before engaging in transactions with the Company. This includes:

- **Identity verification (ID, proof of residence, biometric checks)**
- **Source of funds analysis** for transactions exceeding CHF 50,000
- **Ongoing transaction monitoring** using AI-driven compliance tools
- **Enhanced Due Diligence (EDD) for high-risk clients** (e.g., PEPs, offshore entities)
- **Screening against global sanctions and watchlists (OFAC, EU, Swiss, UN, INTERPOL)**

Failure to meet these compliance requirements will result in **immediate restriction of services and regulatory reporting** where necessary.

3. Customer Due Diligence (CDD) & KYC Procedures

To mitigate AML risks, the Company applies a **risk-based approach (RBA)** in assessing customers and transactions. The following measures are in place:

3.1 Identification & Verification

All customers must provide:

- **For Individuals:**

- Government-issued **passport or national ID**
- **Proof of address** (utility bill, bank statement, or rental contract, issued within the last 3 months)
- **Selfie verification** (to ensure liveness check)
- **For Companies:**
 - **Company registration certificate**
 - **List of ultimate beneficial owners (UBOs)**
 - **Directors' ID copies & proof of address**
 - Financial statements or tax declaration (for high-value participants)

3.2 Risk-Based Classification

Customers are categorized into **low, medium, and high-risk profiles**:

| Risk Level | Criteria | KYC Requirements |
|--------------------|---|--|
| Low Risk | Swiss/EU citizens, verifiable income, no political exposure | Standard KYC |
| Medium Risk | Investors from non-EU jurisdictions, large transactions | Enhanced due diligence (EDD) |
| High Risk | Politically Exposed Persons (PEPs), offshore entities, complex ownership structures | Extensive due diligence, source of wealth verification |

3.3 Politically Exposed Persons (PEPs) & Sanctions Screening

- All customers are screened against global PEP and sanctions lists (OFAC, EU, UN, Interpol, Swiss Watchlists).
- PEPs require senior management approval and enhanced monitoring.
- Transactions involving sanctioned countries or high-risk jurisdictions are automatically declined.

4. Transaction Monitoring & Suspicious Activity Reporting (SARs)

4.1 Transaction Monitoring System

- All transactions above **CHF 15,000** trigger **manual review**.
- AI-powered **real-time blockchain analysis tools** (Chainalysis, CipherTrace) detect anomalies in **crypto transactions**.
- Fiat transactions are monitored via **Swiss-regulated banks (UBS, Credit Suisse)**.
- Multi-signature authentication is required for transactions exceeding **CHF 100,000**.
- Token holders engaging in **secondary sales** must undergo **wallet verification and KYC screening** before funds are released.
- Blockchain analytics tools (Elliptic, Chainalysis, CipherTrace) will be used for forensic monitoring.

- **Blacklist for privacy-focused cryptocurrencies** (Monero, Zcash, Tornado Cash).
- **On-Chain Transaction Scoring** – Mandatory **risk rating for wallets** that interact with high-risk exchanges.
- **Whitelist Approved Crypto Wallets** – Ensure transactions **only occur via verified custodial wallets**.

4.2 Red Flags for Suspicious Activities

The Company reports any of the following red flags to **Money Laundering Reporting Office Switzerland (MROS)**:

- ✓ Unusual transaction patterns (rapid deposits/withdrawals without clear rationale)
 - ✓ Large transactions from high-risk jurisdictions
 - ✓ Attempts to bypass KYC procedures
 - ✓ Use of multiple wallets/accounts to obscure the source of funds
 - ✓ Anonymous transactions or transactions involving privacy coins (e.g., Monero, Zcash)
-

5. Digital Identity Verification & AI-Based Compliance Tools

5.1 To streamline KYC onboarding and improve fraud prevention, the Company implements **automated identity verification** via:

- **AI-powered KYC providers** (SumSub, Onfido, Trulioo)
- **Liveness detection & biometric authentication**
- **Blockchain transaction risk scoring** (Chainalysis, Elliptic)
- **Automated re-screening of accounts every 6 months**

5.2 AML Risk Management for DeFi & DEX Transactions

- The Company actively monitors DeFi interactions to prevent illicit activity.
 - **On-chain analytics tools** will track transactions involving **flagged addresses, Tornado Cash interactions, or suspicious counterparties**.
 - Any identified suspicious activity will be **reported to FINMA and MROS** immediately.
-

6. Source of Funds & Enhanced Due Diligence (EDD)

For transactions exceeding **CHF 50,000**, the Company requires:

- **Tax declarations or financial statements**
- **Business contracts proving income source**
- **Bank account ownership confirmation**

- **Video interview verification**

Additional Criteria for High-Risk Transactions (\geq CHF 100,000)

- **Third-party verified asset declarations** from licensed auditors.
- **Enhanced background checks using open-source intelligence (OSINT).**
- **Mandatory quarterly EDD reviews for high-risk customers.**

All high-risk customers undergo **quarterly compliance reviews.**

7. AML Training & Compliance Audits

- **Quarterly AML training** is mandatory for all employees handling transactions.
 - Compliance officers must undergo **annual certification.**
 - **Bi-annual AML audits** are conducted by **external Swiss compliance firms.**
 - **Whistleblower protection program** encourages employees to report suspicious activities.
-

8. Fund Storage & Custody Measures

Fiat funds are stored exclusively in **regulated Swiss banks (UBS, Credit Suisse).**

Crypto-assets are secured in **insured institutional-grade cold storage wallets (Fireblocks, Ledger Vault).**

Multi-signature authentication is required for transactions exceeding **CHF 100,000.**

9. Reporting Obligations

The Company **immediately reports** any suspicious activities to:

- **Money Laundering Reporting Office Switzerland (MROS)**
 - **Swiss Financial Market Supervisory Authority (FINMA)**
 - **Swiss Federal Tax Administration (SFTA) for tax compliance reporting**
-

10. Data Protection & Confidentiality

All KYC data is stored in compliance with:

- **Swiss Federal Data Protection Act (DPA)**
- **EU General Data Protection Regulation (GDPR)**
- **Secure cloud storage with AES-256 encryption**

- The company maintains **10-year records** of all KYC/AML data.

Customers may **request deletion of their data** in compliance with GDPR.

11. Enforcement & Penalties for Non-Compliance

Non-compliance with AML/KYC regulations will result in:

- Immediate **account suspension**
- **Legal prosecution** under Swiss AML Law (GwG)
- Reporting to **MROS and Swiss regulatory bodies**

The Company **reserves the right to block accounts, freeze funds, and terminate business relationships** if illegal or suspicious activities are detected.

12. Final Provisions

This AML/KYC Policy is binding for all customers, partners, and participants. By engaging with Real Estate and Service AP GmbH, users agree to undergo all necessary AML/KYC procedures.

The Company reserves the right to **update this policy** in compliance with **Swiss and international regulations**.

Sign-Off & Legal Compliance

Andrii Petrovitskyi 
CEO, Real Estate and Service AP GmbH

Date: ____ March 25th, 2025 ____

Location: Zug, Switzerland