

KYC & AML Policy

Sustainable Digital Assets (SDA)

Version 1.0

Last updated: 18 August 2025

Summary

This policy explains how SDA identifies and verifies customers, applies AML/CTF controls, and implements the Crypto-Asset Transfer Rule. We operate a phased onboarding model: Phase 1 (presale utility-token access) and Phase 2 (regulated security-token/equity features).

Primary contacts:

- **Compliance:** compliance@sdafinance.com
 - **DPO:** privacy@sdafinance.com
-

Key Points

- Below €1,000 cumulative: wallet and IP identification.
 - €1,000 or higher: Full KYC is mandatory.
 - Phase 2 access (security-token/equity features) requires Full KYC/KYB, refreshed screening, investor categorisation, and Travel-Rule-ready wallets.
 - We apply risk-based EDD (PEPs, high-risk geographies, complex SoW).
 - Travel Rule data exchanged on all external crypto transfers; self-hosted wallets > €1,000 require ownership proof.
-

1. Scope & Legal Basis

This policy covers onboarding, monitoring, and off-boarding of natural persons and legal entities interacting with SDA's token lifecycle. We follow applicable EU AML/CFT rules (including the Crypto-Asset Transfer Rule) alongside investor-protection duties where relevant. Local laws may impose additional requirements in certain jurisdictions.

2. Phase 1 — Presale / Utility-Token Access

Who: presale participants and holders during the utility-token phase.

We collect (everyone):

- Self-declaration: PEP status and sanctions screening.
- **Wallet checks:** proof of ownership (signed message or micro-tx loopback) for payout/withdrawal addresses.

Tiering during Phase 1:

- **Tier A (under €1,000 cumulative, low risk):** – Wallet and IP identification only. – Self-declaration PEP/sanctions status; geofencing for restricted countries.
- **Tier B (≥ €1,000 or heightened risk):** – Photo ID capture + automated liveness/face-match or robust bank-KYC evidence (e.g., SEPA account in same name). – **Full KYC** before further funding, voting, withdrawals or profit-sharing; apply **EDD** where flags exist.

3. What “Full KYC” Means (Standard)

Individuals

- Government ID (passport/ID card/driver’s licence) + liveness/face-match; second document if needed.
- **Proof of address** (≤3 months): utility bill, bank/credit statement, government letter.
- Sanctions/PEP/adverse media cleared; PEPs require senior approval (EDD).
- Purpose & intended use; expected activity profile.
- **Source of Funds** (SoF) for the transaction; **Source of Wealth** (SoW) where size/risk warrants (e.g., payslips, tax returns, sale contracts, audited statements, exchange withdrawal histories).
- Ongoing monitoring and periodic refresh.

Entities (KYB)

- Legal name, registration number, registered address, formation documents/registry extract; LEI where available.
- **Ownership & control:** identify UBOs ≥25% or effective control; Full KYC on UBOs and directors/signatories.
- Business profile, licences (if applicable), expected activity.
- SoF/SoW at entity and UBO levels as appropriate.
- Sanctions/PEP/adverse media at entity/UBO/director levels; ongoing monitoring.

4. Phase 2 — Security-Token / Equity Features

Who: clients converting to, receiving, or transacting SDA's regulated security-token and any equity-linked rights.

Required before Phase 2 access:

- **Full KYC/KYB** completion and approval.
- **Refreshed screening** (sanctions/PEP/adverse media).
- **Investor categorisation** (retail vs. professional). If we give advice/portfolio-style features: record appropriateness/suitability questionnaires.
- **SoF/SoW evidence** aligned to transaction size/risk and distribution flows.
- **Travel Rule** readiness for any on/off-ramp crypto movements; self-hosted wallets > €1,000 require ownership proof.

5. Travel Rule (Crypto Transfers)

We collect and transmit required **originator/beneficiary** data for external crypto-asset transfers. For **CASP-to-CASP** transfers, we exchange data using industry-standard messaging. For **self-hosted wallets**, we apply **ownership-proof** procedures; above **€1,000**, we verify control (message-sign or loopback tx). Transfers lacking minimum data or with unresolved red flags are **rejected or held** pending review.

6. Risk-Based Approach & EDD

We score risk across **customer, geography, product, delivery channel, and behaviour**. **EDD** applies to: PEPs, high-risk jurisdictions/sectors, complex ownership, unusual velocity/structuring, or adverse media. EDD measures may include senior-management approval, stricter SoF/SoW, lower limits, or refusal/exit.

7. Acceptable Documents (Annex)

ID: passport; national ID; driver's licence (where accepted).

Address: bank/credit statement, utility bill, government letter, lease/tenancy (with authority contact), property tax.

SoF/SoW (examples): payslips, employment contract, audited statements, tax returns, company sale docs, inheritance/probate, exchange withdrawal history with bank trails.

8. Data Protection & Retention

We store only data needed for AML/CTF, onboarding, servicing, and legal obligations. KYC and transactional records are retained for the legally required period and then **deleted or anonymised**. You may exercise privacy rights via privacy@sdafinance.com (subject to AML retention exemptions).

9. Record-Keeping

We maintain reproducible records of **who was identified, how, and when**, including screening results, SoF/SoW evidence, investor categorisation (Phase 2), and Travel Rule data exchanges.

10. Moving from Phase 1 → Phase 2 (Client Checklist)

- ✓ Completed **Full KYC/KYB** (ID + PoA + screening).
- ✓ Provided **SoF/SoW** aligned to investment size.
- ✓ Declared **investor category**; completed any required questionnaires.
- ✓ Registered **wallets** with ownership proof (especially for self-hosted > €1,000).
- ✓ Acknowledged policy & disclosures.

11. Sanctions & Restricted Territories

We do not onboard customers in **sanctioned** or **prohibited** jurisdictions. We may apply additional controls or decline service in **high-risk** locations or sectors consistent with our risk appetite and legal obligations.

12. Contact Compliance

Questions or escalations: compliance@sda fintech.com

13. Revision History

v1.0 — 18 Aug 2025: Initial publication; Phase 1/Phase 2 split; Travel Rule procedures; investor categorisation for Phase 2.

Frequently Asked Questions

Q: Do I need KYC below €1,000? A: Yes—below €1,000 we require wallet and IP identification plus self-declaration. Full KYC starts at €1,000 cumulative or if risk flags appear.

Q: What's different in Phase 2? A: You must complete Full KYC/KYB, refresh screening, provide SoF/SoW, declare investor category, and use Travel-Rule-ready wallets.

Q: Can I use a self-hosted wallet? A: Yes, with ownership proof; above €1,000 we require signed-message or micro-transfer verification.

Q: How long do you keep my data? A: For the legally required period to meet AML/CTF obligations; then we delete or anonymise.

Q: I'm a company — what's required? A: KYB docs, UBO identification (≥25% or effective control), Full KYC on UBOs/directors, and SoF/SoW evidence.