Anti-Money Laundering (AML) Policy

April — operated by Muskays Ltd. · Company No. C 110169 · Malta
Version 3 · Last updated: 14 August 2026

1. Introduction

Muskays Ltd. (the “Company”) is a Malta-registered affiliate marketing company operating the April affiliate platform accessible at aprilftd.com (the “Platform”). The Company connects sub-affiliates with licensed online gambling operators and generates revenue through Cost Per Acquisition (CPA), Revenue Share, hybrid, and fixed-fee commercial agreements.

The Company receives commissions from operators partly in fiat currency (EUR) and partly in stablecoin (USDT), and may settle certain sub-affiliate payments in fiat or in stablecoin. All such flows are processed through regulated financial institutions or regulated virtual asset service providers (VASPs) and are fully reconciled in the Company’s accounting records.

The Company is committed to preventing money laundering, terrorist financing, and other financial crimes. This policy sets out the procedures and controls in place to ensure compliance with applicable anti-money laundering legislation, including the Prevention of Money Laundering Act (PMLA) of Malta and relevant EU directives.

2. Scope

This policy applies to the Director, all employees, contractors, sub-affiliates, and any third parties acting on behalf of Muskays Ltd. in connection with the April Platform. It covers all business activities, including affiliate marketing agreements, fiat and crypto-asset payment processing, and relationships with sub-affiliates and gambling operators.

3. AML Compliance Responsibility

The Director of Muskays Ltd. is responsible for overseeing AML compliance, including the implementation and enforcement of this policy. The Director is the designated Money Laundering Reporting Officer (MLRO) and is responsible for:

- Ensuring the Company complies with all applicable AML obligations.
- Receiving and reviewing internal suspicious activity reports.
- Filing reports with the Financial Intelligence Analysis Unit (FIAU) of Malta where required.
- Maintaining records in accordance with legal requirements.
- Reviewing and updating this policy periodically.

4. Customer Due Diligence (CDD)

The Company conducts due diligence on all business partners before entering into any commercial agreement.

4.1 Online Gambling Operators (Advertisers) — Before entering into any commercial agreement with an Advertiser, the Company performs the following checks:

- Verification that the operator holds a valid gaming license issued by a recognized regulatory authority, including but not limited to the Curacao Gaming Authority, the Malta Gaming Authority (MGA), the UK Gambling Commission (UKGC), or other reputable gaming regulators.
- Collection of company registration details and registered address.
- Identity verification of key directors or beneficial owners where applicable.
- Review of license certificates via official regulatory websites prior to signing any agreement.
- Ongoing monitoring of license validity throughout the commercial relationship.

4.2 Sub-Affiliates — Sub-affiliates engaged through the April Platform are independent contractors. At onboarding, the Company collects basic identification and contact information for the purpose of executing the commercial relationship and processing payments, including:

- Full legal name (or company name, where applicable).

- Contact email and country of residence.
- Bank account details and/or, where payment is made in crypto-assets, the receiving wallet address.

The Company ensures that payment methods used are legitimate and traceable. Where unusual patterns or red flags are identified, additional verification may be requested at the discretion of the Director.

5. Accepted Payment Methods

The Company accepts and processes payments through the following methods only:

- Bank wire transfer (SEPA and international SWIFT).
- PayPal.
- Crypto-asset transfers in established stablecoins (primarily USDT), sent and received through regulated exchanges or virtual asset service providers (VASPs) and identified wallet addresses.

The Company does not accept cash payments under any circumstances. All fiat payments are processed through regulated financial institutions and all crypto-asset payments are processed through regulated VASPs or identified, traceable wallets, ensuring full traceability of funds in accordance with AML standards.

6. Crypto-Asset Transactions and Controls

Given that a portion of the Company’s revenue is received, and certain payments are made, in stablecoin (USDT), the following specific controls apply:

- Crypto-asset transactions are conducted only in established stablecoins (primarily USDT) and only through regulated exchanges / VASPs that apply their own KYC/AML procedures, or with identified counterparties whose wallet addresses are recorded.
- Privacy coins, mixers, tumblers, and any anonymity-enhancing services are not used or accepted under any circumstances.
- Counterparty wallet addresses are recorded and, where appropriate, screened using blockchain-analytics tools to detect links to sanctioned, illicit, or high-risk sources.
- Source of funds and source of wealth checks are applied to material crypto inflows on a risk-sensitive basis.
- Each crypto-asset transaction is recorded with the transaction hash, wallet addresses, asset, amount, fiat-equivalent value at the transaction date, and counterparty, and is reconciled in the Company’s accounting records.
- Enhanced due diligence is applied where a crypto-asset counterparty, wallet, or transaction pattern presents a higher risk profile.

7. Suspicious Activity Reporting

Any contractor, employee, sub-affiliate, or representative who suspects that a transaction or activity may be linked to money laundering or terrorist financing must immediately report their concerns to the Director (MLRO). Reports should include all relevant information and supporting documentation.

The MLRO will review the report and, where appropriate, submit a Suspicious Transaction Report (STR) to the Financial Intelligence Analysis Unit (FIAU) of Malta. Tipping off the subject of the report is strictly prohibited and may constitute a criminal offense under Maltese law.

8. Red Flags and Enhanced Due Diligence

The Company pays particular attention to the following indicators, which may warrant enhanced due diligence:

- Counterparties registered in jurisdictions identified as high-risk by the FATF or the EU.
- Unusual transaction patterns inconsistent with the known commercial profile.
- Reluctance from a counterparty to provide standard identification or business documentation.
- Requests for payment routing through unrelated third parties or jurisdictions.
- Counterparties or beneficial owners appearing on international sanctions lists.

- Crypto-asset payments routed through mixers, tumblers, privacy coins, or wallets linked to illicit activity, or the structuring of transactions across multiple wallets to obscure their origin.

9. Record Keeping

The Company maintains records of all CDD documentation, business agreements, invoices, fiat and crypto-asset transaction records (including transaction hashes and wallet addresses), and AML-related communications for a minimum period of five (5) years from the end of the business relationship or the date of the transaction, whichever is later, in accordance with Maltese law.

10. Training and Awareness

All individuals working with or on behalf of Muskays Ltd. are made aware of their AML obligations. The Director ensures that relevant personnel are informed of this policy and any updates to applicable regulations, and arranges training sessions where appropriate.

11. Policy Review

This policy is reviewed annually or whenever there is a material change in the Company’s business activities, ownership, or applicable legislation. The Director is responsible for approving any updates to this policy.

12. Contact

For any question regarding this policy or to report a suspected violation, contact the MLRO at admin@muskays.com.

Approved by: Director, Muskays Ltd.

Date: 14 August 2026