AML Policy

1. General Provisions

Viralles (hereinafter the “Company”) is committed to maintaining high standards in combating money laundering (AML) and terrorist financing (CFT).

The Company takes the necessary measures to ensure that Clients, Investors, Agents, Intermediaries and other entities involved in its business are not involved in unlawful activities, including but not limited to money laundering, terrorist financing, proliferation of weapons of mass destruction, purchase and sale of narcotic drugs, blackmail, smuggling, concealment of corruption schemes, tax evasion and cybercrime.

This Policy provides general information to prospective and existing Clients of the Company and sets out the Company’s general obligations regarding Client verification and the measures taken to detect and prevent money laundering and terrorist financing.

Before registering a trading account on the platform, the Client confirms that they have read and agreed to the Company’s Anti-Money Laundering Policy and the List of Prohibited Jurisdictions.

2. What Is Anti-Money Laundering (AML)?

Anti-money laundering (AML) refers to a set of measures, procedures and legislative acts aimed at detecting and preventing attempts to convert illegally obtained funds into lawful assets.

Concealing the source of funds from financial regulators or law enforcement authorities constitutes a financial crime and entails serious consequences.

One consequence of the rapid development of the financial industry has been the introduction of legal instruments and laws aimed at combating money laundering. These internationally recognized measures have made it more difficult for companies and individuals involved in illegal activities to evade regulatory and law enforcement authorities.

3. Anti-Money Laundering and Counter-Terrorist Financing Policy Adopted by Viralles

The Company fully complies with the laws, statutes and regulations of the Cook Islands aimed at combating money laundering and terrorist financing. Further details of these laws and regulations can be found on the website of the Cook Islands Financial Supervisory Commission (FSC).

Money laundering and terrorist financing are criminal offences under the laws of the Cook Islands.

In accordance with the Financial Transactions Act 2017 (FTRA), the Company has developed the following Anti-Money Laundering and Counter-Terrorist Financing Programme (hereinafter the “AML Programme”).

3.1 Establishment of an AML/Compliance Department

The AML Department oversees Viralles's compliance with the AML Programme. The AML Department is responsible for: developing, implementing and updating the internal anti- money laundering policy in accordance with FTRA; training Company employees to identify suspicious financial transactions; assisting the Financial Intelligence Unit in detecting and preventing suspicious financial activity; reporting to the Board of Directors and senior management on compliance with the AML Programme and financial risks; and verifying and monitoring the Company's Clients.

The AML Department is headed by a senior AML officer (MLRO) appointed by the Board of Directors.

3.2 Mandatory Know Your Customer (KYC) Policy

The Know Your Customer (KYC) Policy is a mandatory procedure for verifying the Client's identity. It helps protect the interests of Clients and the Company by minimizing the risk of unlawful activity.

Under applicable legislation, financial institutions are prohibited from opening anonymous trading accounts.

The KYC procedure includes, but is not limited to, verification of the following Client information: (1) authenticity of documents; (2) accuracy of personal data; (3) email address and telephone number; and (4) country of residence.

The Company reserves the right to request additional information to complete the KYC procedure where necessary. Incomplete or inaccurate information provided by the Client may result in refusal or termination of services.

Clients are verified by submitting documents electronically through a third-party service provider.

Confidential information collected by the Company may be disclosed to a third party only where the request for such information has been made in accordance with applicable law.

Questions relating to the KYC procedure should be sent to info@viralles.com.

3.3 Automated Risk Assessment System

The Company uses an automated risk assessment system to detect unreliable Clients and high-risk transactions. The Company reserves the right to configure and modify this system as necessary.

The AML Department regularly monitors Clients flagged by the risk assessment system. For security reasons, the Company does not make information about its risk assessment system and internal procedures publicly available. Based on data analysis, the AML Department assesses risks and takes necessary measures.

3.4 Informing Company Employees About the AML Policy

The AML Policy applies not only to persons seeking to legalize illegally obtained funds but also to employees of financial institutions involved in monitoring and processing transactions.

The AML Department regularly informs Company employees about AML instructions and conducts training to identify suspicious patterns used by organizations and individuals to launder money. If an employee suspects misconduct while processing transactions on the basis of AML instructions and this Policy, the employee refers the information to the head of the department and the AML Department for further investigation.

3.5 Politically Exposed Persons (PEPs)

For the purposes of this Policy, the term “Politically Exposed Person” (PEP) is defined in accordance with section 3 of the Financial Transactions Act (FTRA) and includes: (1) an individual holding an important public position domestically or internationally; and (2) family members and associates of that individual as defined by FTRA.

A Client who has PEP status must provide the AML Department with copies of documents confirming that status. Copies must be sent to info@viralles.com before the trading account is registered on the platform.

Every case of establishing a business relationship with a PEP is discussed individually between the interested parties in accordance with applicable law.

The Company is required by applicable law to obtain information about PEPs who use its services. The Company reserves the right to use third-party services to verify PEP status and request additional information where necessary.

3.G Sanctioned Persons

Viralles does not provide services to sanctioned persons.

For the purposes of this Policy, a “sanctioned person” means any individual or legal entity included in any sanctions-related list of specially designated persons, including but not limited to: the US OFAC consolidated non-SDN sanctions list; the US OFAC Specially Designated Nationals and Blocked Persons (SDN) list; Interpol notices; the EU consolidated financial sanctions list; Israeli lists of terrorist organizations and unauthorized associations; the UN Security Council consolidated list; and other sanctions lists.

Prospective Clients who appear on a sanctions list are prohibited from registering trading accounts on the platform.

Clients whose sanctions status changes so that they are included on any sanctions list must immediately report this by email to info@viralles.com.

The Company reserves the right to use third-party services to identify and verify the sanctions status of Clients and may request additional information if it considers this necessary.

4. Retention of Personal Data

The Company reserves the right to store and process personal data obtained during Client identification, verification and financial transactions, including but not limited to: (1) information provided by the Client for identity verification; (2) methods used to deposit and withdraw funds; (3) information about the Client obtained from public databases; and (4) any discrepancies identified during Client identity verification. The Company retains personal data in English for six years from the date of the last financial activity in the Client's personal account or closure of the Client's account. The Company also retains information concerning suspicious Client activity for six years.

For Viralles

Head of Legal Department



Facsimile

S.Langeland