

# ANTI-MONEY LAUNDERING GENERAL POLICY SUMMARY



## 1. The Company

**Evalect Digital UAB** (hereafter the "Company") is responsible for the protection of privacy and the safeguarding of clients' personal and financial information. By opening an account with the Company, the client hereby gives its consent to such collection, processing, storage and use of personal information as explained below. **Evalect Digital UAB** is a company conducts its financial activity as a Virtual currency exchange operator and Depository virtual currency wallet operator under the supervision of Financial Crime Investigation Service (FNIT) of the Interior Ministry of the Republic of Lithuania with Company No: 305970229 (hereinafter referred as "the Company")

## 2. Our Core Principals

The Company is actively working to prevent all Financial Crime (FC) related activities such as Money Laundering (ML) and Terrorist Financing (TF). To prevent such activities the Company constantly works to verify the identity of all clients, and where necessary to assist government agencies and financial intelligence units (FIUs) with their effort to combat ML and TF.

Money Laundering ("ML") is an activity which involves hiding, disguising, or legitimizing the true origin and ownership of money used in or derived from committing crimes. Terrorist Financing ("TF") is generally the act of providing financial support to terrorism or terrorist organizations enabling them to carry out acts of terrorism. Terrorism financing does not necessarily involve illegitimate funds; in fact, it often uses legitimately obtained income and may involve relatively small amounts of money. Failure to comply with the AML/CTF Policy may lead to criminal, civil and/or regulatory sanctions, and penalties.

The company will comply with the AML/CTF laws, rules and regulations of the countries where the Company has permanent places of business in which the Company provides services. Company will engage with relevant regulators, authorities and/or law enforcement agencies in a constructive and cooperative manner (including with respect to information sharing).

### Company Opposes Criminal Undertakings:

Company opposes the crimes of money laundering and terrorist financing and maintains a framework to identify, mitigate and manage the risk that its products and services could be used for such purposes. Company will report to the applicable regulator, authority and/or law enforcement agency suspicious activity that may involve potential laundering, terrorism financing or other activity or transactions that are reportable as suspicious activity under applicable laws.

### Governance and Oversight:

Company recognizes the vital role of robust governance and oversight of its AML/CTF compliance structures. Senior management, including at the board level, have responsibility for managing the money laundering and terrorism financing risks identified by the Company by demonstrating active engagement in approach to mitigating these risks effectively. They also play a key role in fostering the attitude and culture embedded within the Company.

### Company Safeguards:

The company includes an assessment of AML/CTF risk in its financial crime risk assessment framework to ensure that it has a thorough understanding of the AML/CTF risk across the group, including identifying those business areas where such risk is higher. The company will:

# ANTI-MONEY LAUNDERING GENERAL POLICY SUMMARY



- use the risk assessments to ensure that it has proportionate systems and controls in place to identify, assess, monitor, and manage AML/CTF risk.
- apply a risk rating and corresponding level of due diligence standard to all client relationships.
- will maintain adequate safeguards on the confidentiality and use of customer information exchanged with regulators, including safeguards to prevent tipping off and will treat such information in accordance with its internal requirements regarding the confidentiality of data.
- will provide its products and services only for legitimate purposes to customers. Company may decide not to provide products or services based upon decisions guided by its ML/TF risk appetite.
- will take necessary steps to ensure that sufficient funding and resources are available for the implementation and performance of activities required by Macquarie's AML/CTF framework.
- will monitor the activity of its customers, their transactions, and its staff using a risk-based approach that is consistent with the level of money laundering and terrorism financing risk.
- will manage new and revised products, business processes and systems to ensure that money laundering and terrorist financing risks are identified, mitigated, and managed.

### 3. How to Verify your Evalect Digital UAB Account

Verification is a mandatory part of the process of registering with the Company's platform. Regulatory requirements dictate that we verify each new account without any exemptions. This keeps our platform secure and prevents untoward activity. Upon the completion of your account verification, you will be able to enjoy the full benefits of the Company's platform. To verify your account, you are required to provide both a proof of identity (POI) and proof of address (POA) as well as any other documents needed as part of the registration process or thereafter. Only after you provide us with all the necessary documents will your verification process begin.

To identify our clients, the Company may ask for personal data and take steps to confirm the accuracy of this information using various verification tools. It may take from 24 hours up to a couple of workdays to complete this process.

### 4. What is Needed from You

To be compliant with the regulatory requirements and at the same time be able verify your account, we have in place the following practices:

- All clients must submit valid identification documents (i.e. all info should be visible, valid, and not expired, clear, without cropping)
- Records of clients' identification documents are maintained by the Company.

**5. The Type of Documents Needed Will Depend on The Type of Your Accounts**

<b>Personal Accounts:</b>	<b>Corporate Accounts</b>
<p><u>Proof of Identity (POI):</u></p> <p>Your POI document should contain your name, date of birth, a clear photograph, issue date, and if it has an expiry date, that should be visible as well. A passport is the preferred proof of identity, as it is the document which will be quickest for the Company’s team to process. Alternatively, you can use a driving license or any other government-issued ID. If the document is double-sided, and there’s relevant information on the backside, make sure to upload that as well.</p> <p><u>Proof of Address (POA):</u> Your POA document should contain your full name, residential address and an issue date, which should be no older than 3 months. The name or logo of the issuer should also be clearly visible. Please make sure to scan your document against a different-colored background, so that all four corners are visible. Acceptable POA includes bank statement, credit card statement, electricity, water or gas bill, phone or internet bill, council tax bill, tax letter or bill, letter from your local municipality that contains your address</p>	<p>Certificate of Incorporation                      Memorandum &amp; Articles of Association                      Proof of address of the legal entity                      Director’s register                      Shareholders register                      Source of funds                      POI and POA for all directors                      POI and POR for every ultimate beneficial owner that owns 10% or more                      POI and POA for designated traders                      A resolution by the Board of Directors (BOD) of the Company to whom they grant authority to operate the trading account on behalf of the client .</p>

**Note: the above documents listed in the table prescribe the Company’s minimum requirements. Hence, the Company reserves its right to request any further documents deemed necessary.**

**6. Approval Process**

To minimize the risk of ML and TF, the Company does not accept cash deposits nor disburses cash under any circumstances. In addition, the Company reserves the right to refuse to process a transfer at any stage, where it believes the transfer is connected in any way to ML or criminal activity.

## 7. Risk Assessment

Company's AML Model is based on the understanding of the ML risks to which the Company is exposed as a result of its activity, taking into account risk factors including those relating to customers, countries or geographic areas, products, services, transactions or delivery channels. For this reason, company carries out a risk assessment at least once a year, which constitutes the necessary basis for identifying areas for

improvement in each entity's AML control framework and establishing, if necessary, additional mitigating measures to strengthen it.

## 8. Client Identification and Knowledge

**Evalect Digital UAB** implements due diligence measures with respect to clients and retains the documentation on the AML obligations. In general, BBVA obliged entities apply due diligence measures:

- via face-to-face or non-face-to-face means
- before establishing a new business relationship or executing one-off transactions which allow them to know and, when applicable, verify the source of funds and the purpose of the business relationship periodically, so that the available client information is updated

## 9. Client Segmentation by Level of Risk

Company segment clients according to the level of ML risk they present. The risk rating is kept up-to date as a result of continuous monitoring of the business relationship, determining the type and completeness of the due diligence measures with respect to the client. Clients who present a higher risk profile are subject to an enhanced due diligence process and to senior management approval (i.e. PEPs)

## 10. Monitoring of Operations and Reporting of Suspicious Transactions

Company has procedures and tools in place for continuous monitoring of the clients' business relationships and one-off transactions, in order to detect possible signs of money laundering or terrorist financing, and to notify the local Financial Intelligence Unit of the transactions presenting reasonable signs or suspicion of being related to money laundering or terrorist financing.

## 11. Sanctions Review

All individuals and entities will be subject to a review against applicable lists of sanctioned countries as published by the United Nations and will be periodically rechecked against updated lists. The Company will not accept sanctioned individuals / entities as clients.

## 12. Additional Queries

If you have any questions with reference to the documents stated above, please contact our support team at [support@evalectdigital.com](mailto:support@evalectdigital.com)