**Industry Standard on Anti-Money Laundering and Countering Financing of Terrorism**

## A. Preamble

The subject of this standard is the firm establishment of minimum requirements that include effective provisions for the prevention of money laundering and terrorist financing.

Even if not each member of the DLA holds the status of an entity subject to anti-money laundering obligations special attention shall be paid to the prevention of criminal activities through fintech lenders. Members shall implement appropriate processes for early detection and handling of suspicious cases and implement expedient measures to effectively prevent abuse in regard to money laundering or terrorist financing.

## B. Definitions

I. Money Laundering: Is the placement, layering (concealment) of the origin and integration of illegally obtained money or illegally acquired assets into the legal financial and economic.

II. Financing of Terrorism: This is the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, to commit or contribute to the commission of an offense within the meaning of the European legislation; currently, Directive (EU) 2017/541.

III. Identification: Gathering information for the purpose of confirming the identity of a legal or natural person.

IV. Verification: Verification of gathered information for the purpose of confirming the identity of a legal or natural person.

V. Business Relationship: A relationship which is connected with the professional activities of a member and where it can be assumed that at the time the business relationship is established, a know your customer (KYC) check is expected or required for such a business relationship. This includes one-off transactions as well as long-term business relationships.

VI. Transaction: Transaction is an act or, if there appears to be a connection between them, several acts that has or have as their purpose or effect or cause a movement of money or other assets.

VII. Politically Exposed Person (PEP): A natural person who is or who has been entrusted with prominent public functions and includes the following:

1. Foreign PEPs;

2. Domestic PEPs;
3. International organisation PEPs.

No public function referred to in points (a) to (c) shall be understood as covering middle-ranking or more junior officials.

## C. Structure and Indicators of Money Laundering

Money laundering takes place in several phases and can be detected using various indicators.

### I. Phases of Money Laundering

The United Nations Office on Drugs and Crime („UNODC“) has defined the process of money laundering in 3 phases (**link**):

#### 1. Placement

The goal is to bring the illegally obtained (cash) money into the financial and economic cycle. For this purpose, the money is often converted into other valuables, such as merchandise, diamonds or even investments. Often the money is deposited at home or abroad and if possible, here also converted into other currencies. This can also involve smaller amounts which in themselves are not considered "relevant" in terms of anti-money laundering law. Together, however, they add up to a significant amount. This procedure is called "smurfing". Therefore, all transactions of a business partner must always be considered as a whole.

#### 2. Layering

In this phase, the origin of the money is covered up. For this purpose, money is often transferred back and forth between accounts and also persons in various amounts by way of multiple transactions. Usually during this process banks are used, which are subject to less strict regulations. In the case of investments, one indicator may be that the customer indicates different deposit and withdrawal accounts. It is not uncommon for the origin of the money to be concealed by the money launderer faking the supposedly legal origin of the money by falsifying invoices, accounting records or contracts.

#### 3. Integration

After the origin of the money has been covered up and the money has been laundered, the goal of the third phase is to use the money for one's own benefit. The money is in turn converted into cash or new assets such as real estate, insurance or investments.

### II. Money Laundering Indicators

There are many indicators of money laundering. The following are some that are relevant to the work of Digital Lending services. However, they are not exhaustive in any way and should be understood as a guideline:

- Multiplicity of smaller investments in the same project, if the total amount is significant;
- Different deposit and withdrawal accounts;
- Accepting bad terms and conditions if better terms and conditions would be available;
- Specifying many different accounts;
- Refusal to provide identification.

These indicators do not necessarily establish money laundering in every case. However, they should cause the member to take notice and, if necessary, discuss the matter with their supervisory authorities. For the proper handling of actual suspicious cases please refer to section E. of this standard.

These indicators should be taken into account as part of the risk analysis (Section D. I.) and should be part of the principles for identification (Section D. II) and verification (Section D. III) measures developed from the risk analysis.

## D. Minimum Requirements

The following minimum requirements shall be taken into account.

### I. Risk Analysis

Members shall conduct a diligent, complete and appropriate risk analysis, which identifies and assesses the risk of money laundering and financing of terrorism. They should take into account different risk factors including those relating to their customers, operating countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the size, type, scope, complexity and risk content of the members' business activities.

The risk analysis shall be documented and be carried out / updated at least once a year.

### II. Identification

Members should ensure that they sufficiently identify their customers when establishing a business relationship in accordance with the KYC principles.

Where a member already holds the status of an entity subject to anti-money laundering obligations, it is required to comply with these obligations and implement the relevant measures in accordance with applicable law. The legal obligation to comply with these regulations also constitutes the legal basis for obligated members to collect the necessary personal data in the meaning of EURegulation 2016/679 („GDPR").

Non-obligated members shall, within the framework of the KYC principle, at their own discretion collect such personal data that are necessary for the member to be convinced that it knows the identity of the business partnerFurthermore, it should be convincingly established whether the business partner is a PEP.

### III. Verification

After identification, each member should take reasonable measures to verify the legal and natural person's identity, so that the member is sure it knows who the person is.

As long as there is no legal obligation to comply with money laundering regulations, the verification of identity should be performed by verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source as far as this is consistent with data protection requirements.
The identity verification procedures that will be implemented should be based on the evaluation of the risk analysis and data collected and should consider any risk factors that may be present.

### IV. Increased Duties of Care

Customers to whom risk factors or PEP status apply should be subject to increased duties of care - such as finding out where the funds for an investment come from.

### V. Monitoring of the Business Relationship

All members shall ensure that they keep the data that have been collected up to date to the extent possible.

An identity check must be repeated at regular periods to ensure that risk factors do not arise and to verify that the data collected is up to date.
The repeating period should be defined on a risk basis.

### VI. Screening of Company Staff

Employees and other persons closely involved with a member should be screened for general characteristics of suspiciousness by, at a minimum, conducting a plausibility check of the information provided by such a person.

### VII. Designation of Responsibility

Each member should designate a department or person within the company to handle the topic anti-money laundering and countering financing of terrorism and who also receives internal suspicious activity reports.

This department or person is responsible for maintaining measures to prevent money laundering and financing terrorism and serves as a point of contact for suspicious activity reports.

This department or person should have sufficient authority within the company as well as its employees and should be involved in product development processes at an early stage in order to be able to adequately assess the impact on prevention measures.

### E. Suspicious Cases

Suspicious cases can be identified on the basis of various risk factors. These may include:

- Unusually high transactions;
- Different incoming and outgoing bank accounts;
- Different senders and recipients for money transfers;
- domicile/ residence in high-risk countries.

Internal anonymous reporting channels should be established for reports to the internal responsible department or person.

### F. Training

In general, every person in the company of the member should be instructed about the potential dangers of money laundering and financing terrorism and made aware of the risk factors.

Employees of members obliged under anti-money laundering law must be trained and tested on the prevention of money laundering or financing of terrorismat least at the time of engagement and on a regular basis, i.e. at least once a year. This also applies to the members of management.

In addition, employees and management should be trained on how to react in cases of suspicious activity related to money laundering and financing of terrorism.

### G. Recording and Storing of Gathered Personal Data

Each member should be aware of any retention requirements that may exist in order to comply with the principles of data protection.

### H. Controls of Compliance with this Industry Standard

The members shall have plans in place for regular monitoring of compliance with this industry standard and specify the allocation of responsibilities. The results shall be reported to a member’s management.

### I. Comply or Explain

As a general rule, there shall be no deviation from the provisions of this industry standard.

As business models differ quite significantly from each other, depending on the size, type, scope, complexity and risk level of business activities, the standard is open to implementation in different dimensions or even only partially. In case the members deviate

from the standard, they shall disclose which parts they implement differently and provide comprehensible reasoning towards the DLA Secretariat.

## J. Revision Clause

This industry standard shall be subject to revision by the Committee on Legal & European Affairs of the Digital Lending Association at two-year intervals. Any amendments and/or additions shall be approved by the General Assembly by qualified majority.