

Industry Standard on Compliance Management

A. Preamble

The Digital Lending Association is the central representative body of the Digital Lending ecosystem. Its affiliated members stand for the professional, honest and transparent operation of their businesses as well as the fulfillment of the highest quality standards in the interest of debtors, investors, and business partners. With the adoption of the "General Principles and Rules of Conduct" by the General Meeting on 4 June 2019, these self-imposed standards were codified. In accordance with the Articles of Association, all Ordinary Members undertake to comply with these principles and rules.

By resolution number 30 of the Board of Directors on 29 May 2020 (30-VS-200529-1), it was decided to flesh out these General Principles and Rules of Conduct by developing individual standards and thus set benchmarks for the entire industry. The authority to adopt them as "Industry Standards" lies with the General Meeting.

The subject of this standard is the firm establishment of Sections I/1 and IV/7 of the General Principles and Rules of Conduct.

The aim of the standard is to develop and promote an industry-wide "compliance culture" based on a common understanding of how to monitor and control compliance risks.

B. Definitions

- I. Employee: this is a person who is permanently employed or freely employed by the member. Interns are also employees for this purpose.
- II. Conduct: This is any act, acquiescence, or omission.
- III. Regulatory Framework: This includes the applicable legal framework, regulatory circulars, standards, guidelines and recommendations, the General Association Principles and Rules of Conduct together with the industry standards that substantiate them, and internal company policies and processes.

C. Industry Standard on the Compliance Officer

The Member shall have an organization that ensures that compliance with the regulatory framework and the measures taken to remedy deficiencies are continuously monitored and evaluated. In order to effectively counteract the risks that may arise from non-compliance, it is necessary to permanently establish a preventive and process-accompanying compliance organization that performs its duties independently. For this purpose, the member shall permanently appoint a Compliance Officer and designate him/her as "Compliance Officer" (m/f/d).

The Compliance Officer shall have a broad range of practical experience as well as a sufficient level of professional competence and judgment to adequately and effectively perform the tasks of the compliance function and to safely assess conflicts of interest. At a minimum, this includes:

- Knowledge of national and EU level laws, regulations, guidelines, guidance, etc. relevant to the member's business.

- Knowledge of the organization and responsibilities of the relevant supervisory authorities.
- Knowledge of the requirements and design of appropriate processes to prevent and detect breaches of (regulatory) legal, association and internal requirements.
- Experience in setting up monitoring plans and exercising control actions.
- Experience in various operational or control functions.

The Executive Board is responsible for ensuring compliance with the applicable regulatory framework as well as the measures taken to remedy deficiencies and their monitoring by the Compliance Officer. The Compliance Officer therefore reports directly to the Executive Board. They can also be linked to other corporate units if there is a direct reporting line to the management. A link to internal auditing is excluded. Depending on the type, scope, complexity and risk content of the business activities as well as the size of the member, the task of compliance officer may also be assigned to a managing director as an exception.

The tasks, powers and reporting duties of the Compliance Officer shall be set out in writing. These shall also include provisions on deputization in order to ensure the proper performance of duties of the compliance function during absences.

D. Industry Standard on Controls

In the first instance, each operational business unit of the member is itself responsible for compliance with the applicable legal framework, the General Principles and Rules of Conduct together with the industry standards that concretize them, internal policies and processes, and for the implementation of controls (first line of defense).

Downstream, the Compliance Officer regularly monitors, on a risk-based basis, whether the regulatory framework is actually being complied with and whether controls are being carried out (second line of defense).

The Compliance Officer must be granted sufficient authority and unrestricted access to all information required to perform their duties. Instructions and resolutions of the management of importance for the monitoring and control by the compliance officer must be communicated to them without delay. This also applies to significant changes in the regulations designed to ensure compliance with the regulatory framework.

A monitoring plan must be drawn up annually, which includes all of the member's business areas. Based on the risk analysis, priorities shall be set in the monitoring plan to ensure comprehensive compliance risk monitoring. The purpose of the monitoring plan is to assess whether the member is fulfilling its obligations arising from the regulatory framework and whether the internal organization and processes are effective and appropriate.

Audits shall be conducted on-site and through the compliance officer's own actions. Random samples are to be taken; the number is to be recorded and justified. A monitoring practice that is limited solely to file- or computer-based actions is insufficient.

The Compliance Officer shall consider the quantity and quality of complaints as a source of information in the context of his monitoring task, as they can provide valuable information for their monitoring activities. Further details on the subject of complaints can be found in the industry standard for complaint management.

Any deficiencies identified and the measures taken to rectify them are discussed and documented together with those responsible for the business area concerned. The Compliance Officer monitors, controls and documents the implementation of these remedial measures. They shall act in a constructive and supportive manner in resolving conflicts.

In the case of serious deficiencies, the management shall be informed in text form of the source and extent immediately after their identification. The report shall include a proposal for corrective action. Any changes or additions to the report by management shall be documented in an addendum to the report. In addition, the ad hoc notification should also be sent to the supervisory body, if one exists.

The Compliance Officer is available to assist the specialist departments with the (further) development of processes, with strategic decisions or as part of the development of new products or the opening up of new markets. If their recommendations are not followed, this must be documented and explained in the annual compliance report.

E. Compliance Meeting

The Compliance Officer and representatives of all relevant stakeholders hold regular meetings several times a year to discuss changes to risks already identified and, in particular, new risks that have arisen as a result of controls. In addition, the development of complaint topics and numbers as well as the solutions offered to customers are to be discussed.

F. Compliance Report

The Compliance Officer shall report to the management in written form on their monitoring and control activities (compliance report) at least once a year and/or on an ad hoc basis. This report shall contain at least the following points:

- Presentation of the relevant regulatory framework; in particular, also the relevant changes and foreseeable developments that occurred during the reporting period, as well as the measures taken or to be taken to ensure compliance with them.
- Presentation and assessment of the member's risk profile and, in particular, its systems for compliance with the regulatory framework.
- Presentation and evaluation of the adequacy of the staffing and material resources of the compliance organization, with particular regard to the member's risk profile. If the function of compliance officer is performed by a business manager, this solution must be presented and justified in a plausible manner.
- Presentation and evaluation of the internal system for avoiding conflicts of interest within the meaning of Section IV/7 of the General Association Principles and Rules of Conduct.
- Presentation of the main deficits with compliance relevance and evaluation of the corresponding remedial measures and strategies as well as their effectiveness.
- Number of complaints, development of complaint topics and key performance indicators, amounts for damages and goodwill payments.
- Information on correspondence with the relevant supervisory authorities.
- Training provided to employees and delay.

The management must pass a formal resolution taking note of the compliance report. In addition, the report should also be sent to the supervisory body, if one exists.

F. Compliance Risk Assessment

Every two years, the Compliance Officer shall conduct a comprehensive risk inventory (Compliance Risk Assessment). The risks must be fully and systematically recorded, documented, presented in terms of their probability of occurrence for different time periods (short-term/1 year; medium-term/3 years; long-term/5 years) and the assessment of their potential damage levels. For identified risks, the organizational units concerned must promptly specify remedial measures, the implementation of which is monitored by the Compliance Officer.

The Executive Board must pass a formal resolution acknowledging the results of the Compliance Risk Assessment. In addition, the results of the risk inventory should also be communicated to the supervisory body, if one exists.

The assessment shall be commenced within a two-year period and shall also be completed, in principle, with any remedial action taken.

G. Continuing education of the compliance officer; training of employees

The Compliance Officer shall attend a relevant training event at a reputable educational institution at least once a year. The objective is to provide continuing education in the specialized areas of compliance management relevant to the member.

Employees are trained and tested by the Compliance Officer at least once a year on compliance-relevant topics. The training and testing obligation also includes members of the Executive Board.

H. Controls of Compliance with this Industry Standard

The members shall have plans for regular monitoring of compliance with this Industry Standard and specify the allocation of responsibilities. The results shall be reported to the management.

To ensure the effectiveness of the control, it shall be exercised by a function distinct from the compliance organization. The results shall be reported to management.

If available, the performance of the control by the internal audit department or a department comparable to the tasks of the internal audit department lends itself as a third line of defense.

Further details on the Three Lines of Defense model can be found in the Industry Standard for Enterprise Risk Management.

I. Deviations from the Provisions of this Industry Standard

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

Since the business models are various, depending on the size, type, scope, complexity and risk content of business activities, the standard can be implemented by the members in different

dimensions and for some only partially. In justified cases, deviations are therefore possible as an exception. For this purpose, an application in text form justifying the deviation shall be submitted to the Board of Directors. The decision shall be taken by a qualified majority in accordance with the Articles of Association.

A member who has been awarded the Quality Seal may have it withdrawn by the General Meeting by a simple majority if the member deviates from the provisions of this Industry Standard without having previously informed the Board of Directors about the deviations in good time.

J. Review clause

This Industry Standard shall be subject to revision by the Committee on Risk & Compliance Management of the Digital Lending Association at two-year intervals. Any amendments and/or additions shall be adopted by the General Meeting by qualified majority.