Management, Processing, and Investigation Procedure for the Information Received through the Communication Channels of the Center for Monetary and Financial Studies Foundation (CEMFI)

1. Definition

The Procedure for the Management, Processing, and Investigation of the Information Received through the Internal Information Channels of the Center for Monetary and Financial Studies Foundation (CEMFI), hereinafter referred to as "the Foundation," regulates the management, processing, and investigation of the information received from whistleblowers under the framework of Law 2/2023, of February 20, which regulates the protection of individuals who report regulatory violations and fight against corruption.

2. Subject Scope: Whistleblowers and Affected Individuals. Their Rights and Obligations.

2.1. Whistleblowers

The Internal Information System, through the configured internal channels, is available to all employees, individuals belonging to the administration, management, and supervisory bodies, collaborators, and personnel subcontracted by the Foundation.

Likewise, the Channel is accessible to former employees of the Foundation, including those whose employment or statutory relationship has ended, volunteers, interns, trainees, individuals whose employment has not yet begun but have acquired information during the selection process or pre-contractual negotiations that may reveal a violation as stated in section 3.1, as well as third parties who come into contact with the activities carried out by the Foundation.

All the aforementioned individuals are potential whistleblowers.

When making a report, the whistleblower may provide a postal address, email, or secure location to receive notifications, without prejudice to the fact that the internal information channels allow for the submission and subsequent processing of anonymous communications.

Anyone who submits a report has the right to have their identity kept confidential and not revealed to third parties. The Internal Information System must have appropriate technical and organizational measures in place to preserve the identity and ensure the confidentiality of data concerning the affected individuals and any third parties mentioned in the provided information, particularly the identity of the whistleblower if they have been identified.

The identity of the whistleblower can only be disclosed to the Judicial Authority, the Prosecutor's Office, or the competent administrative authority within the framework of a criminal, disciplinary, or sanctioning investigation. Specifically, the whistleblower will be informed of the communication of their identity before it is disclosed unless such information could compromise the investigation or judicial process. If the competent authority communicates the disclosure of the confidential data to the whistleblower, they will be provided with a written explanation of the reasons for such disclosure.

In any case, the whistleblower is not responsible for evaluating the events that occurred but should only specify what happened with the utmost detail possible.

In this framework, the following requirements must be met:

• Confidentiality.

• Possibility of anonymous reporting, which, in the case of anonymous communications, implies the implementation of a tool that allows communication with the anonymous whistleblower.

• Protection against retaliation towards the whistleblower.

• Impartiality of the investigations.

Whistleblowers will have the right to protection measures when they have reasonable grounds to believe that the information provided is true at the time of communication or disclosure, even if they do not provide conclusive evidence, and when the communication is made in accordance with the established procedures.

Therefore, as a protective measure, there is an explicit prohibition of acts constituting retaliation, including threats and attempts of retaliation against individuals who submit a report. This prohibition also applies to:

• Specifically, the legal representatives of the employees in the exercise of their functions to advise and support the whistleblower.

• Individuals who, within the organization where the whistleblower provides their services, assist them in the process.

• Individuals who are related to the whistleblower and may suffer retaliation, such as colleagues or family members.

• Legal entities for whom the whistleblower works or with whom they maintain any other kind of relationship in a work-related context or in which they hold a significant interest.

Thus, the rights of the whistleblower are as follows:

• Decide whether they want to submit the report anonymously or not, ensuring the preservation of their identity if applicable.

• Submit the report verbally or in writing.

• Provide a postal address, email, or secure location to receive communications related to the investigation or waive receiving such communications.

• Right to confidentiality. The Responsible for the Internal Information System cannot disclose the whistleblower's identity to the affected individual, and it can only be communicated to third parties in the cases legally provided for or when the whistleblower expressly consents to it.

• Exercise the rights conferred by personal data protection legislation.

• Right to protection against retaliation.

• Right to know the status of the processing of the report and the results of the investigation, as well as to be informed, if applicable, of the resolution or closure of the report.

• Right to the protection provided for in Law 2/2023 in the event that they report or disclose violations mentioned in section 3.1 when there are reasonable grounds to believe that the information provided is true at the time of communication or disclosure.

Similarly, the duties of the whistleblower are:

• Act in good faith. Reports or communications made in bad faith may lead to disciplinary and/or sanctioning measures that are applicable to the whistleblower.

• Provide the data and documents they possess related to the reported facts.

• Duty of confidentiality. The whistleblower cannot disclose the identity of the reported individual affected to any entity or person other than the Responsible for the Internal Information System, except in cases legally provided for.

When a person who has participated in the commission of the administrative offense being reported is the one who informs of its existence, in good faith and with a willingness to cooperate, by submitting the information, and provided that the report was submitted before the initiation of the investigative or sanctioning procedure, the competent body responsible for resolving the procedure, for the purpose of determining their involvement or relationship with the reported facts, may, through a reasoned report, exempt them from the administrative sanction that would otherwise be applicable, as long as they have ceased to commit the offense at the time of the report and have identified, if applicable, the other individuals who have participated or contributed to it, and have proceeded, if necessary, to repair the damage caused for which they are responsible. The mitigation of the sanction may also be extended to the other participants in the commission of the offense, depending on the degree of active cooperation in clarifying the facts, identifying other participants, and repairing or mitigating the damage caused.

2.2. Affected Individuals

The affected individuals will have the following rights:

• Presumption of innocence and the right to defense, being able to appear with legal representation, with their identity preserved, and ensuring the confidentiality of the facts and data of the procedure.

• Right to be informed as soon as possible that they are under investigation due to a report filed against them or their actions. This communication will include, at a minimum, the reported facts, their rights, and the procedure for processing the report.

• Right to access the file, to submit written allegations, and to the processing of their personal data, being provided with a summary of the investigated facts, without revealing information that could identify the whistleblower or other individuals affected by the procedure.

• Right to rectify inaccurate or incomplete personal data.

• Right to be informed of the resolution, closure, or dismissal of the report, if applicable. When notifying the affected individual that they are the subject of a report could jeopardize the Foundation's ability to investigate or gather evidence effectively, due to the risk of destruction or alteration of evidence by the reported individual, this notification may be postponed until the

hearing stage.

3. Internal Information Channel: Scope, Operation, and Identification

3.1. Scope and Operation

The Internal Information Channel is an integral part of the Internal Information System and should allow for both written and/or verbal communications. Additionally, the whistleblower may request to present their communication through a face-to-face meeting within a period of 7 days regarding:

• Any actions or omissions that may constitute violations of European Union law, in accordance with Article 2.1.a) of Law 2/2023.

• Actions or omissions that may be subject to serious or very serious criminal or administrative offenses. In any case, it includes all serious or very serious criminal or administrative offenses that involve economic harm to the Public Treasury and Social Security.

The Internal Information Channel is the preferred method for reporting these actions or omissions. However, when verbal communications are made, including those through face-to-face meetings, phone calls, or voice messaging systems, they must be documented in one of the following ways, with prior consent from the whistleblower:

• By recording the conversation in a secure, durable, and accessible format, or

• Through a complete and accurate transcription of the conversation carried out by the personnel responsible for handling it.

Additionally, individuals who make the communication through internal channels will be informed, in a clear and accessible manner, about external channels of information available to report to the competent authorities and, if applicable, to the institutions, bodies, or agencies of the European Union.

In the case of communications made through the Internal Information Channel, which will be managed by the Responsible for the Internal Information System as the guarantor of the process, through the designated person for this purpose, the process will begin with a written communication about the incidents, violations, or non-compliances that have come to their knowledge.

Upon receiving the communication, an acknowledgment of receipt will be issued to the whistleblower within 7 natural days following its reception unless this could jeopardize the confidentiality of the communication.

During the response period, there is the possibility of maintaining communication with the whistleblower and, if deemed necessary, requesting additional information from them. Furthermore, the affected individual must be informed of the actions or omissions attributed to them, and they must be given the right to be heard at any time. The requirement to respect the presumption of innocence and the honor of the affected individuals must also be emphasized.

The investigation proceedings must be responded to within a maximum period of 3 months from the receipt of the communication if an acknowledgment of receipt has been made. In cases where no acknowledgment of receipt was made, a period of 3 months will be available from the

expiration of the 7 natural days following the communication. If there is a need for additional time due to the special complexity of the case, an additional extension of 3 months may be granted. Additionally, the Responsible for the Internal Information System must immediately submit the information to the Public Prosecutor's Office if the reported facts could constitute a criminal offense.

In cases where the reported facts may involve violations of European Union law and affect the financial interests of the European Union, the information should be communicated to the European Public Prosecutor's Office.

The investigation process should be carried out with diligence and impartiality, ensuring the rights of all parties involved, including the whistleblower and the affected individuals. The confidentiality of the investigation must be preserved, and the final resolution or decision should be communicated to all relevant parties.

3.2. Identification of Internal Information Channels

Any individual within the scope established in section 2.1 of this procedure, who becomes aware of conduct related to the objective scope mentioned earlier (criminal offenses, serious or very serious administrative offenses, and violations of European Union law), shall inform the Responsible for the Internal Information System through one of the following means:

In Writing:

By postal mail, using the following postal address: Calle Casado del Alisal, 5, 28014 Madrid (Madrid), attention to the Responsible for the Internal Information System.
Through the designated email address: canalinfo@cemfi.es.
Via the website: www.cemfi.es.

Verbally:

In a face-to-face meeting with the Responsible for the Internal Information System, with the conversation possibly being recorded in a secure, durable, and accessible format or transcribed accurately and completely by the personnel responsible for handling it.
Through a telephone call using the designated phone number, with the conversation possibly being recorded in a secure, durable, and accessible format.
Via a voice messaging system using the phone number mentioned above, with the conversation possibly being recorded in a secure, durable, and accessible format.

Competent body.

The Responsible for the Internal Information System will be responsible for receiving and processing these reports. The Responsible will autonomously and independently investigate all information received through this channel, provided that it appears credible, the reported facts constitute one of the violations mentioned in the section dedicated to the objective scope of this procedure, and the communication is not evidently unfounded or lacks rational indications of having been obtained through the commission of a crime.

Regardless of whether an investigation is conducted or not, all information received through the Internal Information System will be recorded in the register book for statistical purposes.

Annually, the Responsible for the Internal Information System will prepare an anonymized report on the received reports, conducted investigations, and their outcomes, which will be presented to

the Foundation's Executive Committee.

4. Personal data protection

The processing of personal data resulting from the receipt of communications through the whistleblowing channel will be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016; Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights; Organic Law 7/2021, of 26 May, on the protection of personal data processed for the purposes of prevention, detection, investigation, and prosecution of criminal offenses and the enforcement of criminal penalties; and Title VI of Law 2/2023, of 20 February, on the protection of persons who report regulatory violations and fight against corruption.

Personal data that is not relevant for processing specific information will not be collected, and if collected accidentally, it will be promptly deleted.

The objectives related to data protection and security are confidentiality, integrity, and availability for the protection of the whistleblower and the affected subject, complying with the following principles:

• Non-linkability, meaning that data is only processed and evaluated for the purpose for which it was collected.

• Transparency, ensuring that data is adequately controlled and managed throughout all processes.

• Capacity to intervene, enabling the whistleblower or the affected subject to actively exercise their rights at any time.

5. Identification of external information channels.

Any individual may report to the Independent Authority for Whistleblower Protection (AAI), once it is established, or to the corresponding regional authorities or bodies, regarding any actions or omissions falling within the scope of application of this Law, either directly or after making a prior communication through the respective internal channel.