Procedure on the Internal Reporting System

MdF
FAMILY PARTNERS

MdF
FAMILY PARTNERS

INDEX

1. Document information

Versions

DRAFTING:	Regulatory Compliance		
APPROVAL:	Responsible	**Board of Directors**	
	Date of 1st Approval	19 March 2024	
CURRENT VERSION:	v.1	Brief description	Date of Approval
		Internal information system	25 March 2025
UPDATE HISTORY	Date of Update	Detail Update / Reason	Date of Approval
	v.1	Initial drafting	19 March 2024
	V.2	Physical mailbox update	25 March 2025

2. Introduction

This document contains MdF Gestefin SGIIC, S.A. (hereinafter "MdF" or the "Entity") procedure, by virtue of which the operation of the Entity's internal reporting system or whistleblowing channel is developed (hereinafter, the "Procedure"). This Procedure is supplemented by the MdF Policy on the Internal Reporting System (hereinafter the "Policy"), which sets out the basic principles of the Entity's internal reporting system or whistleblowing channel.

The purpose of this system is to be able to receive confidentially or anonymously any possible irregularity or act that is suspected or known to be improper or contrary to current legislation or MdF's internal regulations.

3. Reference standards

- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law.
- Law 2/2023 of 20 February on the protection of persons who report regulatory violations and the fight against corruption ("Law 2/2023").
- Law 10/2010 of 28 April 2010 on the prevention of money laundering and terrorist financing ("Law 10/2010").
- Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments ("MiFID II").
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("GDPR").
- Regulation 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse ("Market Abuse Regulation").

4. Scope of application

4.1 Subjective scope of application

The subjective scope of application of the Procedure is all employees, senior managers, members of the board of directors of MdF (hereinafter "Subject Persons").

This system may also be used by any person working for or under the supervision of the Entity's suppliers.

It may also be used by all persons who have had an employment or statutory relationship with MdF that has ended, volunteers, interns, trainees in training periods, whether or not remunerated, as well as those whose employment relationship has not yet begun, in cases where the information on breaches has been obtained during the selection process or pre-contractual negotiation.

4.2 Objective scope of application

Any possible irregularity or act suspected or known to be improper or contrary to the legislation in force or to MdF's internal regulations, committed within the Entity or its activity, may be reported through the internal reporting system.

In particular, they may report on the infringements contained in Article 2 of Law 2/2023, i.e. those which:

- may constitute infringements of EU law provided that they fall within the scope listed in the Annex to Directive 2019/1937 and that they affect the EU's financial interests or have an impact on the internal market. Among the matters detailed in the Annex to the Directive are:
    - financial services, products and markets,
    - prevention of money laundering and terrorism financing,
    - investor and consumer protection,
    - protection of privacy and personal data, and security of networks and reporting systems,

- may constitute a serious or very serious criminal or administrative offence. In any case, all serious or very serious criminal or administrative offences that involve financial loss for the Public Treasury and for the Social Security will be understood to be included.
- may constitute breaches of the Entity's internal policies and procedures.

5. Internal Whistleblowing channel

The reporting of a potential irregularity may be made through one of the following channels:

- Physical mailbox at the Entity's offices

  In order to guarantee the anonymity of those whistleblowers who so wish, a physical mailbox will be set up. The physical mailbox will be located at Calle Serrano, 1, 3º. 28001, Madrid and at Avenida Diagonal 550, 3º 1ª. 08021, Barcelona.

- Postal mail. Sending the report in writing to the following postal address for the attention of Responsible for the Whistleblowing Channel to any of the following postal addresses:
  - Calle Serrano, 1, 3º. 28001, Madrid
  - Avinguda Diagonal 550, 3º 1ª. 08021, Barcelona
- Access to the physical mailboxes established in the Entity's offices shall be restricted to:
  - The Channel Manager.
  - The persons in charge of the physical mailboxes located in the Entity's offices, who are only responsible for transferring the reports received in the mailboxes set up for this purpose, in order to transfer them to the Channel Manager.
- At the request of the whistleblower, communication of reportable facts may also be made through a face-to-face meeting, following a formal written request. Verbal communications made through a face-to-face meeting must be documented in one of the following ways, subject to the whistleblower's consent:
  - by a recording of the conversation in a secure, durable and accessible format, or
  - through a complete and accurate transcript of the conversation made by the staff responsible for dealing with it.

Without prejudice to his or her rights under data protection law, the whistleblower shall be given the opportunity to verify, rectify and agree by signature to the transcription of the conversation.

When making the communication (verbal or written), the whistleblower may indicate an address, e-mail address or safe place to receive notifications, including the aforementioned acknowledgement of receipt.

Where the report has been made through a channel other than the competent channel or to persons other than the person responsible, it must be ensured that the staff who have received the report do not disclose information that could identify the whistleblower or the person concerned and that they immediately forward the communication, without modifying it, to the person responsible for the internal reporting system.

6. External whistleblowing channels

Supervisors, depending on the regulatory environment, have specific channels where reports regarding reportable facts and conduct can be submitted on their websites. In any case, these authorities ensure that the complaint can be submitted both in writing and verbally.

The authorities that have specific channels are the following:

- Independent Authority for Whistleblower Protection[1]
- Bank of Spain: https://www.bde.es/wbe/es/para-ciudadano/gestiones/canal-de-denuncias-del-banco-de-espana/
- National Securities Market Commission: https://www.cnmv.es/portal/whistleblowing/presentacion.aspx
- Spanish Agency for Data Protection: https://www.aepd.es/la-agencia/transparencia/canal-proteccion-whistleblowere

7. Procedural rights and guarantees

7.1 Rights of the whistleblower

The following rights of whistleblowers will be guaranteed by MdF:

[1] Not yet incorporated.

- **Right not to suffer retaliation:** MdF will ensure that the whistleblower who acts in good faith does not receive any type of retaliation and, in the event that, despite the measures implemented by the Entity, the whistleblower receives any type of retaliation, it will act in such a way that the whistleblower's rights are protected, sanctioning, where appropriate, the perpetrator of the retaliation.
- **Right to be informed:** the whistleblower shall be informed of the status and outcome of the investigation.
- **Confidentiality:** confidentiality is one of the basic pillars of the internal reporting system and the identity of the whistleblower will be kept strictly confidential. Likewise, all those involved in the investigation process are obliged to keep the identity of the whistleblower confidential.

7.2 Rights of the investigated person

The following rights of those under investigation will be guaranteed by MdF:

- **Right to be informed:** the person under investigation must be informed of the investigation being carried out and the facts on which it is based, so that he/she can exercise his/her right to defence and allege everything that allows him/her to prove his/her innocence. Without prejudice to the right to be informed, the communication of the initiation of the file to the person under investigation may be delayed up to a maximum period of three (3) months from the filing of the complaint, provided that knowledge of the same could jeopardise the normal development of the investigation, and this decision must be documented in a well-founded manner by the person responsible for the internal information system.
- **Right to the presumption of innocence:** the presumption of innocence of the person under investigation shall be preserved and no sanctioning measures may be applied until the veracity of the facts reported is verified, the appropriate evidence is gathered and, where appropriate, it is concluded that a breach has taken place on the part of the person under investigation.
- **Confidentiality:** Throughout the investigation process, the right to confidentiality of your personal data must be guaranteed in order to avoid any irregular use of the information that could affect their privacy and reputation.

- **Right of defence and the principle of contradiction:** it shall be guaranteed that the person investigated may exercise his or her right of defence on the basis of the principle of contradiction, and that the person responsible shall carry out an objective analysis of the evidence gathered, guaranteeing an effective and transparent investigation.

8. Procedure for the processing of reports

Based on the general principles and safeguards listed in section 7 above and detailed in the Policy on Internal Reporting System, the present procedure is defined.

This procedure foresees that the steps will be carried out in a personalised manner and in collaboration with the parties involved, leaving a documentary record of all the actions carried out.

The steps involved in this procedure are as follows:

8.1 Initial phase. Admission or rejection of the report.

Any person falling within the subjective scope of application of the procedure (section 4 of the procedure) may make a report through one of the internal channels mentioned in section 5. This report must contain at least the information indicated in section 8.2.

All reports received shall be registered by the person in charge of the internal reporting system and, upon receipt and provided that the whistleblower is not anonymous, acknowledgement of receipt shall be given within a maximum of seven (7) calendar days, unless this could jeopardise the confidentiality of the communication.

Once the report has been registered, the person responsible of the internal reporting system must analyse and evaluate the report in order to admit or reject it, taking into account the criteria described below:

- **Admission for processing:** only reports that clearly and obviously state facts constituting an infringement, irregularity or non-compliance with the legal regulations in force, the policies, rules or procedures of the Entity shall be admitted for processing. In this case, the report will be assigned an identification code or internal registration number, which will be sent to the whistleblower.
- **Rejection:** reports that do not contain all the required information, do not constitute an infringement or non-compliance or do not provide sufficient clarity or detail to determine whether a potential irregularity exists will not be admitted for processing.

In both cases, provided that the complaint is not anonymous, the whistleblower will be informed of this fact. In the event of inadmissibility, the whistleblower may consider reformulating the report or using other alternative legal channels that he/she considers appropriate.

8.2 Minimum content of the report

The report shall include at least the following information:

- In the case of non-anonymous whistleblower; name, ID card (or similar) and contact details (telephone, e-mail, etc.).
- Facts and approximate dates of the facts that are the subject of the report.
- The subject matter and reasons for which the communication is made.
- Evidence available to the whistleblower that can be attached.
- Whether or not this is an event that affects customers.

The report must be precise, with sufficient information and presented as objectively as possible to enable the Entity to carry out its analysis.

In cases where insufficient information is available, additional information will be requested from the whistleblower, provided that he/she has identified him/herself in his/her report.

If the report is anonymous and there is insufficient information available, it will be rejected as not complying with the established requirements.

8.3 Investigation phase

At the investigation stage, for both anonymous and non-anonymous reporting, reports will be in one of three (3) possible statuses:

- **Not reviewed:** the communication has been received, but the Entity has not started its analysis.
- **Under review:** a preliminary analysis of the reported facts, their veracity and the reasons for reporting is being carried out.
- **Review completed:** the investigation has been completed.

Throughout the analysis process, the basic principles of the Procedure and the basic rights of the person under investigation will be complied with at all times, including the presumption of innocence, the right to be heard and the right to honour, documenting in writing each of the actions carried out, recording, among others, the nature of the complaint and its date, the dates of each action and the justification for each of them, the persons involved in the process and the current status of the investigation.

When one of the evidences presented by the whistleblower is the testimony of a person or the system administrator considers that, based on the account of the facts, there are persons who can help to discern the veracity of the facts reported, he/she may request to interview these persons (provided that it is duly provided and the minimum number of persons involved is selected). In such cases, the system administrator shall take and document all appropriate and necessary measures to ensure confidentiality and compliance with other rights and principles of the Procedure.

When, in order to analyse the necessary facts, the person responsible for the system considers it necessary to access information restricted by the entity's IT security measures or information held by the defendant, such access must be justified and shall be carried out after weighing up the privacy of those potentially affected.

In order to carry out the investigation, MdF may contact legal advisors, external auditors, consultants or other advisors to assist it in the investigation and analysis of the results, taking into account the circumstances and nature of the reported event. In such cases, the external entities and persons involved in carrying out the investigation shall abide by this Procedure and strictly comply with the defined principles and rights, undertaking in particular to treat as confidential any information to which they have access in the course of providing the service.

8.4 Resolution phase and deadline

Once the investigation has been completed and after assessment by the system administrator, the latter will make a well-founded decision as to whether the complaint is admissible. In this regard, the system administrator may decide:

- **Whether the report is admitted:** in this case, a report shall be issued containing at least the following content:
    - Description of the facts, avoiding the incorporation of data that could identify individuals when this is not strictly necessary for the development and understanding of the report.
    - The data relating to the report received**.**
    - The actions carried out to investigate the reported facts.
    - The results of the investigation.
    - The recommendation of corrective measures to be taken and if they cannot be implemented immediately, a timetable with a remediation plan shall be included.

  The report shall be submitted to the Board of Directors. The Board of Directors shall review the report and shall approve the proposed measures and adopt any additional measures it deems necessary.
- **Whether the report is not admitted**, the procedure will be terminated and the case will be closed, and the whistleblower, if not anonymous, will be informed of the closure of the case.

The file will be closed and the information and evidence, as well as the documentation generated during the process, will be kept.

In any case, a response to the investigation proceedings shall be given within a maximum of three (3) months from receipt of the communication or, if no acknowledgement of receipt was sent to the whistleblower, within three (3) months from the expiry of the seven-day period following the communication, except in cases of particular complexity requiring an extension of the time limit, in which case, this may be extended for a maximum of another three (3) months.

When the file is closed and the investigation report is submitted to the Entity's Board of Directors, the measures to be implemented shall be approved and, in the event that they cannot be implemented immediately or in the short term, an action plan shall be included with a timetable of a maximum of one (1) year, which the person responsible for the system shall monitor and document compliance with the timetable.

In the event that the reported facts and the final report determine or conclude that the situation has or may have legal implications, it should be brought to the attention of external legal advisors and the competent public and police authorities.

8.5 Adoption of Measures

MdF will take such action as it deems appropriate in response to the facts under investigation, including, but not limited to, the following:

- Disciplinary measures (up to and including dismissal) against the Person Subject who, in the opinion of the entity, has engaged in irregular or illegal conduct.
- Reporting to the competent authorities to the extent necessary as required by law and the facts under investigation.

Whistleblowers are presumed to be in good faith, however, if it is proven that they deliberately or maliciously report false information for personal gain or with the aim of damaging the reputation of others, they may be subject to disciplinary action, including dismissal.

9. Personal Data Processing

Personal data that may be processed in the course of a file within the Internal Reporting System Procedure shall be treated with the utmost confidentiality. MdF Gestefin SGIIC, S.A. is responsible for the processing of such data.

The purpose of the processing of personal data in the internal reporting system is to manage the reporting of irregular conduct when the user wishes to report suspected irregular conduct, unlawful acts or breaches of regulations. MdF may obtain data directly from the whistleblower as well as from third parties (e.g. witnesses, investigated, MdF areas, expert or police reports).

Likewise, in accordance with the requirements of the RGPD, the whistleblower may exercise his/her rights of access, rectification, elimination and opposition, limitation of processing and portability obtained through this system by contacting the data protection officer, via the email address of the data protection officer (dpo@mdffp.com).

10. Approval, review and dissemination of the procedure

This procedure shall be approved by the Board of Directors of the Entity, as well as any subsequent modifications. However, the person in charge of the internal information system, as the person responsible for the procedure, shall review its content annually and, if he/she deems it appropriate, shall modify it.

- when legal or regulatory changes affecting the procedure take place.
- The Board of Directors may propose to Regulatory Compliance when it considers that there are aspects that could be improved in order to achieve the proposed objectives or to suitably adapt to the characteristics of the services offered by the Entity at any given time.