

Resolution of 5 June 2023, by FROB's Governing Committee, approving FROB's internal reporting system.

The purpose of Act 2/2023, of 20 February, regulating the protection of individuals who report regulatory breaches and fight corruption, is to protect people who, in a work or professional context, detect criminal or serious administrative offences and report them through the mechanisms regulated in the Act. Article 1 of this Act establishes the dual objective: first, to guarantee proper protection against retaliation that may be suffered by individuals who report any actions or omissions that constitute offences through the procedures provided for in the Act. And second, to strengthen the culture of reporting, organisational integrity, and promote the use of reporting as a mechanism to prevent and detect threats to the public interest.

To achieve these objectives, Articles 5, 8, and 9 of Act 2/2023 of 20 February establish several obligations, in particular (i) to implement the "Internal Reporting System" within their respective entities, (ii) to appoint a responsible individual for managing this system, referred to as the "System Manager", who may also be a collegiate body, and (iii) to approve the "Information Management Procedure", which must establish the necessary provisions to ensure that the internal reporting system and existing internal channels comply with the legal requirements. The responsibility for fulfilling these obligations lies with the administrative or governing bodies of each entity or organisation, and in FROB's case, this falls on its Governing Committee.

FROB's Internal Reporting System, attached as an Annex to this Resolution, consists of five chapters: the first includes the general provisions, the purpose of the Internal Reporting System, as well as the material and personal scope of application, the general principles that must govern the Information Management Procedure, and provisions concerning the protection of informants and the prohibition of retaliation. The second chapter sets out the composition and responsibilities of the System Manager. The third defines the internal reporting channel and outlines its operation. The fourth establishes the Information Management Procedure, and finally, the fifth chapter addresses the sanctions regime.

In view of the foregoing, the Governing Committee of FROB resolves:

First. To approve the *FROB Internal Reporting System*, attached as an Annex to this Resolution, in accordance with the provisions of Act 2/2023, of 20 February, regulating the protection of individuals who report regulatory breaches and the fight against corruption.

Second. To order the inclusion on FROB's website of a specific section providing access to the Internal Reporting Channel, as well as publication of the applicable regulations and this Resolution.

Third. To entrust the Chair of FROB with implementing measures to inform and communicate this to all FROB personnel, which will be reported to this Governing Committee within a period of 3 months.

Madrid, 5 June 2023. Chair of FROB, Paula Conthe Calvo.

ANNEX
FROB INTERNAL REPORTING SYSTEM

CHAPTER I. GENERAL PROVISIONS.....	3
First. <i>Purpose</i>	3
Second. <i>Material scope of application</i>	3
Third. <i>Personal scope of application</i>	4
Fourth. <i>General principles</i>	4
Fifth. <i>Whistleblower protection</i>	4
Sixth. <i>Prohibition of retaliation</i>	5
Seventh. <i>Protection measures against retaliation</i>	5
Eight. <i>Preservation of the Whistleblower’s identity</i>	5
CHAPTER II. RESPONSIBLE BODY FOR THE INTERNAL REPORTING SYSTEM.....	6
Ninth. <i>Composition</i>	6
Tenth. <i>Functions</i>	6
CHAPTER III. INTERNAL REPORTING CHANNEL.....	7
Eleventh. <i>Definition</i>	7
Twelfth. <i>Operation</i>	7
CHAPTER IV. INFORMATION MANAGEMENT PROCEDURE	7
Thirteenth. <i>Receipt of communication</i>	7
Fourteenth. <i>Processing</i>	8
Fifteenth. <i>Conclusion</i>	8
Sixteenth. <i>Participants</i>	9
Seventeenth. <i>Personal data</i>	9
CHAPTER V. NON-COMPLIANCE	10
Eighteenth. <i>Sanctions</i>	10

CHAPTER I. GENERAL PROVISIONS

First. Purpose

This document aims to define the FROB Internal Reporting System, which will serve for receiving communications regarding breaches of the legal framework within the context of a professional relationship, in accordance with the provisions of Act 2/2023, of 20 February, regulating the protection of individuals reporting regulatory infringements and combating corruption (hereinafter referred to as the “Whistleblower Protection Act”).

The FROB Internal Reporting System consists of:

- a) An entity responsible for the Internal Reporting System (Chapter II)
- b) An internal reporting channel (Chapter III)
- c) A procedure for managing reports (Chapter IV).

The Internal Reporting System is supplemented by the external reporting channel established by the Independent Whistleblower Protection Authority (A.A.I.).

Second. Material scope of application

This document applies to all information specified in Article 2 of the Whistleblower Protection Act relating to:

- a) Any actions or omissions that may constitute infringements of European Union law as outlined in Article 2 of Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, on the protection of individuals reporting breaches of Union law, provided that:
 - i. They fall within the scope of the acts of the Union listed in the annex to the aforementioned Directive¹;
 - ii. They affect the financial interests of the European Union²; or
 - iii. They impact the internal market³.
- b) Actions or omissions that may constitute a serious or very serious criminal or administrative offence.

Individuals who communicate information referred to in Article 35.2 of the Whistleblower Protection Act are expressly excluded from the protection provided for in this document. ⁴

¹ Relating to the following areas: I. Public Procurement; II. Financial Services, Products, and Markets, and Prevention of Money Laundering and Terrorist Financing; III. Product Safety and Compliance; IV. Transportation Safety; V. Environmental Protection; VI. Protection against Radiation and Nuclear Safety; VII. Food and Feed Safety, Animal Health, and Animal Welfare; VIII. Public Health; IX. Consumer Protection; X. Protection of Privacy and Personal Data, and Security of Networks and Information Systems.

² As provided for in Article 325 of the Treaty on the Functioning of the European Union (TFEU).

³ As provided for in Article 26, paragraph 2 of the TFEU.

⁴ In particular: a) Information contained in communications that have been rejected by any internal reporting channel or for any of the reasons set forth in Article 18.2.a). b) Information related to claims about interpersonal conflicts or that affect only the informant and the individuals referred to in the communication or disclosure. c) Information that is already fully available to the public or that constitutes mere rumors. d) Information referring to actions or omissions not covered in Article 2.

Third. *Personal scope of application*

As established by the Whistleblower Protection Act in its Article 3, the provisions set forth in this document and the aforementioned Act shall protect individuals who work in the private or public sector and who have obtained information regarding infringements in a work or professional context.

This includes whistleblowers who communicate or publicly disclose information about infringements obtained in the context of an employment or statutory relationship that has already ended, as well as volunteers, interns, and trainees, regardless of whether they receive remuneration or not, along with those whose employment relationship has not yet commenced, in cases where information regarding infringements has been obtained during the selection process or pre-contractual negotiations.

Fourth. *General principles*

In accordance with the Whistleblower Protection Act, the Internal Information System of FROB is based on the following principles:

- a) Free submission of information communications.
- b) Confidentiality of content and anonymity of the communication.
- c) Objectivity and effectiveness in the management and processing of communications.
- d) Independence from the internal information systems of other entities or organisations.
- e) Protection and defense of whistleblowers.
- f) Presumption of innocence, the right to defense, and the right to honour.
- g) Protection of personal data.

Fifth. *Whistleblower protection*

In accordance with Article 35.1 of the Whistleblower Protection Act, individuals who communicate or disclose infringements referred to in the second section of this document shall be entitled to protection provided that:

- a) They have reasonable grounds to believe that the information provided is truthful; and
- b) The communication or disclosure has been made in accordance with the requirements set out in this document and the Whistleblower Protection Act.

Individuals who have communicated or disclosed information about actions or omissions referred to in the second section of this document anonymously but who have subsequently been identified and meet the conditions stipulated in this document and the Whistleblower Protection Act shall be entitled to the protection recognised therein.

These protective measures shall also apply, where applicable, to individuals referred to in Article 3.4 of the Whistleblower Protection Act.

Sixth. Prohibition of retaliation

It is prohibited for any individual or body of FROB to execute, provoke, or assist in the execution of acts constituting retaliation as defined in Article 36⁵ of the Whistleblower Protection Act, including threats of retaliation and attempts at retaliation, against individuals who submit a communication in accordance with the provisions of this document and the Whistleblower Protection Act.

Administrative acts aimed at preventing or hindering the submission of communications and disclosures, as well as those that constitute retaliation or cause discrimination following the submission of such communications, shall be null and void and may result in the imposition of sanctions as provided for in the Whistleblower Protection Act, without prejudice to those established by the FROB Code of Conduct.

FROB shall inform the Independent Whistleblower Protection Authority (A.A.I.) of these administrative acts.

Seventh. Protection measures against retaliation

In accordance with the provisions of Articles 38 and 39 of the Whistleblower Protection Act, FROB shall adopt all necessary protection measures detailed in these articles to ensure the protection of both whistleblowers and individuals affected by the content of such information.

FROB shall ensure that, in cases where individuals involved in the commission of an infringement report the same under the terms of Article 40 of the Whistleblower Protection Act, they may benefit from exemptions and/or mitigations in any potential administrative penalties that may arise from such infringing conduct.

Eight. Preservation of the Whistleblower's identity

Individuals who submit a communication or make a public disclosure have the right to have their identity not revealed to third parties. Likewise, communications may be made anonymously, and FROB shall not seek data that aims to identify the whistleblower.

FROB shall preserve the confidentiality of the information received and the identity of the whistleblower, if identified, as well as that of any affected or mentioned individuals, at all times.

FROB may only disclose the identity of the whistleblower to the judicial authority, the Public Prosecutor's Office, or the competent administrative authority, and only within the context of a criminal, disciplinary, or sanctioning investigation.

The individual referred to in the reported facts shall not, under any circumstances, be informed of the identity of the whistleblower or of the person who made the public disclosure. The whistleblower shall be expressly informed that their identity will, in all cases, be kept confidential.

⁵ Any acts or omissions that are prohibited by law, or that directly or indirectly result in unfavourable treatment placing individuals who experience them at a particular disadvantage compared to others in the workplace or professional context, solely because they are whistleblowers or have made a public disclosure.

CHAPTER II. RESPONSIBLE BODY FOR THE INTERNAL REPORTING SYSTEM

Ninth. Composition

The body responsible for the FROB Internal Reporting System is composed of the holders of the Administration and Control Directorate, the Legal Directorate, the Deputy Legal Directorate, and the Head of the Procedures and Control Department (hereinafter referred to as the “responsible body of the System”)

The responsible body of the System will delegate one of its members with the function of managing the internal reporting system and processing the investigation files (hereinafter referred to as the “System Management Delegate”).

The composition of the responsible body of the System, as well as any modifications to it, must be communicated to the Independent Authority for the Protection of Whistleblowers, A.A.I., within ten days, specifying, in the event of cessation, the reasons for it.

Tenth. Functions

The responsible body of the System shall carry out its functions independently and autonomously, without being subject to any instructions of any kind.

In exercising its functions, it must have all the necessary personal and material resources at its disposal.

Without prejudice to those that may be delegated to the System Management Delegate, the functions of the responsible body of the System include:

- a) Facilitating access to this document for those subject to it.
- b) Ensuring compliance with the provisions of this document and, in particular, being accountable for the diligent processing of the information management procedure set out herein.
- c) Gathering the information received through the FROB Internal Reporting System.
- d) Diligently following up on the information received via the FROB Internal Reporting System.
- e) Ensuring that the levels of confidentiality and, where applicable, anonymity required by the Whistleblower Protection Act are maintained.
- f) Ensuring that all information received is managed with the same level of independence and objectivity.
- g) Requesting the participation of other individuals when necessary, in accordance with the provisions set out in section sixteenth of this document.
- h) Maintaining, where appropriate, communication with the whistleblower.
- i) Evaluating the effectiveness of the measures established in this document.
- j) Acting as a liaison with the Independent Authority for the Protection of Whistleblowers, A.A.I.
- k) Keeping a record of the information received and the internal investigations that have resulted from it, ensuring confidentiality requirements in accordance with Article 26 of the Act.
- l) Any other equivalent duties that may be necessary for compliance with the Act.

CHAPTER III. INTERNAL REPORTING CHANNEL

Eleventh. Definition

The FROB Internal Reporting Channel will enable the submission of information regarding the infringements outlined in the second section of this document.

Additionally, it may be used by FROB staff to report any infringement related to FROB's internal regulations, as established by its Code of Conduct. However, if these communications fall outside the scope established in the second section of this document, they and their senders will be excluded from the protection provided by the Whistleblower Protection Act.

The internal reporting channel will be published on the FROB website.

Twelfth Operation

The internal channel will allow communications to be made in writing, verbally, or in both forms through the communication mailbox established on the FROB website. If applicable, verbal communications must be documented in accordance with the provisions of Article 7.2 of the Whistleblower Protection Act. The internal channel will provide the option to communicate information anonymously.

At the request of the whistleblower, information may also be submitted through an in-person meeting, to be held within a maximum of seven days from the request. In such cases, and with the prior consent of the whistleblower, the in-person meeting will be documented in one of the forms contemplated in Article 7.2 of the Whistleblower Protection Act.

When making the communication, the whistleblower may provide a postal address, email, or any other secure reference for the purposes of receiving notifications.

In the area established for accessing the Internal Reporting Channel, a link will be included to facilitate access to the external channel of the Independent Whistleblower Protection Authority (A.I.I.).

CHAPTER IV. INFORMATION MANAGEMENT PROCEDURE

Thirteenth. Receipt of communication

Once the communication is sent by the whistleblower through the Internal Reporting Channel, the responsible body of the System will register it in a secure database.

No later than seven calendar days from the receipt of the information, the whistleblower will receive an acknowledgment of receipt through the notification method specified, except in cases of anonymous communications and those where confidentiality of the communication may be compromised.

When a communication is received through a channel of FROB that is not the competent one, or by staff members who are not responsible for its handling, the FROB staff who received it are prohibited from disclosing any information about it and must promptly forward the communication, without alteration, to the responsible body of the System.

All communications received must be managed in accordance with the provisions on personal data protection as outlined in the seventeenth section of this document and Title VI of the Whistleblower Protection Act.

Fourteenth. Processing

The objective of the processing is to verify the plausibility of the information received through the necessary internal investigation procedure. At all times, respect for the presumption of innocence and the honour of the affected individuals will be upheld.

The System Management body will communicate to the affected person the existence and content of the information received, without in any case revealing the identity of the informant, nor giving them direct access to the communication received. Additionally, they will be informed of their right to submit allegations and to be heard at any time. This communication will take place in the time and manner considered appropriate to ensure the successful completion of the investigation.

Without prejudice to the right to submit written allegations, the processing will include, whenever possible, an interview with the affected person, which will be documented in a record, inviting them to present their version of the events and to provide any evidence they consider relevant and pertinent.

If it is deemed that the investigation could be compromised by informing the affected person of the existence of the information received, due to the risk that evidence may be concealed, destroyed, or altered, the communication may be delayed.

The affected person will be able to know at any time the status of the processing of the procedure.

The management delegate of the System will be responsible for maintaining communication with the whistleblower and for requesting any supplementary or clarifying information, whenever necessary and provided the whistleblower has supplied contact details. Whenever the successful completion of the investigation advises it, they may also propose an in-person hearing with the whistleblower.

The maximum period for concluding the processing of the information will be three months from the sending of the acknowledgment of receipt of the communication or, failing that, from the expiration of the seven-day period established for this purpose. In cases of particular complexity, the maximum period may be extended by an additional three months.

The responsible body of the System will immediately forward the information to the Public Prosecutor's Office when the facts may indicatively constitute a crime or, where applicable, to the authority deemed competent for processing. In cases where the facts affect the financial interests of the European Union, they will be forwarded to the European Public Prosecutor's Office. Without prejudice to the right to make allegations in writing, the procedure shall include, whenever possible, an interview with the affected person, which will be documented in a record in which they will be invited to present their version of the events and to provide such evidence as deemed appropriate and relevant.

Fifteenth. Conclusion

Once the content of the received communication has been analyzed and the necessary investigative actions deemed necessary to verify the plausibility of the information have been carried out, the responsible body of the System will issue a report reflecting the result of this analysis. This report will include an account of the reported facts, the actions taken to verify their accuracy, and the final conclusions of the investigation, as well as, if applicable, the classification of the detected fraud as systemic or isolated.

Subsequently, the responsible body of the System will proceed, based on all the actions taken, to:

- a) Archive the received information if, after its final analysis, no additional actions are required.

- b) Internally apply the corresponding punitive or disciplinary actions and measures in accordance with current legislation and the internal regulations of FROB in cases where the reported infraction is confirmed.
- c) Forward the actions to the competent authority, in accordance with what is provided in the final clause of the previous section..

The conclusions of the report will be notified to the whistleblower, provided they have supplied an adequate notification method for this purpose.

Sixteenth. Participants

The responsible body of the System may request the participation of any member of FROB that they deem necessary for the resolution of the procedure. Such participants will be warned and must respect the protection measures provided in this document and in the Whistleblower Protection Act.

Exceptionally, if circumstances justify it, the participation of an external person to FROB may be requested.

Seventeenth. Personal data

The procedure established in this document ensures compliance with current data protection regulations. The processing of personal data arising from the application of this document will be governed by the regulations cited in Article 29 of the Whistleblower Protection Act⁶.

The processing of personal data collected under this document will be considered lawful under the provisions of Article 6.1(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, and Article 8 of Organic Law 3/2018 of December 5.

If it is established that the information provided, or part of it, is not true, it will be immediately deleted from the moment this circumstance is confirmed, unless this lack of truth could constitute a criminal offense, in which case the information will be retained for the necessary time during which the judicial procedure is processed.

In any case, three months after the receipt of the communication, if no investigative actions have been initiated, the information must be deleted, unless the purpose of retention is to provide evidence of the system's functioning. Communications that have not been acted upon may only be recorded in an anonymized form, and the obligation to block provided in Article 32 of the aforementioned Organic Law 3/2018 will not apply.

Personal data relating to the information received and internal investigations will only be retained for as long as is necessary and proportionate to comply with the Whistleblower Protection Act. Under no circumstances may the data be retained for a period exceeding 10 years.

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data and the free movement of such data; Organic Law 3/2018 of 5 December on Personal Data Protection and the Guarantee of Digital Rights; Organic Law 7/2021 of 26 May on the Protection of Personal Data Processed for the Purposes of Preventing, Detecting, Investigating, and Prosecuting Criminal Offences and the Enforcement of Criminal Sanctions; and Title VI of the Whistleblower Protection Law..

Access to the personal data contained in the Internal Reporting System will be limited to those involved in its management and to individuals whose participation is requested, with the limitation of the persons listed in Article 32.1 of the Whistleblower Protection Act.

CHAPTER V. NON-COMPLIANCE

Eighteenth. Sanctions

The exercise of the sanctioning power arising from the commission of infractions provided in Title IX of the Whistleblower Protection Act corresponds to the Independent Authority for the Protection of Whistleblowers (A.A.I.).

To this end, any indication of an infraction will be communicated to the aforementioned Authority.

FROB, for its part, may apply the sanctioning regime set forth in its internal regulations.