



PRISA GROUP

PROCEDURE FOR MANAGING THE INTERNAL REPORTING SYSTEM OF THE WHISTLEBLOWING CHANNEL.

May 2023



**PROCEDURE FOR MANAGING THE INTERNAL REPORTING SYSTEM OF THE
WHISTLEBLOWING CHANNEL**

CONTENTS

1. PURPOSE AND SCOPE.....	3
2. DEFINITIONS.....	3
3. COMMUNICATION OF IRREGULARITIES	4
3.1. Identification of an irregularity.....	4
3.2. Communication and receipt of communication.....	5
3.3. Receipt and classification of complaints	6
3.4. Communication to the whistle-blower.....	6
3.5. Informing the affected person.....	6
3.6. Protection of personal information	7
4. MANAGEMENT OF THE PROCEDURE	8

Changes from the prior version

First version. It takes as a reference and in Spain replaces the procedure for managing the whistleblowing channel of November 2021 to align it with the provisions of Act 2/2023 of 20 February 2023 on the protection of persons who report regulatory violations and the fight against corruption (**Act 2/2023 of 20 February 2023**).

Prepared by:	Reviewed by:	Approved by:
PRISA Compliance Unit (Carmen Ingelmo)	Business Compliance Unit and DPO (Ignacio Calle and Juan Pablo Nocete)	Board of Directors of Promotora de Informaciones, S.A. (23 May 2023)

1. PURPOSE AND SCOPE

The purpose of this document is to establish a procedure to regulate the management of the Internal Reporting System for irregularities that are sent through the whistleblowing channel of the PRISA Group, related to breaches of both external regulations (laws and/or provisions of lower hierarchy) and internal regulations (Code of Ethics, Internal Regulation of Conduct on Securities Markets, as well as other codes, regulations, rules and procedures defined within the PRISA Group), and any situations or facts that require the attention of the Compliance Unit of PRISA in matters that affect the Companies of the PRISA Group, its Professionals or its activities (hereinafter, we will refer to these documents jointly as the "Rules").

There will be just one Internal Reporting System for all PRISA Group companies in Spain. However, the independence of the compliance models of Promotora de Informaciones, S.A. (PRISA) and the Media and Education businesses of the PRISA Group in Spain, as designed and implemented, will be maintained.

The Manager of the Internal Reporting System will be the Chief Compliance Officer (CCO) of PRISA, although he/she will coordinate and inform the Managers of Compliance of the businesses in Spain if the reported irregularity affects the businesses and/or their professionals.

This procedure is established to ensure that, if an action contrary to the provisions of the Rules is reported, it will be treated diligently and confidentially, ensuring the anonymity and/or confidentiality of the identity of the whistle-blower, the affected person or persons and any third party mentioned in the communication.

For this purpose, a whistleblowing channel is available, accessible either through the intranet or through Post Office Box 35160, Madrid Capital, through which any employee, anonymously and confidentially, can report any irregularity or breach of both external and internal regulations.

The Group also has a third-party whistleblowing channel, accessible from the corporate website, through which one can also report anonymously and confidentially.

These whistleblowing channels are integrated into the Internal Reporting System.

It also guarantees that no retaliation will be taken against those whistle-blowers who, in good faith, report alleged breaches or irregularities. PRISA will take the necessary measures to comply with the legal provision that is also included in the Code of Ethics of the PRISA Group.

In terms of scope, this procedure will be mandatory for all companies of the PRISA Group in Spain.

2. DEFINITIONS

Affected or denounced party.- Person who, under the provisions of this procedure, is accused by the whistle-blower of the alleged commission of an irregularity.

Whistle-blower or accuser.- Person who under the provisions of this procedure reports an incident or complains of an irregularity.

Irregularity or breach.- Violation or performance of practices contrary to the principles established in the Code of Ethics, the rules and procedures defined within the PRISA Group, the applicable external regulation and any situations or facts that require the attention of the PRISA Compliance Unit in matters that affect the Companies of the Prisa Group, their employees or their activities.

Reporting System.- Computer system in which the whistleblowing channel of PRISA accessible through the corporate web and those of the intranet of the employees are integrated. The System processes all communications sent through the indicated channels and those received by other means that must be immediately reported to the CCO of PRISA, as Manager of the Internal Reporting System. The processing of the information will be in accordance with the provisions of Act 2/2023 of 20 February 2023.

Compliance Unit.- The PRISA Compliance Unit (PRISA CU) is the body in charge of Compliance, which in PRISA is constituted as a single-member body, the Chief Compliance Officer being the one in charge of this function. This Compliance Unit is an independent body that reports to the Audit, Risk and Compliance Commission of PRISA. In addition, there are Compliance Units in the Education and Media businesses, which will act regarding the companies comprising their businesses. These Compliance Units must promote ethical behaviour of employees and monitor compliance with the current legislation applicable to the activities of the Group in the different countries in which it operates and the internal regulations of the organisation.

The definitions of terms used in this procedure, not included in this paragraph, will have the scope established in Act 2/2023 of 20 February 2023 and applicable legislation.

3. COMMUNICATION OF IRREGULARITIES

3.1. Identification of an irregularity

Any person who knows of wrongdoing, breach or violation of the Rules must report it immediately.

The whistleblowing channel is the preferred channel through which to make these communications, which may be sent in writing, or made orally by telephone, directly to the Compliance Unit, the hierarchical superior or the Human Resources Office, which will transfer them to the PRISA CCO. The whistle-blower may also request a face-to-face meeting to report the irregularity. This request must be honoured within a maximum period of seven days in accordance with the applicable law.

If the communication is not sent through the whistleblowing channels integrated in the Internal Reporting System, and other communication channels are used, PRISA in any case guarantees the confidentiality of the information, which will be treated in a secure environment in addition to the personal information protection provisions imposed by law.

Oral communications, whether by face-to-face meeting or by telephone, shall be documented in any of the following ways:

- a) by recording the conversation in a secure, permanent and accessible format, provided that the whistle-blower is informed in advance that his/her communication will be recorded, that his/her data will be processed in accordance with the applicable law and that his/her consent is sought; or

- b) through a complete and accurate transcription of the conversation made by the staff responsible for processing it, in which case it will be provided to the whistle-blower to verify, correct and accept by signing the transcription of the message.

There are also compliance mailboxes available in different companies, through which complaints, allegations or inquiries can be sent, such as the following by way of example:

- PRISA mailbox: cumplimiento@prisa.com
- Prisa Media Mailbox: cumplimiento@prisamedia.com
- Santillana Global Mailbox: cumplimiento@santillana.com

The recipient of any irregularity that reaches compliance mailboxes or other mailboxes such as HR, or by any other means, must immediately notify the Reporting System Manager.

The exchange of information between the business compliance units and the PRISA CU will always be carried out in an environment of confidentiality, and will aim at the proper coordination and the best performance in compliance with the provisions of this procedure.

Likewise, a person knowing of the existence of irregular conduct, breach or violation of the rules may also inform the competent authorities and, if appropriate, the institutions, bodies, offices or agencies of the European Union. In Spain, one can contact the AII (*Autoridad Independiente del Informante*, or Independent Whistle-blower Authority), AEPD (*Agencia Española de Protección de Datos*, or Spanish Data Protection Agency) www.aepd.es, the CNMC (*Comisión Nacional de los Mercados y la Competencia*, or National Markets and Competition Commission) www.cnmc.es, or the CNMV (*Comisión Nacional del Mercado de Valores*, or National Securities Market Commission) www.cnmv.es depending on the nature of the irregularity.

3.2. Communication and receipt of communication

The communication should be as descriptive and detailed as possible, thus making it easier for the recipient to identify the potentially irregular behaviour and the person/s or department/s involved.

Any person who makes a complaint must do so in accordance with an unwaivable principle of good faith, with sufficient reasons and objective evidence to demonstrate the existence of the breach.

In any case, given the possibility of anonymity in the whistleblowing channel, complaints shall contain all the information that allows an analysis of the facts and, to the extent possible, the following information:

- Clear and detailed account of the facts.
- Identification of the Company or Business Unit in which they took place.
- Identification of the persons involved in the reported behaviour or with knowledge thereof.
- Time when the event occurred or has been occurring.
- Quantification, whenever possible, of the impact of the reported event.
- Provision, if considered to be necessary, of documents, files or other information deemed relevant for the assessment and resolution of the complaint.

When making the communication, the whistle-blower may indicate a domicile, e-mail address or secure place for the purpose of receiving notifications.

Unless it would jeopardise the confidentiality of the communication and if the complainant is not anonymous, an acknowledgement of receipt of the complaint shall be sent within a maximum period of seven days from its receipt. Communication with the whistle-blower may be maintained and, if necessary, additional information may be requested that may be useful for the handling of the complaint, always in a secure and confidential environment.

3.3. Receipt and classification of complaints

Complaints reported through the whistleblowing channel are received by the PRISA CU.

Upon receipt of the complaints, the PRISA CU will, in a first stage, determine whether the information provided constitutes an irregularity that must be investigated and the appropriate resources, methods and procedures for the investigation of each complaint, taking into account the nature and gravity of the complaint:

- Employment or human resources complaints
- Financial or accounting complaints
- Complaints concerning other areas of external regulation
- Other allegations or complaints.

If a reported event affects a specific Business Unit of the Prisa Group (either one of its companies or its employees), the PRISA CU will forward the complaint to the Compliance Unit of the corresponding Business Unit, and coordinate the analysis thereof with it, unless the complaint directly affects a member of that Compliance Unit.

The PRISA CU, always taking into account the relevance or risk of the reported facts, may inform the Chairman of the Audit, Risk and Compliance Commission (Audit Commission) in advance and on an extraordinary basis. Likewise, if the acts prima facie constitute a crime, in coordination with the legal and enforcement officer of the unit concerned it shall inform the Public Prosecutor's Office or the European Public Prosecutor's Office if the acts affect European Union interests.

The decisions taken by the PRISA CU at this stage shall be duly documented.

3.4. Communication to the whistle-blower

If the complaint constitutes an irregularity and additional information is required the Compliance Unit shall, following the analysis of the information provided, contact the whistle-blower if it provided contact information and, within a reasonable period which shall not exceed 3 months from the notification of the acknowledgement of receipt or 3 months and 7 days which may be extended to 6 months in cases of particular complexity, from the receipt of the communication for which no acknowledgement of receipt was sent, the whistle-blower shall be notified of the status of the complaint.

In the case of complaints that do not constitute irregularities, but can be considered as other types of complaints or requests for information, the Compliance Unit will refer them to the unit, area or department concerned for analysis or management and, where appropriate, to notify the response.

3.5. Informing the affected person

When and in the manner that the PRISA CU deems appropriate to ensure the successful outcome of the investigation, and in coordination, where appropriate, with the Business

Compliance Unit, managers or third parties that support the investigation process, the affected person will be duly informed of the actions and omissions attributed thereto. The affected person shall also have the right to be heard at any time during the investigation of the facts reported, and his/her statement shall be formally documented. In no case shall the identity of the whistle-blower be disclosed.

The recipient of the complaint and the person, if any, who processes it shall always respect the presumption of innocence of the affected person, as well as his/her right to honour.

3.6. Protection of personal information

The investigation of substantiated allegations should be initiated within the maximum term of three months from the date of the communication.

The personal information of complaints for which there is no investigation, due to their unsubstantiated nature, must be erased or anonymised when three months have elapsed after their receipt. The personal information of complaints that are not investigated may be kept after this period, provided that the purpose of the storage is to leave evidence of the functioning of the system. PRISA has a register of information received and investigations carried out in accordance with the provisions of the law. The personal information will be kept for the period necessary and proportionate for the purpose of complying with the legal provisions. In no case may the information be kept for a period longer than 10 years.

The processing of personal information relating to the reports received and to the investigations carried out by PRISA will be aimed at complying with legal obligations and carrying out the investigative actions that are deemed necessary. In no case will personal information, including information in special categories, that is not necessary for awareness and investigation of complaints be processed, proceeding, if necessary, to its immediate deletion.

Communications received through channels other than the Whistleblowing Channel, such as compliance or HR mailboxes, should be deleted immediately after informing the System Manager.

Access to the personal information contained in the Reporting System shall be limited, within the scope of their powers and functions, exclusively to:

- a) The System Manager and the person directly managing the System.
- b) The human resources officer or the duly designated competent body, only when disciplinary action could be taken against a worker.
- c) The person responsible for the legal services of the entity or body, if it is appropriate to take legal action in relation to the facts described in the communication.
- d) Any designated data processors.
- e) The data protection officer:

However, the processing of data by other persons, or even their communication to third parties, shall be lawful when necessary for the adoption of corrective measures in the entity or the conduct of the sanctioning or criminal proceedings, if applicable.

If it is proven that the personal information provided in the communication is not true, it will be immediately deleted from the moment that this circumstance is known, unless such lack of truth may constitute a criminal offence, in which case the information will be kept for the necessary time during which the judicial proceedings are processed.

Users of the Whistleblowing Channel may, if they are applicable, exercise the rights of access, rectification, deletion, opposition, limitation and portability with respect to their personal information appearing therein by written communication to PRISA at its registered office, providing sufficient proof of their identity, and identifying themselves as users of the Whistleblowing Channel.

The workers and collaborators of the Prisa Group, as subjects of possible complaints, are informed of the existence of this system of internal complaints, through the respective privacy policies for workers and collaborators.

PRISA undertakes to use those measures of a technical nature that are necessary to ensure the security, integrity, non-alteration and unauthorised access of the data provided.

The PRISA Group will act at all times under the current legislation and the values, principles and procedures established in its internal regulations.

4. MANAGEMENT OF THE PROCEDURE

This procedure is managed by the Chief Compliance Officer of PRISA, appointed by the Board of Directors as Manager of the Internal Reporting System. The modification of this procedure shall be approved by the PRISA Board of Directors.