POLICY OF THE FOUNDATION'S INTERNAL INFORMATION SYSTEM

Table of Contents

CHAPTER I: OBJECT, OBJECTIVE, SUBJECTIVE SCOPE, GENERAL PRINCIPLES AND GUARANTEES

Article 1. Purpose

The purpose of this policy is to regulate the operation of the Foundation's internal information system provided for in Article 5 of ***Law 2/2023, of 20 February, regulating the protection of people who report regulatory breaches and the fight against corruption***.

The internal information system includes the ethics or whistleblowing channel, which is a tool through which members of the Foundation's governing body, managers, workers, scholarship holders, etc. (informants) can inform the Foundation of the commission of criminal actions or infractions of which they are aware.

Article 2. Objective scope: Which violations can be reported

The Foundation's internal information system will allow whistleblowers (persons listed in Article 3) to report the following offences:

a) Actions or omissions that may constitute a serious or very serious criminal or administrative offence established in the legislation in force in Spain, especially in the field of the fight against corruption (including non-compliance with the obligations contemplated in the Foundation's code of good governance and the general regulations applicable to the Foundation's activity).

b) The following actions or omissions that may constitute breaches of European Union law:

- falling within the scope of the European Union acts listed in the Annex to EU Directive 2019/1937 (on matters relating to public procurement; financial services, products and markets and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety, animal health and animal welfare; public health; consumer protection; protection of privacy and personal data, and security of networks and information systems.)

- affecting the financial interests of the European Union as set out in Article 325.

- that have an impact on the internal market as established in Article 26 of the Treaty on the Functioning of the European Union.

Excluded from the scope of application of this policy are cases that are governed by its specific regulations, provided for by sectoral laws or by EU instruments, such as in relation to the prevention of occupational risks, prevention of sexual harassment, etc.

Article 3. Subjective scope of application: To whom it applies: the informants

3.1.- This policy applies to persons who report violations of the scope described in Article 2 above who have obtained the information in a work or professional context, including:

a. The Foundation's workers.
b. Self-employed or self-employed who provide services for the Foundation.
c. Members of the Foundation's governance, administration, management or supervisory bodies, as well as any entity that relates to the Foundation.
d. Any person working for or under the supervision and direction of contractors, subcontractors, and suppliers of the Foundation.
e. People who have obtained information within the framework of an employment relationship that has ended, such as volunteers, interns, workers in training periods regardless of whether or not they receive remuneration, as well as those who have obtained the information in a selection process in which they have participated.

The policy also applies to the legal representatives of the workers in the exercise of their functions of advising and supporting the whistleblower, to the people who assist the whistleblower, to the people who are related to the whistleblower and may suffer any type of retaliation (such as their relatives) and to the people of the Foundation who are appointed to collaborate in the management of any kind retaliatory. Internal information channel established by this entity.

3.2.- Respecting this policy is an employment or contractual obligation, so non-compliance with it could be subject to disciplinary sanctions in accordance with the provisions of the regulatory labor regulations where the Foundation carries out its function (e.g. applicable Collective Agreement), as well as the corresponding regulations or contractual document.

Article 4. General principles of action of the Foundation in terms of the internal information system. Guarantees.

The general principles of action and guarantee that govern the internal information system of this Foundation are the following:

1. General principles of action:

a. ACCESSIBILITY: all persons referred to in Article 3 may report information on the infringements referred to in Article 2 through the ethics and whistleblowing channel integrated into the Foundation's internal information system.

b. ANONYMITY: Whistleblowers will be allowed the possibility of making anonymous communications if they so choose.

c. INDEPENDENCE AND IMPARTIALITY: independence and impartiality will be guaranteed in the management of the information received and its processing.

2. Procedural safeguards:

a. Confidentiality: The internal information system will guarantee the confidentiality of the identity of the informant and of any other person mentioned in the communication, as well as of the actions carried out during the management and processing.

b. Presumption of innocence: All persons affected by any type of communication, action and investigation shall have the right to the presumption of innocence, the right of defense and the right of access to the file, as well as the protection established by the informants, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

c. No retaliation: Acts constituting retaliation, including threats of retaliation and attempts at retaliation against persons who submit a communication in accordance with the provisions of these regulations, are expressly prohibited. Retaliation is understood to be any act or omission that, directly or indirectly, involves unfavorable treatment that places the people who suffer it at a particular disadvantage compared to others in the work or professional context due to their status as a whistleblower.

d. Compliance with the provisions on the protection of personal data: the processing of personal data within the communications of the Foundation's internal information system will be governed by the provisions of *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*, and the *Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.* No data that is not manifestly owned will not be collected to process specific information. If they are collected by accident, they will be deleted without delay.

CHAPTER II: THE PERSON RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM

Article 5. Responsible for the internal information system

The person responsible for the internal information system will be the director of the Foundation, who may be dismissed and replaced by the Board of Trustees. This responsible person will act with full autonomy and independence with respect to any other body, committee or commission of the Foundation.

Any worker or professional of the Foundation is obliged to collaborate with the person responsible for the system in accordance with this policy and current regulations.

The appointment and dismissal of the person responsible for the System will be notified to the Independent Authority for the Protection of Whistleblowers (AAI) or to the competent authority of the Generalitat de Catalunya, i.e. the Anti-Fraud Office of Catalonia, within a maximum period of ten working days, specifying, if applicable, the reasons and reasons for their dismissal.

CHAPTER III: EXISTING EXTERNAL CHANNELS OF INFORMATION

Article 6. External information channels

Any whistleblower referred to in Article 3 may also make use of the external information channels established by the Spanish Government, the Government of Catalonia, the institutions, bodies, offices and agencies of the European Union, and in particular what is established by the Independent Authority for the Protection of Whistleblowers (AAI) or the Anti-Fraud Office of Catalonia. which is the counterpart body at the regional level.

CHAPTER IV: THE PROCEDURE FOR COMMUNICATION AND MANAGEMENT OF INFORMATION

Article 7. Information management procedure

The communication and information management procedure is made up of the following phases:

1) **Carrying out the communication:**

The persons listed in Article 3 may make their communications **through the Pau Costa Foundation website** www.paucostafoundation.org/transparencia.

It is important that the respondent gives a detailed description of the infraction, providing as far as possible the following data:

- Description of the fact of what is reported with an indication of the date on which it occurred.
- Identity of the person(s) responsible for the act if known
- Evidence available, if applicable
- Identification of the informant, although he or she may report/report anonymously.

It is the obligation of the informant not to be untruthful in the information provided.

2) <u>Reception and admission/non-admission for processing:</u>

Once a communication has been received by the person in charge of the information system, (at the time of submitting the communication, the system will inform you of a code to be able to follow up on your communication.

The person in charge of the information system will study the facts reported and the documents, if any, provided and will decide whether to admit the communication or not.

A communication may not be admitted provided that it is one of the following cases:

a) When the facts reported are totally implausible.
b) When the facts reported do not constitute an infringement or omission of compliance with the legal system as established in Article 2.
c) When the communication of the information is manifestly grounded or there are indications that it has been obtained through the commission of a crime. In this case, moreover, the non-admission will be sent to the Public Prosecutor's Office with a detailed account of the facts that are considered to constitute a crime.

Non-admission must always be justified, and the informant will be notified.

In case of admission, the next phase of instruction will be carried out.

3) <u>Instruction</u>

The system manager shall carry out the necessary actions and investigations in order to obtain sufficient information to reach a conclusion on the communication received from the reporting person and may maintain the communications it deems appropriate with the reporting person and may request additional information. The system manager may be supported by specialised technicians, if necessary.

The person or persons affected by the communication and the information received or obtained shall have the right to be informed at all times of the actions or omissions attributed to them, and to be heard at any time during the proceedings and investigations, at the time and in the manner considered most appropriate in each case. informing them that they can appear with legal assistance.

All communications will be duly registered, and if they are verbal, the provisions of Article 7 of Law 2/2023 will apply to them.

The person or persons affected by the communication and the information received shall have the right to have access to the file, without any type of information that could identify the reporting person being disclosed.

4) Completion of the procedure

1. Once the proceedings and investigations have been completed within the period established in Article 11, the person in charge of the system shall issue a report containing at least:

- ✓ Identification of the communication code and the date of registration.
- ✓ An exposition of the facts.
- ✓ The actions and investigations carried out in order to verify the plausibility of the facts.
- ✓ The conclusions and the assessment of the proceedings and the evidence that supports them.

2. Once the report has been issued, one of the following decisions will be taken:

- ✓ File the file.
- ✓ Imposition of disciplinary measures.
- ✓ Referral to the Public Prosecutor's Office immediately, if there are indications that the facts may constitute a crime.
- ✓ Referral to the European Public Prosecutor's Office in cases where the facts affect the financial interests of the European Union.
- ✓ Referral of the file to the authority, entity or body that is considered competent in cases of actions or omissions that are considered a serious or very serious administrative offense.

3. The decision shall be communicated to the reporting person and to the affected party or parties within a period not exceeding seven working days from the date of issuance of the report.

The maximum period for resolving the file, including the investigation phase, will be **three months from the receipt of the communication**. In cases of special complexity that require an extension of the deadline, provided that it has a properly reasoned report, the period may be extended by a maximum of three more months.

Article 8. Registration of communications and information

All communications, information, actions and investigations shall be recorded in a communications record book containing the following data:

a) Date of receipt.
b) Identification code.
c) Actions to be carried out.
d) Measures adopted.
e) Date of closure of the file.

This record book will not be public, and its contents may only be accessed in whole or in part at the reasoned request of the competent judicial authority, within the framework of a judicial process and under the tutelage of the judicial authority.

Article 9. Protection of personal data

The personal data collected through the ethics and complaints channel will be processed for the exclusive purpose of processing the complaints and queries received and, if appropriate, investigating the reality of the facts reported.

Both the complainant and the person reported will be duly informed, in each case, of the specific persons and bodies to which their data will be communicated.

The processing of data within the framework of the channel is carried out to fulfil a mission carried out in the public interest, such as the management of an internal channel that aims to prevent and discover possible behaviors that contravene both current legal regulations. All this in accordance with 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 (GDPR) and Organic Law 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights (LOPDGDD).

The PAU COSTA FOUNDATION is responsible for the processing of personal data, and the contact details are:

- Address: Av. Mossèn Cinto Verdaguer, 42 esc. A. bxs 2ª, 08552 Taradell

- Email address: info@paucostafoundation.org

Any complainant or reported person may contact here, to consult any question that strictly affects the processing of their personal data, as well as for the exercise of their legitimate rights, such as the right of access, rectification, deletion, limitation and opposition to the processing of their data by writing to FUNDACIÓN PRIVADA, at the addresses indicated, including the name and surname, address for notification purposes, copy of ID card and right exercised. Likewise, you may also contact the competent supervisory authority to file the complaint you consider appropriate.

The PAU COSTA FOUNDATION does not communicate personal data to third parties. Except in cases where required by law, your personal data may be provided to public bodies, State security forces and bodies, and judges and courts.

The data of the person making the complaint, of the person reported and third parties, will be kept for the time necessary to decide on the suitability of initiating an investigation into the facts denounced, and if so, the data will be kept for the time that it remains open.

If it is concluded that it is inappropriate to initiate an investigation, the data will be blocked immediately and will be kept only for the legal period of limitation of any possible claims that may arise.

The personal data collected within the framework of the whistleblowing channel will be limited to those strictly necessary to process the complaints. This data will be processed at all times in accordance with the applicable data protection regulations, for legitimate and specific purposes in relation to the investigation that may arise as a result of the complaint, and will be appropriate and not excessive in relation to the aforementioned purposes.

The PRIVATE FOUNDATION will ensure that all the necessary technical and organizational measures are adopted to preserve the security of the data collected in order to protect them from unauthorized disclosure or access. To this end, the Foundation has adopted appropriate measures to guarantee the confidentiality of all personal data.

Single additional provision

In all matters not provided for in these regulations, the provisions of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory and anti-corruption infringements, as well as those regulatory provisions that develop it, and the rules approved by the Generalitat of Catalonia on this aspect, will apply.

Approval date: 04/12/2024