CEAMSA

# Internal information systems policy

www.ceamsa.com

# Index

# INTERNAL INFORMATION SYSTEMS POLICY

In compliance with the provisions of article 5.2.h of Law 2/2023 of 20 February, regulating the protection of individuals who report regulatory infringements and the combat against corruption, **CEAMSA** has drawn up the following Internal Reporting System Policy.

**CEAMSA** has implemented an internal information system that meets the requirements established within the regulations (among others), which is accessible, guarantees confidentiality, has sound practices in terms of monitoring, investigation, and protection of the informant.
In addition, a person responsible for the Internal Information System has been appointed, who will be the person in charge of managing and, where appropriate, processing all communications received through our communications channels.

## 1. SCOPE

### 1.1 Personnel

This Policy applies to informants who are employed by the Company and who have obtained information about violations in an employment or professional context, including in any event:

- Employees and the self-employed;
- Shareholders and persons belonging to the administration, management or supervisory body of the company, including non- executive members, as well as volunteers, trainees and interns, whether paid or unpaid; individuals who no longer have a relationship with the organisation due to the termination of their contract;
- Any individual working under the supervision and direction of contractors, subcontractors and suppliers;

• Informants who communicate or publicly disclose information on offences obtained in the framework of an employment relationship that has already ended;

• Informants whose contractual relationship has not yet commenced, if the offence is obtained during the selection process or pre-contractual negotiation;

• All individuals who are directly or indirectly involved in the procedure may be retaliated against as a result (advisors of the informant, representatives, etc.).

## 1.2 Material breach

The following shall be subject to investigation

(a) Any acts or omissions which may constitute breaches of European Union law provided that:

Within the applicable scope of the European Union acts listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and the Council of 23 October 2019 on the protection of persons reporting breaches of Union law, irrespective of the classification of such breaches in the domestic legal system.

The financial interests of the European Union are affected, as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); or have an impact on the internal market, as referred to in Article 26(2) TFEU, including infringements of EU competition rules and aid granted by States, as well as infringements relating to the internal market in relation to acts in breach of corporate tax rules or practices aimed at obtaining a tax advantage that would defeat the object or purpose of the legislation applicable to corporate taxation.

(b) Deeds or omissions that may constitute a serious or very serious criminal or administrative offence. In any event, all serious or very serious criminal or administrative offences that involve financial loss sustained by the Public Treasury and the Social Security will be deemed to be included.

***By way of example, and without prejudice to the exclusion of others, these are subject matters of communication:***

- Public procurement;
- Financial services, products and markets, and 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;
- Privacy and personal data protection, network and information systems security;
- Infringements affecting the EU's financial interests (competition, state aid, tax advantages or corporate tax infringements);

Infringements of workers' rights;

- Bribery and embezzlement;
- Actions or omissions that may constitute serious or very serious criminal or administrative offences, always including those that affect financial losses to the Public Treasury and Social Security.

## 2. GENERAL GUIDELINES

The entire communications procedure and the existing internal communication channels comply with the requirements set out in art. 9.2. of Law 2/2023. In particular, the procedure meets the following minimum content and standards:

• Identification of the internal information channels;

• Issuing an acknowledgement of receipt to the informant on receiving the communication;

• Establishment of the maximum time limit for responding to the investigation proceedings;

• Provision for the possibility of maintaining communication with the reporting person and, if deemed necessary, requesting additional information from the reporting individual;

• Establishing the right of the person concerned to be informed of the actions or omissions attributed to him/her, and to be heard at any time;

• The guarantee of confidentiality of the communications sent and, where appropriate, the obligation of the individual receiving the communication to forward it immediately to the individual in charge;

• Ensuring the presumption of innocence and the honour of the persons affected;

• Compliance and respect for the protection of personal data;

Immediate forwarding of the information to the Public Prosecutor's Office when the facts may be indicative of a criminal offence. In the event that the facts affect the financial interests of the European Union, it shall be referred to the European Public Prosecutor's Office.

## 3. RIGHTS OF REPORTING PARTIES

### 3.1 Rights and guarantees

The reporting person shall have the following rights and guarantees in their actions:

• Decide whether they wish to make the report anonymously or non- anonymously; in the latter case, the identity of the informant shall be kept confidential,

• Formulate communication verbally or in writing;

• Indicate an address, e-mail address or safe place to receive communications regarding the investigation;

• Waive the right to receive communications from the investigation;

• Appear on one's own initiative or when required to do so in the proceedings, being represented, if considered appropriate, by a lawyer;

• To request that the appearance be made by videoconference or other telematic means that guarantee the identity of the informant, and the security and fidelity of the communication;

• Exercise the rights conferred by personal data protection legislation;
To know the status of their complaint and the results of the investigation;

### 3.2 Prohibition of victimisation

The principle of informant protection is established by expressly prohibiting reprisals, which are understood as any acts or omissions that are prohibited by law, or that, directly or indirectly, entail unfavourable treatment that places the individuals who suffer them at a particular disadvantage with respect to another in the employment or professional context, solely because of their status as informants, or because they have made a public disclosure.

According to the regulations, reprisals include, but are not limited to, actions taken in the form of:

• Employment contract suspension, dismissal or termination of the employment or statutory relationship, unless the measures were carried out as part of the regular exercise of management powers under labour legislation, due to circumstances, facts or accredited infringements unrelated to the submission of the report.

• Damages, including those of a reputational nature, or economic losses, coercion, intimidation, harassment or ostracism.

- Negative evaluation or references regarding job or professional performance.
- Blacklisting or dissemination of information in a particular sectoral area, which makes it difficult or impossible to obtain employment or contract work or services.
- Refusal or cancellation of a licence or permit.
- Refusal of training.
- Discrimination, or unfavourable or unfair treatment.

In addition, a person who submits a communication or makes a public disclosure has the right not to have his or her identity disclosed to third parties.

Internal information systems, the external channels and those receiving public disclosures shall not obtain data that allow the identification of the informant and there has to be adequate technical and organisational measures in place to preserve the identity and ensure the confidentiality of the data pertaining to the persons concerned and any third party mentioned in the information, especially the identity of the informant in case he/she has been identified.

## 4. COMMUNICATION CHANNELS

Any person and external parties who are linked to the organisation can submit their information or claims through the whistleblowing channels set up by the company and managed by an external office, which are:

***• Ethics e-mail address: ceamsa@denunciascanal.com***
***• Toll-free number: 900 869 931***
***• Complaints channel form on the website, in a separate and easily identifiable section.***
***• By letter to the postal address.***
***• In person: If the informant requests, he/she may report by means of an in-person meeting within a maximum period of seven days.***

If, after an investigation, it can be concluded that the facts investigated are false and that the complaint has been made in bad faith, the person responsible for the procedure shall conclude that the complaint has been archived, stating in writing the reasons for the archiving of the complaint.

It must be known that the filing of a false report by an employee with reckless disregard for the truth or a clearly malicious attitude constitutes an infringement of the covenant of good faith that must govern employment relations in any company.

In addition, this conduct is typified in Article 456 of the Penal Code, which punishes this act, in the event of legal proceedings and a judge determines this to be a less serious offence, punishable by means of a fine from twelve to twenty-four months and, in the case of a serious offence, by imprisonment from six months to two years and a fine from twelve to twenty-four months.
Internal reporting mechanisms, by any form or means:

- Enable all the above-mentioned individuals to communicate information of infringements of the aforementioned material scope of application.
- These systems are designed, established and managed in a secure manner, and in such a way as to guarantee the confidentiality of the informant and of any third party mentioned in the communication, and of the actions carried out in the management and processing of the aforementioned communication, as well as the protection of data, impeding access by unauthorised personnel.
- They allow the submission of communications in writing, verbally, or both.

They guarantee that the communications submitted can be dealt with effectively so that the first to know about the possible irregularity is the entity itself.

- A systems manager is in place.
- A procedure has been implemented for investigating and managing the information received.
- It establishes guarantees for the protection of informants within the entity.

## 5. INFORMATION ON THE INTERNAL REPORTING CHANNEL

The purpose of this document, together with the Complaints Channel User Manual, is to provide information in a clear and easily accessible manner on the use of any implemented internal information channel, as well as on the main principles of the management procedure in accordance with the provisions of art. 25 of Law 2/2023.

## 6. REGISTERING OF INFORMATION

It is hereby notified that, in compliance with the provisions of art. 26 of Law 2/2023, this organisation keeps a register of the information received and the internal investigations which have been conducted, guaranteeing, in all cases, the confidentiality requirements provided for in this law.

It should be noted that this register shall not be public and only at the justified request of the competent judicial authorities, by means of an order, and within the framework of judicial proceedings and under its supervision, may access all or part of the contents of the said register.

## 7. PERSONAL DATA PROTECTION

The provisions of articles 29 to 32 of Law 2/2023, as well as the provisions on this matter in any of its precepts and other applicable regulations on data protection will be applicable.


CE
AM
SA