

<b>COSENTINO</b>	<b>INTERNAL INFORMATION SYSTEM</b>	<b>Version 1</b>
	<b>POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION</b>	<b>Edition: 22<sup>nd</sup> January 2025</b>

**POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION**

<b>SUPERVISED BY</b>
Compliance Body
<b>Date:</b> January 2025

<b>APPROVED BY</b>
Board of Directors
<b>Date:</b> February 2025

The original document, approved by the Company's Board of Directors on the date indicated above, is safeguarded by the *Compliance Body*.

<b>COSENTINO</b>	<b>INTERNAL INFORMATION SYSTEM</b>	<b>Version 1</b>
	<b>POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION</b>	<b>Edition: 22<sup>nd</sup> January 2025</b>

**Table of contents**

<b>1. Purpose</b>	<b>3</b>
<b>2. Scope</b>	<b>3</b>
<b>3. The Internal Information System (IIS)</b>	<b>4</b>
<b>3.1 General Principles and Safeguards</b>	<b>4</b>
<b>3.2 Information Channels</b>	<b>4</b>
<b>3.3 Head of the Internal Information System</b>	<b>5</b>
<b>3.4 Procedure</b>	<b>5</b>
<b>4. Protection of Whistleblowers</b>	<b>6</b>
<b>4.1 Protection requirements</b>	<b>6</b>
<b>4.2 Prohibition of retaliation</b>	<b>7</b>
<b>4.3 Support and protection measures</b>	<b>7</b>
<b>5. Publicising</b>	<b>9</b>
<b>6. Personal data protection</b>	<b>9</b>
<b>7. Entry into force</b>	<b>9</b>

<b>COSENTINO</b>	<b>INTERNAL INFORMATION SYSTEM</b>	<b>Version 1</b>
	<b>POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION</b>	<b>Edition: 22<sup>nd</sup> January 2025</b>

## **1. Purpose**

The purpose of this Policy is to outline the general principles that inspire the Internal Information System (“IIS”) of the business group led by Cosentino, S.A. (referred to collectively as “**Cosentino**” or the “**Organization**”), in accordance with the provisions of Spanish Act 2/2023, of February 20, regulating the protection of persons who report regulatory violations and anti-corruption measures (the “**Whistleblower Protection Act**”), without prejudice to its particular development by non-Spanish subsidiaries in accordance with the local legislation that affects them, if applicable.

In line with the compliance and business ethics culture of Cosentino, S.A., as reflected, among other things, in its General Criminal Compliance Policy and the adoption of criminal compliance models (“**CCM**”) within the Organization, the Internal Information System has a dual objective: on the one hand, to protect individuals who report breaches within its scope, and on the other, to strengthen and promote a culture of information and communication as a mechanism to prevent and detect irregular conduct, and to respond to it.

## **2. Scope**

For the purpose of this Policy, breaches are considered to be actions or omissions covered by Article 2 of the Whistleblower Protection Act, as well as any conduct contrary to the CCM adopted in the Organization and the measures that are part of them or any other measures implemented to prevent any actions contrary to the law and the principles and values defined by the Organization.

Breaches may also be reported when they may have been committed by third parties outside the Organization, as long as they participate in the exercise of social activities on behalf of the Organization.

This Policy applies to whistleblowers, that is, any natural person who reports possible actions or omissions covered by Article 2 of the Whistleblower Protection Act in a labor or professional context as provided in paragraphs 1 and 2 of Article 3 of said Act.

It also applies to, and whistleblowers will be considered for the purposes of this Policy, the recipients of the Organization's CCM when, in accordance with the provisions of the CCM, they fulfil their obligation to report any conduct that may be contrary to the CCM and the measures that are part of them.

In any case, communications or information outside the material scope of application established in Article 2 of the Whistleblower Protection Act and their senders will be outside the scope of regulation and protection provided by said Act.

<b>COSENTINO</b>	<b>INTERNAL INFORMATION SYSTEM</b>	<b>Version 1</b>
	<b>POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION</b>	<b>Edition: 22<sup>nd</sup> January 2025</b>

### **3. The Internal Information System (IIS)**

The IIS mainly consists of the channel enabled for receiving communications related to breaches, the head of the IIS, and the procedure to be followed for processing the aforementioned communications, called the ***“Procedure for the Management of Information Received in the Internal Information System” (“IIS Procedure”)***.

#### **3.1 General Principles and Safeguards**

All actions carried out within the framework of the IIS will be conducted securely, in accordance with criteria of proportionality and objectivity, with the utmost respect for current legislation and recognizing the rights of all parties involved.

In any case, confidentiality and the rights to privacy, honour, defence, and presumption of innocence of the persons involved in the investigation process initiated as a result of receiving a communication through the Organization's IIS will be guaranteed.

Communications may be made in writing or verbally and may be anonymous.

The identity of the whistleblower, if known, as well as the third parties mentioned in the communication, may only be disclosed, in addition to the third parties indicated in the privacy policy, to the Judicial Authority, the Public Prosecutor's Office, or the competent Administrative Authority within the framework of a criminal, disciplinary, or sanctioning investigation, after informing the whistleblower or the affected third party, provided that this circumstance does not compromise the investigation or the ongoing judicial procedure.

Actions aimed at verifying and clarifying the facts contained in the received communications must be carried out observing all guarantees expressly provided in the IIS Procedure for the persons involved.

In the case of the person affected by the communication, their right to be informed of the facts attributed to them and to be heard at any time is recognized. Once informed, they may request to examine the information and documentation contained in the Investigation File referred to in section 3.4 of this Policy, although necessary measures must be taken to ensure that no information revealing the identity of the whistleblower is disclosed.

Investigation actions must be carried out with the greatest diligence, agility, and effectiveness possible, considering the complexity of the facts, always observing the deadlines established in the IIS Procedure.

#### **3.2 Information Channels**

The IIS should be used as the preferred channel for reporting breaches through the internal channel established by the Organization, as diligent and effective action by the Organization could potentially limit the harm caused by the investigated actions.

<b>COSENTINO</b>	<b>INTERNAL INFORMATION SYSTEM</b>	<b>Version 1</b>
	<b>POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION</b>	<b>Edition: 22<sup>nd</sup> January 2025</b>

In this regard, the channel enabled in Cosentino's IIS for the communication of information related to possible non-compliance is the Ethical Channel (<https://www.cosentino.com/ethical-channel/>), which was implemented and operational in the Organization prior to the entry into force of the Whistleblower Protection Act.

This internal channel is securely designed to ensure the confidentiality of the Whistleblower's identity, the affected person, and any third party mentioned in the communication, as well as the protection of personal data, preventing access by unauthorized personnel.

Without prejudice to the preferential use of the internal channel described above, for the communication of possible non-compliance covered by the Whistleblower Protection Act, Whistleblowers may also access the channels established by Public Administrations for these purposes ("**external channels**"), either directly or after communication through the aforementioned internal channel.

### **3.3 Head of the Internal Information System**

The Board of Directors of Cosentino, S.A., after having carried out the mandatory consultation with the legal representation of the workers, is responsible for the implementation of the IIS and appoints the Director of Compliance or Chief Compliance Officer ("**CCO**") of Cosentino as the head of the IIS.

This is a single-person body that also assumes the function of supervising the CCM of the Organization.

The appointment of the head of the IIS will be notified to the Independent Authority for Whistleblower Protection.

The head of the IIS will diligently, and in the absence of conflict of interest, manage the information received through the established channel, ensuring the proper application of the IIS Procedure, without prejudice to the possible outsourcing of the reception of information.

The head of the IIS will also maintain a register of the information and communications received and the Investigation Files that have resulted from them, as indicated in the IIS Procedure, guaranteeing the confidentiality of such information and compliance with data protection regulations.

The head of the IIS has the necessary material and personnel resources for the proper development of their functions, which they perform autonomously and independently from the rest of the Organization's bodies, and their actions must be governed by the general principles set out in this Policy.

### **3.4 Procedure**

The IIS Procedure regulates the management and processing of communications received through the Organization's Internal Information System.

<b>COSENTINO</b>	<b>INTERNAL INFORMATION SYSTEM</b>	<b>Version 1</b>
	<b>POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION</b>	<b>Edition: 22<sup>nd</sup> January 2025</b>

The set of actions carried out to verify and clarify the facts contained in the communications received through the internal channel established by the Organization will form the Investigation File, the phases of which are regulated in the IIS Procedure.

In the event that the facts subject to the information could potentially constitute a crime, they must be reported to the Public Prosecutor's Office or the European Public Prosecutor's Office, as appropriate, applying in any case the provisions of the Organization's **"Special Protocol on Internal Investigations concerning Legal Entities"**.

## **4. Protection of Whistleblowers**

### **4.1 Protection requirements**

Whistleblowers must act in good faith. Communications should be made observing the criteria of truthfulness and proportionality and should only refer to facts that have some relation to the Organization. False or malicious communications or information may lead to the application of the current disciplinary regime, as well as the adoption of corresponding legal actions for the claim of any damages that may have been caused.

In addition to the Whistleblowers referred to in sections 1 and 2 of Article 3 of the Whistleblower Protection Act, the protection measures provided for in Title VII of said Law and this Policy will also extend to the legal representatives of the workers in the exercise of their advisory and support functions to the Whistleblower, as well as to the natural and legal persons related to the Whistleblower under the terms provided in section 4 of the aforementioned Article 3.

All of them will have the right to the protection provided in this section of this Policy as long as the following circumstances are met:

- They have reasonable grounds to believe that the information provided in this section is true at the time of communication or disclosure, even if they do not provide conclusive evidence, and that the said information falls within the scope of the Whistleblower Protection Act.
- The communication or disclosure has been made in accordance with the requirements set forth in the Whistleblower Protection Act.

Those who communicate or disclose information that is inadmissible according to the provisions of the IIS Procedure, those related to claims about interpersonal conflicts or that only affect the Whistleblowers, and the people referred to in the communication or disclosure, or those completely available to the public or mere rumours, are expressly excluded from the protection provided in this section.

Although those who communicate or disclose actions or omissions outside their material scope are also excluded from the protection provided by the Whistleblower Protection Act, the Organization strictly prohibits any kind of retaliation against those who communicate actions or omissions that are, in any case, contrary to the CCM and the

<b>COSENTINO®</b>	<b>INTERNAL INFORMATION SYSTEM</b>	<b>Version 1</b>
	<b>POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION</b>	<b>Edition: 22<sup>nd</sup> January 2025</b>

measures that are part of them or any other measures implemented for the prevention of any actions contrary to the law and the principles and values defined by the Organization.

## **4.2 Prohibition of retaliation**

The Organization will not adopt (and will ensure that its professionals do not adopt) any form of retaliation, direct or indirect, including threats or attempts of retaliation, against any person who has reported a non-compliance through the IIS or by any other means.

For the purpose of this Policy, retaliation is understood as any act or omission prohibited by law, or that, directly or indirectly, constitutes unfavourable treatment that places the person suffering it at a particular disadvantage compared to another in the work or professional context, solely because of their status as an Whistleblower, or for having made a public disclosure.

By way of example, the following are considered retaliations:

- Suspension of the employment contract, dismissal, or termination of the employment or statutory relationship; imposition of any disciplinary measure; demotion or denial of promotions and any other substantial modification of working conditions; and the non-conversion of a temporary employment contract into a permanent one, if the person who made the communication had legitimate expectations in this regard; unless these measures are carried out within the regular exercise of management power under labor legislation or the corresponding public employee statute, due to circumstances, facts, or proven infractions, and unrelated to the submission of the communication.
- Damages, including reputational damage, or economic losses, coercion, intimidation, harassment, or ostracism.
- Negative evaluations or references regarding work or professional performance.
- Inclusion in blacklists or the dissemination of information in a specific sectoral scope, which hinder or prevent the person from accessing employment or contracting works or services.
- Denial or cancellation of a license or permit.
- Denial of training.
- Discrimination or unfavourable or unfair treatment.

## **4.3 Support and protection measures**

Additionally, the Whistleblower Protection Act provides a series of support and protection measures for Whistleblowers who report the actions or omissions outlined in its Article 2. These measures, which may be facilitated by the Independent Authority for Whistleblower Protection or another competent authority or body, include the following:

<b>COSENTINO®</b>	<b>INTERNAL INFORMATION SYSTEM</b>	<b>Version 1</b>
	<b>POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION</b>	<b>Edition: 22<sup>nd</sup> January 2025</b>

- Support measures:
  - Comprehensive, independent, and free information and advice on available procedures and resources, protection against retaliation, and the rights of the affected person.
  - Effective assistance from competent authorities before any relevant authority involved in their protection against retaliation, including certification that they can receive protection under the Whistleblower Protection Act.
  - Legal assistance in criminal proceedings and cross-border civil proceedings in accordance with community regulations.
  - Financial and psychological support, exceptionally, if decided by the Independent Authority for Whistleblower Protection (A.A.I.), after assessing the circumstances arising from the submission of the communication.
  
- Protection measures:
  - It will not be considered that the Whistleblower has violated any disclosure restrictions, and they will not incur any liability in relation to such communication or public disclosure, provided they had reasonable grounds to believe that the communication was necessary to reveal a non-compliance, in accordance with the definition included in the Whistleblower Protection Act. This measure will not affect criminal liabilities. The provisions of the previous paragraph extend to the communication of information made by the representatives of the workers, even if they are subject to legal obligations of secrecy or not to disclose confidential information. All this without prejudice to the specific protection rules applicable under labor regulations.
  - The Whistleblower will not incur liability regarding the acquisition or access to the communicated information, provided that such acquisition or access does not constitute a crime.
  - In proceedings before a judicial body or other authority related to the damages suffered by the Whistleblower, once they have reasonably demonstrated that they made a communication and suffered harm, it will be presumed that the harm occurred as retaliation for reporting. In such cases, the person who took the harmful measure will have to prove that the measure was based on duly justified reasons unrelated to the communication.
  - In judicial processes, including those related to defamation, copyright infringement, breach of secrecy, violation of data protection regulations, disclosure of trade secrets, or claims for compensation based on labor or statutory law, the Whistleblower and those legally extended whistleblower

<b>COSENTINO®</b>	<b>INTERNAL INFORMATION SYSTEM</b>	<b>Version 1</b>
	<b>POLICY OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION</b>	<b>Edition: 22<sup>nd</sup> January 2025</b>

protection will not incur any liability. The Whistleblower and those legally extended whistleblower protection will have the right to argue in their defence and within the framework of the aforementioned judicial processes that they communicated, provided they had reasonable grounds to believe that the communication was necessary to reveal an infringement under the Whistleblower Protection Act.

## **5. Publicising**

The head of the IIS will ensure that the necessary and appropriate information is provided clearly and easily accessible so that Whistleblowers can make use of the Organization's internal channel.

All information about the use of the internal channel established by Cosentino, as well as the essential principles of the IIS, can be consulted on the Organization's corporate website at the following address:

<https://www.cosentino.com/ethics-compliance/>

## **6. Personal data protection**

The processing of personal data carried out within the framework of the IIS will be done in full compliance with the general principles and obligations established in personal data protection regulations and the Whistleblower Protection Act.

The data collected in the IIS will be processed by the Organization acting as the data controller.

## **7. Entry into force**

This Policy shall enter into force on 1<sup>st</sup> March 2025.