

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

**PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE
INTERNAL INFORMATION SYSTEM**

SUPERVISED BY
Compliance Body
Date: January 2022
Date: June 2023
Date: January 2025

APPROVED BY
Board of Directors
Date: October 2022
Date: October 2023
Date: February 2025

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

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

Table of contents

1. Purpose	3
2. Scope	3
2.1 Objective Scope	3
2.2 Subjective Scope	4
3. Head of the internal information system	4
4. Information Channels	4
4.1 Internal Channels	5
4.2 External Channels	6
5. Processing of investigation files	7
5.1 General issues	7
5.2 Receipt, acknowledgement of receipt and acceptance/rejection for processing	7
5.3 Investigation File Instruction	9
6. Record	16
7. Publicising	16
8. Personal data protection	16
9. Preparation of Periodic Reports for the Organization's CCM	16
10. Entry into force	17

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

1. Purpose

The purpose of this Procedure is to develop the general principles outlined in the Policy of the Internal Information System and whistleblower protection of the business group led by Cosentino, S.A. (“**Cosentino**” or the “**Organization**”), regulating the process of receiving information related to any conduct that may constitute a breach within the objective scope outlined below, as well as the processing of investigation files that may arise. All in accordance with the provisions of Law 2/2023, regulating the protection of persons who report regulatory breaches and anti-corruption measures (the “**Whistleblower Protection Act**”).

2. Scope

2.1 Objective Scope

This Procedure applies to information received through the Organization's Internal Information System (the “**IIS**”) related to potential breaches.

For the purposes of this Procedure, breaches are considered to be:

- a. Any actions or omissions that may constitute violations of European Union (“EU”) law, provided they:
 1. Fall within the scope of the EU acts listed in the annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law, regardless of how they are classified under domestic law.
 2. Affect the financial interests of the EU as contemplated in Article 325 of the Treaty on the Functioning of the European Union (TFEU).
 3. Impact the internal market as contemplated in Article 26, paragraph 2 of the TFEU, including breaches of EU competition rules and state aid, as well as breaches related to the internal market concerning acts that violate corporate tax rules or practices aimed at obtaining a tax advantage that distorts the object or purpose of the applicable corporate tax legislation.
- b. Actions or omissions that may constitute a criminal offense or serious administrative violation.

Any conduct contrary to the criminal compliance models (“CCM”) adopted by the Organization and the measures that are part of them, or any other measures implemented to prevent any action contrary to the law and the principles and values defined by the Organization.

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

Breaches committed by third parties outside the Organization, provided they participate in the exercise of social activities on behalf of the Organization.

2.2 Subjective Scope

Any natural person who makes a communication about possible actions or omissions listed in Article 2 of the Whistleblower Protection Act in a work or professional context, as provided in paragraphs 1 and 2 of Article 3 of said Law, will be considered a whistleblower.

For the purpose of this Procedure, whistleblowers include, but are not limited to employees, shareholders, participants, suppliers, contractors, subcontractors, members of governing, management, or supervisory bodies, including non-executive members, volunteers, interns, trainees, job applicants, persons who have had a work or statutory relationship with the Organization, even if it has ended.

Likewise, the recipients of the Organization's CCM will be considered whistleblowers for the purposes of this Procedure 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.

3. Head of the Internal Information System

The Board of Directors of Cosentino, S.A. appoints the Director of Compliance or Chief Compliance Officer (“**CCO**”) of Cosentino, S.A. 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 manage the information received through the established channel, ensuring the proper application of this Procedure, without prejudice to the possible outsourcing of information reception.

In accordance with the general principles outlined in the Policy of the Internal Information System and whistleblower protection, the head of the IIS has the necessary material and personal resources for the proper development of their functions, which they perform autonomously and independently from the other bodies of the Organization and must act in accordance with these general principles.

4. Information Channels

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

4.1 Internal Channels

The Organization will permanently make available to its directors, managers, employees, shareholders, suppliers, and other third parties related to the Organization, the internal channel indicated below, suitable for reporting potential breaches related to or affecting their professional activity, without prejudice to the possibility of directing their communications to the Independent Authority for Whistleblower Protection or any other competent authority or body.

The channel enabled in the Organization's IIS constitutes the preferred means for reporting information related to potential breaches, being the **Ethical Channel**.

The means established for directing information related to potential breaches through the internal channel are as follows:

- Written communication addressed either to the following postal address: Ctra. A-334 Km. 59; 04850 Cantoria (Almería) or through electronic resources at <https://www.cosentino.com/ethical-channel/>, where communication is allowed without providing the informant's name and other personal data.
- Verbal communication addressed to the following phone number: +34 660 667 966 or through the voice messaging system of the WhatsApp application or to the head of the IIS if opting to report in a face-to-face meeting, which will take place within **seven business days** following the request.

Verbal communications must be documented, with the informant's prior consent, in one of the following ways: i) by recording the conversation or ii) by a complete transcription of the conversation that can be reviewed by the informant.

The informant may indicate a postal or email address in their communication for receiving notifications and may also expressly waive receiving any further communication.

Communication can also be made anonymously by sending written communication to the aforementioned postal address without indicating the sender or personal data in its content.

The confidentiality of the communication and the identity of the informant and any third party mentioned in the communication will be protected through appropriate technical measures and organizational measures outlined in this procedure.

The identity of the informant, 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 in the context of a criminal, disciplinary, or sanctioning

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

investigation, after informing the informant or the affected third party, provided that this does not compromise the ongoing investigation or judicial procedure.

Informants must act in good faith. Communications must 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 disciplinary regime in force in the Organization, as well as the adoption of legal actions for the claim of damages that may have been caused.

Retaliation, including threats and attempts of retaliation against informants and persons in their environment, is expressly prohibited. Retaliation is understood as any acts and omissions that are prohibited by law, or that, directly or indirectly, constitute unfavourable treatment that places the persons suffering them at a particular disadvantage compared to others in the work or professional context, solely because of their status as informants or for having made a public disclosure.

When the information provided by the informant refers to the breaches indicated in paragraphs a) and b) of section 2.1. of this Procedure, the informant may access the following support measures that, if applicable, would be provided by the Independent Authority for Whistleblower Protection or another competent authority or body:

- Information and advice on available procedures and resources, protection against retaliation, and the rights of the person potentially responsible for the facts subject to the communication or information received (the “**affected person**”).
- Assistance from competent authorities before any relevant authority involved in their protection against retaliation.
- Legal assistance in criminal proceedings and cross-border civil proceedings in accordance with community regulations.
- Financial and psychological support, exceptionally.

4.2 External Channels

Without prejudice to the preferred channel of the internal channel described above, informants may also access the channels established by Public Administrations for reporting breaches (“**external channels**”), either directly or after communication through the aforementioned internal channel.

The above will not apply to communications of breaches consisting of any conduct contrary to the measures that are part of the CCM, as well as any other measures implemented to prevent any action contrary to the law and the principles and values defined by the Organization.

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

5. Processing of investigation files

5.1 General issues

The Investigation File regulated in this section will only be processed if there is no specific procedure or protocol in the Organization to instruct the file based on the content of the information (e.g., protocols in the labor field for the prevention and treatment of complaints of moral, sexual, and/or gender-based harassment, sexual orientation, and gender identity).

An Investigation File is understood as the set of actions carried out to verify and clarify the facts reported in the communications that the head of the IIS becomes aware of.

The head of the IIS will document the various phases of the investigation and keep all documentation generated during the processing, adopting the necessary measures to ensure the confidentiality of the Investigation File and complying with personal data protection regulations.

This is understood without prejudice to the custody tasks that may be entrusted to those teams or individuals who may support the Investigator of the Investigation File.

Notifications that must be sent to the informant, as well as to members of the Organization and other third parties related to the Investigation File, will be sent from an email address or, if applicable, from a specific platform that allows communication with these individuals and obtaining their responses in a reserved and confidential manner, so that only the head of the IIS or the Investigator of the Investigation File have access to the content of these communications, complying with personal data protection regulations.

5.2 Receipt, acknowledgement of receipt and acceptance/rejection for processing

5.2.1 Receipt

The head of the IIS will initiate an Investigation File when they become aware of facts or circumstances that may constitute a breach, either ex officio or by virtue of a communication or information received through the channels enabled for this purpose, or by any other means.

The most common ways of becoming aware of potential breaches are as follows:

- Communications received through the channels enabled for this purpose.
- News reports.
- Judicial/Fiscal/Police requests.

COSENTINO*	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

- Findings within the framework of an internal control procedure.

If any member of the Organization, other than the head of the IIS, receives a communication or information related to a potential breach, they must immediately forward it to the head of the IIS, preserving the confidentiality of the communication and, if applicable, the identity of the informant. The head of the IIS will enter this communication or information into the appropriate internal channel and proceed in accordance with this Procedure.

The head of the IIS will ensure that the obligation to forward such communications is communicated, as well as the consequences of non-compliance, which may result in disciplinary measures.

All information and communications that the head of the IIS becomes aware of will be identified with a registration number.

5.2.2 Acknowledgement of receipt

If the Investigation File is initiated due to the receipt of a communication, the head of the IIS will send an acknowledgment of receipt to the informant within **seven calendar days** from the receipt of the communication, provided the informant has not waived receiving notifications or their anonymity is not at risk (if applicable), unless doing so could jeopardize the confidentiality of the communication.

5.2.3 Acceptance/rejection for processing

Once the communication has been received and registered, and the absence of a conflict of interest has been confirmed, the head of the IIS must decide on its admission or rejection. To do this, they will verify whether the information pertains to facts that potentially constitute a breach as defined in this Procedure.

If necessary to decide on the admission or rejection of the communication, the head of the IIS may request additional information from the informant regarding the facts subject to the received communication, provided the informant has not waived receiving notifications or their anonymity is not at risk (if applicable).

In any case, the rejection of a communication must be based on at least one of the following reasons:

- The reported facts lack any credibility.
- The reported facts do not constitute a breach as defined in this Procedure.
- The communication is manifestly unfounded, or, in the judgment of the head of the IIS, there are rational indications that the information contained in the communication was obtained through the commission of a crime.

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

- The communication does not contain new and significant information about a breach compared to a previous communication for which the corresponding procedures have concluded, unless there are new factual or legal circumstances that justify a different follow-up.

If the information is admitted for processing, the head of the IIS will verify whether there is a specific procedure or protocol for instructing the Investigation File. By legal imperative, there is a Protocol for the prevention and treatment of complaints of moral, sexual, and/or gender-based harassment, sexual orientation, and gender identity, which allows employees and external personnel to report any behaviour constituting harassment in accordance with the definitions contained in said protocol.

If, through the internal channel, complaints of behaviours allegedly constituting harassment in the workplace, sexual harassment, and/or harassment based on sex, sexual orientation, and gender identity are filed or channelled, they will be processed in accordance with the procedure contained in said protocol.

In any case, once the procedure in accordance with said protocol is completed, the result of that investigation will be forwarded to the head of the IIS for the adoption of any additional measures to those provided in the protocol, as necessary in accordance with this Procedure.

If the facts subject to the received 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 "*Special Protocol on Internal Investigations concerning Legal Entities*" of the Organization.

The decision on the admission or rejection of the received communication must be made within **ten business days** from the date of its registration and will be communicated to the informant within **five business days following** the adoption of the decision. In case of rejection, the reasons will be communicated to the informant. All of this provided the informant has not waived receiving notifications or their anonymity is not at risk (if applicable).

5.3 Investigation File Instruction

Once the communication is admitted for processing, the instruction of the Investigation File will begin, which will include all actions aimed at verifying the credibility of the facts subject to the information.

The maximum period for carrying out the investigation actions shall not exceed **three months** from the receipt of the communication or information, except in cases of special complexity that require an extension of the period, in which case it may be extended for a maximum of **three additional months**. In any case, regarding possible labor infractions committed by workers, the statute of limitations provided by law and/or conventionally will not begin until there is a complete and thorough understanding of

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

what happened, and the investigation actions carried out will interrupt any statute of limitations that may have begun.

All phases of the Investigation File must be documented, under the direction and supervision of the head of the IIS, in an adequate and sufficient manner to ensure its traceability and allow its accreditation before a potential third party.

5.3.1 Appointment of the Investigator

The head of the IIS will appoint the person responsible for processing the Investigation File and coordinating the investigation actions to be carried out (the “**Investigator**”), who may be himself, another member of the Organization, or an external professional to the Organization.

In any case, the following guidelines must be followed for the selection of the Investigator:

- If the communication or information affects any member of any governing body of the Organization, an external person to the Organization must be appointed as Investigator.
- If the communication or information affects the head of the IIS, he cannot participate in the Investigation File and must inform the Audit and Control Delegate Commission, which will appoint another person from the Organization or an external person as Investigator.
- If the person affected by the communication or information is a member of the works council, staff delegate, or delegate of any union section, the specific formalities that apply to this condition must be taken into account, for which the Human Resources Manager of the Organization must be informed.

In the event that an internal Investigator, different from the head of the IIS, is appointed, the head of the IIS will notify them of this appointment.

If an external Investigator is appointed, the corresponding service provision contract will be formalized, including the data processing agreement as required by personal data protection regulations.

The Investigator must ensure confidentiality and impartiality in the performance of their duties, which include, but are not limited to, the following:

- Collection of background information and relationship with the Organization of the persons involved in the received information.
- Notification to the affected persons of the existence of the Investigation File.

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

- Decision on the necessary investigation actions to clarify the facts, according to a planned schedule.
- Determination, if applicable, of the areas of activity of the Organization that should be involved in the Investigation File.
- Identification of persons who can provide information about the facts and additional information.
- Determination of documentation requirements to be sent to any third party.
- Opening, if applicable, of new lines of investigation based on the evidence obtained.
- Evaluation of relevant evidence obtained in the investigation.

The Investigator may request the collaboration of external advisors or personnel belonging to internal bodies or departments of the Organization. In the latter case, any conflicts of interest must be ruled out beforehand.

5.3.2 Development of the Instruction

During the instruction, the necessary actions will be carried out for the investigation and clarification of the facts contained in the communication or information admitted for processing.

Respect for the presumption of innocence and the honour of the affected person, as well as the protection of their personal data, will be guaranteed at all times. The affected person will be informed of the initiation of the instruction and, succinctly, of the facts attributed to them, as well as their right to be heard at any time in the manner and time deemed appropriate to ensure the successful outcome of the investigation.

If such information could favour the concealment, destruction, or alteration of evidence by the affected person, it may be postponed until the time of their interview, with the reasons for such a decision being recorded in the Investigation File. Under no circumstances will the affected person be informed of the identity of the whistleblower nor given access to the communication.

Once the affected person has been informed about the existence of the Investigation File, they may request to examine the information and documentation contained therein, although necessary measures must be taken to ensure that no information revealing the identity of the whistleblower is disclosed.

If the presence of the affected person in the Organization during the instruction period could compromise the successful outcome of the Investigation File, the Investigator may propose, in accordance with labor and data protection regulations, to limit their access

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

to the premises, documentation/information, and IT systems of the Organization, as well as suspend their employment but not their salary, to ensure the necessary investigation activities are carried out without interference.

If necessary for the successful outcome of the Investigation File, the Investigator may request additional data from the whistleblower regarding the facts subject to the communication, provided the whistleblower has not waived receiving notifications or their anonymity is not at risk (if applicable).

Furthermore, if other facts that could constitute new breaches are detected as a result of the investigation actions, the head of the IIS, previously informed by the Investigator, will decide to open a new Investigation File or, if related to the ongoing Investigation File, to expand it.

If, as a result of the investigation actions carried out during the instruction of the Investigation File, indications of a possible crime are identified, the Public Prosecutor's Office or the European Public Prosecutor's Office, as appropriate, must be informed, always applying the provisions of the Organization's *"Special Protocol on Internal Investigations concerning Legal Entities"*.

5.3.2.1 Collection and/or extraction of information and documentation in any format

During the development of the instruction of the Investigation File, all information and documentation that could contribute to the clarification of the investigated facts will be collected.

If necessary, the Investigator will coordinate the e-discovery work to be carried out on the computer equipment and devices that may contain relevant information for the investigation, selecting the keywords that allow the extraction of such information. Access to computer devices will be carried out in legally established terms and in accordance with the current regulations on the use of IT resources in the Organization.

The documentation and information collected will become part of the Investigation File and may be used to defend the interests and rights of the Organization.

The Investigator may rely, respecting personal data protection regulations, on a forensic investigation team to carry out the necessary technical tasks, which may be internal or external:

- Internal forensic team: the collaboration of internal professionals or departments with the technical capacity for the collection and processing of information and documentation necessary for the development of the Investigation File will be requested. The existence of a conflict of interest must be ruled out beforehand.

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

- External forensic team: an external firm specialized in forensic work will be hired for the collection and processing of information and documentation necessary for the development of the Investigation File.

If the intervention of these forensic teams is necessary, they will primarily carry out the following tasks:

- *E-discovery*: consisting of the acquisition, processing, and indexing of information stored on computer devices included in the investigation perimeter.
- *Forensic accounting*: aimed at analysing corporate economic-financial documentation.
- *Corporate intelligence*: analysis of the corporate and asset structure and the personal, financial, and asset links that the affected persons may have.
- *Data tracking*: analysis of information flows to identify possible illicit acquisitions or uses of information.

Additionally, in carrying out these tasks, the forensic team will be responsible for safeguarding all documentation and information, in any format, acquired and generated during the development of the Investigation File. They will establish the necessary technical guarantees to ensure confidentiality and the chain of custody.

5.3.2.2 Interviews

In the development of the Investigation File, the Investigator may conduct as many interviews as deemed necessary to verify and clarify the facts.

The interviews will be announced with sufficient notice and will be conducted by the Investigator in the presence of at least one other person, always respecting the interviewee's rights to privacy, honour, defence, and presumption of innocence. Additionally, the following considerations will be taken into account depending on who is being interviewed:

- Affected person: The interview will begin by informing the affected person of their rights, specifically: to be informed of the reported facts and to provide documents or evidence they deem pertinent for their defence, which will be included in the Investigation File. The affected person will be informed of all matters related to the processing of personal data in compliance with applicable regulations, unless they already have this information. They will be invited to present their version of the facts and may refuse to answer all or some of the questions posed or choose to answer only the questions they consider appropriate.
- Person other than the affected: The interview will begin by informing the interviewee of the duty to maintain absolute confidentiality regarding the ongoing

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

Investigation File and their participation in it. They will be informed of all matters related to the processing of personal data in compliance with applicable regulations, unless they already have this information. Additionally, they will be informed of their duty to cooperate in the investigation, answering questions truthfully and providing any data at their disposal that is requested during the investigation.

In any case, the development of the interviews will be carried out in a context that fully respects the rights of the interviewees.

A written record of the interview will be made, capturing its content. The record will be read to the interviewee for their agreement with the content. In case of discrepancies, these will be analysed, and if necessary, the required modifications will be made to the record, or the discrepancies will be noted. The record will be signed at the end of the interview by both the Investigator and the interviewee. If the interviewee does not wish to sign the record, this circumstance will be noted.

Additionally, if the interviewee authorizes it, instead of a written record, the interview may be recorded and included in the Investigation File. In this case, an equally effective alternative procedure will be offered, and the data protection information, if not previously provided, will include the processing of image and/or voice data.

In the event that the affected person or any members of the Organization, duly summoned to appear within the framework of the Investigation File, do not acknowledge receipt of the communications sent or do not confirm their participation in the investigation as requested, the Investigator will obtain this confirmation by telephone or even through personal contact—always ensuring the confidentiality of the communication—and will document the result of the management carried out.

If, after that communication, the summoned person still does not appear for the procedure for which they are cited, the Investigation File will continue its course.

In the case of third parties who do not have a contractual relationship with the Organization and do not appear after the first written communication, it will be understood that they decline to participate in the open investigation. Consequently, no additional communication will be sent.

5.3.3 Resolution of the Investigation File

Once all investigation actions have been completed, the Investigator will issue a report containing at least the following information:

- Identification code assigned to the communication or information that gave rise to the Investigation File.

COSENTINO*	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

- Chronological description of the main milestones in the processing of the Investigation File.
- List of investigation actions carried out to verify the credibility of the facts reported, as well as the documentation provided.
- Assessment of the results of the investigation actions carried out and the conclusions reached.
- Proposed resolution.
- Recommendations or improvement proposals to be considered in the Organization's CCM.

When the Investigator is a person other than the head of the IIS, they will submit the report along with the Investigation File to the head of the IIS, who, based on the conclusions reached in the report, will adopt one of the following resolutions:

- Favourable result: This will be adopted in cases where it is understood that no breach has been proven, which will determine the conclusion of the Investigation File without the need to take any measures. The resolution must be notified to the affected person.
- Unfavourable result: This will be adopted when it is determined that a breach attributable to the affected person has been proven.

In this case, and when labor regulations apply, the appropriate measures will be taken in accordance with the applicable disciplinary regime, specifically with what is stipulated in the Collective Agreement applicable to the corresponding relationship and the Workers' Statute.

If the affected person's relationship with the Organization does not allow the application of labor regulations in disciplinary matters, the corresponding legal or statutory regime will be followed.

If the breach consists of conduct contrary to the CCM and the measures that are part of them, the specific sanctioning regime provided, if applicable, in the corresponding model will be applied.

The result of the Investigation File will be communicated to the whistleblower, provided they have not waived receiving notifications, or their anonymity is not at risk (if applicable), as well as the confidentiality of the received information. The express prohibition of adopting any type of retaliation, including threats and attempts at retaliation, against whistleblowers and their surroundings is reiterated.

The express prohibition of adopting any type of retaliation, including threats and attempts at retaliation, against whistleblowers and their surroundings is reiterated.

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

6. Record

The head of the IIS will also maintain a logbook of the information and communications received and the Investigation Files they have given rise to, ensuring the confidentiality of such information.

The logbook will contain the following information for each communication or information received:

- Date of receipt
- Registration number
- Internal investigation processing: yes / no
- Closing date

For the preservation of the information collected in the logbook, the provisions of the personal data protection regulations and Law 2/2023 will be followed. In particular, personal data that, if applicable, are included in the logbook may only be retained for the period necessary to demonstrate compliance with the Whistleblower Protection Act.

7. 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 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/ethical-channel/>

8. Personal data protection

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

9. Preparation of Periodic Reports for the Organization's CCM

COSENTINO	INTERNAL INFORMATION SYSTEM	Version 3
	PROCEDURE FOR THE MANAGEMENT OF INFORMATION RECEIVED IN THE INTERNAL INFORMATION SYSTEM	Edition: 22nd January 2025

The head of the IIS will prepare specific annual reports that will be part of the action plans of the Organization's CCM, which will include information related to the communications received in the Organization's IIS concerning any conduct contrary to each CCM and the measures that are part of it, indicating the processing stage they are in.

If the Investigation File concludes with an unfavourable resolution, the report will include: i) the specific breaches that have been verified, ii) the area(s) of activity affected by the breaches; and iii) the improvement actions that, according to the head of the IIS, could be carried out as reaction measures in the process of updating and continuously improving the corresponding CCM.

10. Entry into force

This Procedure shall enter into force on 1st March 2025.