# ZENNIO GROUP INTERNAL INFORMATION SYSTEM POLICY



| Version 2 | Prepared by: | Reviewed by: | Approved by: |
|---|---|---|---|
| **Area** | Legal | Compliance Committee | Sole Administrator |
| **Date** | October 2025 | October 2025 | October 2025 |

# TABLE OF CONTENTS

# 1. VERSIONS

| Version | Reason for Change | Page(s) | Date |
|---|---|---|---|
| 1 | Creation of the Ethical Channel Policy. | All | 01/03/2024 |
| 2 | Update to the Internal Information System Policy, in accordance with Law 2/2023 of 20 February, regulating the protection of persons who report regulatory violations and the fight against corruption. | All | 01/10/2025 |

# 2. REGULATORY FRAMEWORK

- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law ("DPI").
- Law 2/2023 of 20 February regulating the protection of persons who report regulatory violations and fight corruption ("LPI").
- Royal Decree 1101/2024 of 29 October approving the Statute of the Independent Whistleblower Protection Authority, A.A.I.
- Any other related regulations, such as:
    - Organic Law 10/1995, of 23 November, on the Criminal Code ("CP").
    - Law 10/2010, of 28 April, on the Prevention of Money Laundering and Terrorist Financing ("LPBCFT").
    - Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights ("LOPDGDD").

# 3. SCOPE AND OBJECTIVES

The Internal Information System ("SII") is managed by Zennio Avance y Tecnología, S.L. for itself and its subsidiaries (**"Zennio** Group" or "Zennio"), ensuring that all communications received, including those from outside the European Union, maintain a level of protection for whistleblowers equivalent to that provided by the LPI, DPI and the regulations that extend or replace them.

The purpose of this Policy is to regulate the operation of the Zennio Group's Internal Information System, allowing employees and related third parties to report, in good faith, any violations of **(i)** European Union law; **(ii)** local criminal or administrative legislation; and **(iii)** Zennio's Internal Policies and Procedures; committed by employees and/or collaborators of the Zennio Group. All this has a dual purpose:

- **Preventive:** To discourage irregular behaviour by providing a mechanism for any member of the organisation or related third party to report possible violations, thereby promoting ethical conduct and regulatory compliance.
- **Reactive:** To facilitate the confidential reporting of possible violations, allowing for the timely detection and addressing of any situation that may entail criminal or administrative liability for Zennio, as well as ensuring that corrective actions are taken.

All communications must be handled in accordance with the principles of confidentiality, independence and non-retaliation.

# 4. ROLES AND RESPONSIBILITIES

## 4.1 Zennio Employees and Related Third Parties

- Reporting irregular conduct: All Zennio employees and related third parties, i.e. collaborators, suppliers, subcontractors and customers, are obliged to report, in good faith and as accurately as possible, any irregular conduct committed by Zennio employees or collaborators. False or malicious reports may result in disciplinary or legal action.

## 4.2 Administrative Body

- Appointment and dismissal of the SII Manager: The Administrative Body shall appoint a natural person to act as the SII Manager and, specifically, to be responsible for managing the **Ethics Channel** and investigating each report received ("**SII Manager**").
- Regulatory framework: The Administrative Body shall approve this Internal Information System Policy and its related rules.
- Autonomy and resources: The Administrative Body shall ensure that the Head of the IIS can perform their duties autonomously, independently and with sufficient resources.
- Annual evaluation**:** The Administrative Body shall evaluate the effectiveness of the SII, compliance with deadlines and confidentiality guarantees on an annual basis, by reviewing the investigation reports and by any other means of evaluation it deems appropriate, adopting improvement measures if any irregularities are detected.
- Deputy Head: If the Head of the SII is the subject of the communication or must abstain due to a conflict of interest, the deputy head shall act in the order indicated in section 4.7.

## 4.3 SII Manager

- SII Management**:** The SII Manager is the individual responsible for managing communications received through the Internal Information Channels and ensuring the confidentiality and protection of the whistleblower.
- Instruction and delegation: The SII Manager may instruct each investigation himself or delegate it to persons from other more specialised areas or even to external service providers under his supervision and subject to strict confidentiality.
- Report and notification**:** The SII Manager must prepare a detailed report on each communication received and submit their conclusions to the Management Body for decision-making. They will also inform the Compliance Committee, providing as little personal data as possible, unless strictly necessary, so that this body can implement improvement measures within the organisation.
- Confidentiality: The SII Manager shall treat communications and their investigation with the strictest confidentiality, ensuring that third parties involved in the investigation maintain an equivalent level of confidentiality.
- Protection: The SII Manager shall not take any reprisals against whistleblowers and shall promote the necessary measures for their protection when necessary.
- Abstention: The SII Manager shall refrain from participating in the investigation in the event of a conflict of interest with the reported facts. In such cases, the alternate managers shall participate in the order indicated in section 4.7.

## 4.4 Delegated Investigator

- Delegated investigation: The Delegated Investigator shall be in charge of investigating those reports that the Head of the SII delegates to them at any given time, and shall be subject to the same obligations as the Head of the SII in terms of confidentiality, non-retaliation and abstention in the event of a conflict of interest.

### 4.5 Compliance Committee and Legal Department

- Support: The Compliance Committee and the Legal Department may be informed by the SII Manager of all or some of the communications received and shall support the SII Manager in conducting investigations, if requested. They shall also be responsible for implementing corrective measures within the organisation.
- Deputy Investigators: They may also take on the investigation of cases in which the Head of the SII has a conflict of interest.
- Deputy SII Manager: If the SII Manager is the subject of the communication or must abstain due to a conflict of interest, the deputy managers will act in the order indicated in section 4.7.
- Confidentiality, Non-Retaliation and Abstention**:** The Compliance Committee and the Legal Department are subject to the same obligations as the SII Manager in terms of confidentiality, non-retaliation and abstention in the event of a conflict of interest.

### 4.6 External provider of the Ethics Channel

- Receipt of communications: The external provider shall be responsible for the technical management of the **Ethics Channel** on behalf of the SII Manager, supervising on a daily basis whether any communications have been received by the **Ethics Channel**, although it shall have no decision-making power over investigations and may only advise and, in the case of section 4.7, instruct the investigation.
- Forwarding of communications: After reviewing the content of the communication, the external provider will forward its entire content to the SII Manager. If the SII Manager is the subject of the communication or must abstain due to a conflict of interest, they will forward the communication to the alternate managers in the order indicated in section 4.7.
- Support in the investigation: The external provider shall provide the SII Manager with support in order to properly document the communications received, shall monitor deadlines and shall support the SII Manager in conducting investigations if requested to do so.
- Confidentiality, non-retaliation and abstention**:** The External Provider shall be subject to the same obligations as the SII Manager in terms of confidentiality, non-retaliation and abstention in the event of a conflict of interest and, in addition, shall sign the corresponding personal data processing agreement.

### 4.7 Conflicts of interest and substitutions

In the event that the SII Manager is the subject of the communication or must abstain due to a conflict of interest, the Compliance Committee, the Legal Department and even the Administrative Body may act as substitute managers in the following order, provided that they are not affected by any conflict of interest: **(1)** Compliance Committee; **(2)** Legal Department; and **(3)** Administrative Body; which in turn must delegate the investigation to one of their members.

In the exceptional case that all substitute responsible parties are subject to the communication or have a conflict of interest, the external provider will take charge of the investigation.

# 5. COMMUNICATIONS MANAGEMENT

## 5.1 Submission of Communications

### 5.1.1 Who can report and what types of conduct should be reported.

- Obligation to report breaches: Any employee, collaborator or partner of the Zennio Group, or any third party that has a business relationship with Zennio, who becomes aware of a breach committed by employees, collaborators or partners of Zennio in a work or professional context, must report it immediately through the SII. If the whistleblower is the perpetrator of the misconduct (self-reporting), the report may be considered an internal mitigating factor, without implying automatic exemption from liability.

- Conduct that can be reported through the SII:

    - **Breaches of EU law**: *Conduct that violates European regulations on public procurement, services and financial markets, money laundering and FT, product and transport safety, the environment, public health, consumer protection, personal data, the financial interests of the EU or the internal market (Art. 2 DPI).*

    - **Breaches of local legislation**: *Conduct constituting criminal offences or serious or very serious administrative offences (Art. 2 LPI).*

    - **Breach of Zennio's internal regulations**: *Conduct that violates the Code of Ethics and/or internal policies and/or protocols in force at any given time.*

- Conduct that cannot be reported through the SII: The following acts are not considered reportable through the SII:

    - **Interpersonal or human resources conflicts:** Minor interpersonal conflicts (such as friction, misunderstandings or coexistence problems that can be resolved through internal organisation), as well as ordinary administrative issues relating to the employment relationship (salary, shifts, conditions, variables, etc.), that are not serious enough to constitute a serious or very serious administrative offence or a criminal offence (workplace harassment, sexual harassment, etc.) should be dealt with directly by the HR Department.

    - **Commercial complaints**.

    - **Public information that does not contain new information or is repetitive**.

    - **False or unsubstantiated information.**

### 5.1.2 Content of the communication

The communication must include a clear and detailed description of the facts, as well as all available documentation to clarify or support the information provided, specifically:

- Details of the informant, unless they have opted for anonymous communication.
- Description of the events that occurred.
- Date of the events.
- First and last names of the persons mentioned.

- Any evidence available to you that can prove the reality of the events and/or conduct that are the subject of the report.

#### 5.1.3 Available communication channels

Internal communication channels

- **Ethics Channel (*preferred method*):** Zennio provides whistleblowers with its **"Ethics Channel**", a website that allows them to submit written reports using a simple form designed to ensure confidentiality if the whistleblower so wishes. However, anonymous reports may hinder the investigation if no alternative secure means of contact is provided, such as a temporary email address. The Ethics Channel can be accessed via the Zennio website in the "Ethics Channel" section at the bottom of the page, or directly via the following link: https://centinela-canal.lefebvre.es/canal-denuncias/zennio.

- **Verbally:** Communications may also be made verbally, by telephone or through a face-to-face meeting within a maximum period of seven days, at the request of the informant. Verbal communications, whether in person or by telephone, will be documented in one of the following ways: **a)** by recording the conversation, or **b)** through a complete and accurate transcript of the conversation made by the staff responsible for handling it. The whistleblower will be given the opportunity to check, rectify and accept the transcript of the conversation by signing it. The use of this means of contact is authorised by the LPI, but the nature of the verbal channel makes it impossible to guarantee anonymity. If you wish to use this method, the call or meeting must be arranged by sending an email to responsablesii@zennio.com.

External Communication Channels

In addition to the Internal Channels, communications may also be made directly through the following channels, although it is advisable to use the Internal Channels first:

- **Independent Whistleblower Protection Authority (AINPI) channel**: it is possible to contact the AINPI directly through its official channel (https://whistleblowersoftware.com/secure/canal_externo_de_denuncias_AINPI). It will also be possible to contact the regional authority, should it be established in the future, as well as those of the European Union institutions.

- **Other authorities**: Directly to the security forces, the public prosecutor's office, labour, social security and environmental authorities, etc.

### 5.2 Protection Measures

#### 5.2.1 Protection of Whistleblowers

Any person who, in good faith, communicates or reports potentially irregular conduct shall be protected against disciplinary measures or reprisals. This protection extends to persons connected with the whistleblower or those who assist them during the process.

However, for this protection to apply, the information provided must be based on good faith, as the law does not protect those who provide false, misrepresented or illegally obtained information.

The following is a summary of the **main protective measures** recognised by law for persons who report irregularities or breaches in good faith:

- **No penalties for reporting:** anyone who reports or makes public an infringement may **not** be punished or held liable for doing so, provided that they acted in good faith and had reasonable grounds to believe that it was necessary to do so.

- **Legitimate access to information:** whistleblowers shall not be penalised for obtaining or accessing the information they report, provided that they do not commit a crime to obtain it.

- **Limits of protection:** legal protection only covers acts necessary to report or disclose the violation. If the whistleblower takes actions that are not directly related to that report or that exceed what is reasonably necessary (such as tampering with evidence, disseminating private information or committing a crime), those actions will not be protected and may give rise to liability.

- **Presumption of retaliation:** if someone suffers harm after filing a complaint, the law presumes that it was retaliation, unless the company proves otherwise.

- **Defence in court:** in the event of lawsuits (e.g. for defamation, breach of confidentiality or labour disputes), whistleblowers may claim protected whistleblower status and will not be held liable if they acted in good faith and within the framework of this policy.

#### 5.2.2 Protection of persons subject to the report

During the processing of the case, the persons affected by the report shall have the right to the presumption of innocence, the right of defence and the right of access to the case file under the terms regulated in this law, as well as the same protection established for whistleblowers, preserving their identity and guaranteeing the confidentiality of the facts and data of the proceedings.

#### 5.2.3 Confidentiality

Zennio undertakes to ensure that the identity of the person making the communication through the SII's Internal Channels is not disclosed, unless they give their express consent or it is required by the competent authorities in the context of an external investigation. In this regard, except for persons specifically authorised to receive, follow up on or resolve the communications received, no one may know the identity of the communicator or any other information that may be deduced about their identity.

In the event that the identity of the informant is to be disclosed, Zennio will notify them in advance, unless this could compromise the investigation.

The SII Manager shall report to the Management Body on the conclusions of each investigation and may also report to the Compliance Committee, Legal Department and HR Department, providing pseudo-anonymised documents, unless it is essential to know the identity of the persons mentioned for the purposes of taking disciplinary or legal action or implementing improvement measures.

The staff of the External Provider, the SII Manager and their collaborators (Compliance Committee, Legal Department, etc.) are subject to a duty of confidentiality, as reflected in their contracts, and technical and organisational measures have also been implemented to strengthen this confidentiality.

Zennio cannot guarantee the confidentiality of data and facts communicated through channels other than those established, especially if it is through members of the organisation who are not responsible for this matter. However, Zennio undertakes to adequately train its staff on this matter to minimise these situations and promote the use of official channels that best guarantee confidentiality and traceability.

Finally, Zennio undertakes to pursue any breach of the duty of confidentiality by adopting disciplinary sanctions and/or legal action.

### 5.2.4 Technical measures

#### 5.2.4.1 Ethics Channel platform, receipt and safekeeping of communications

The Zennio Group's Ethics Channel is an encrypted IT tool (HTTPS), based on GlobalSuite, located on servers within the European Economic Area and managed by an external provider, which stores and records communications without Zennio accessing the platform at any time.

#### 5.2.4.2 Verification of conflicts of interest in Ethics Channel communications

Upon receiving a communication through the Ethics Channel, the external provider conducts an initial review to verify that the SII Manager can handle the case, as they are not the subject of the communication and do not have a conflict of interest a priori.

- If no conflict is detected, the file is forwarded to the SII Manager.
- If a conflict is detected, the substitution order set out in section 4.7 (***Compliance Committee → Legal Department → Management Body***) is applied, also verifying that the substitutes are not the subject of the communication and do not have a conflict of interest a priori.

Due to this initial filtering of potential conflicts of interest, the preferred Internal Channel is the Ethics Channel and not direct verbal communication with organisation personnel.

#### 5.2.4.3 Secure data storage and deletion

The files generated in the investigations of communications received through any of the internal channels will be kept blocked for a maximum period of ten years, except in the case of ongoing judicial or administrative proceedings. Once this period has expired, the data will be deleted from both the Channel and Zennio's systems.

#### 5.2.4.4 Supplier training and internal controls

The external supplier guarantees that all its personnel with access to the platform are trained in information security, data protection and confidentiality, and that only strictly necessary personnel may intervene in the management of communications received.

## 5.3 Communications Management

| ACTIVITIES | | | |
|---|---|---|---|
| PHASE | ACTION | DESCRIPTION | RESPONSIBLE |
| 1 | **Receipt of communication** | 1. Information/communications may be received in writing through the **Ethics Channel**.<br><br>2. The whistleblower will be provided with a copy of this Policy by including it on the **Ethics Channel's** IT platform.<br><br>3. If the communication is sent through channels other than the official one or through staff members not responsible for its management, the non-responsible staff members involved will be informed of their obligation to maintain due confidentiality, warning them of the recipient's obligation to immediately forward any additional information about the communication to the SII Manager under penalty of a very serious offence.<br><br>4. Once the communication has been received through the SII, it will be verified whether it is anonymous or identified and whether it indicates an address, telephone number or email address for receiving notifications.<br><br>5. If the informant is identified, their identity will be kept confidential in accordance with Article 33 of the Whistleblower Protection Act, without disclosing it to third parties.<br><br>6. The communication received on the IT platform will be forwarded by the External Provider to the SII Manager or, failing that or if this | SII manager |

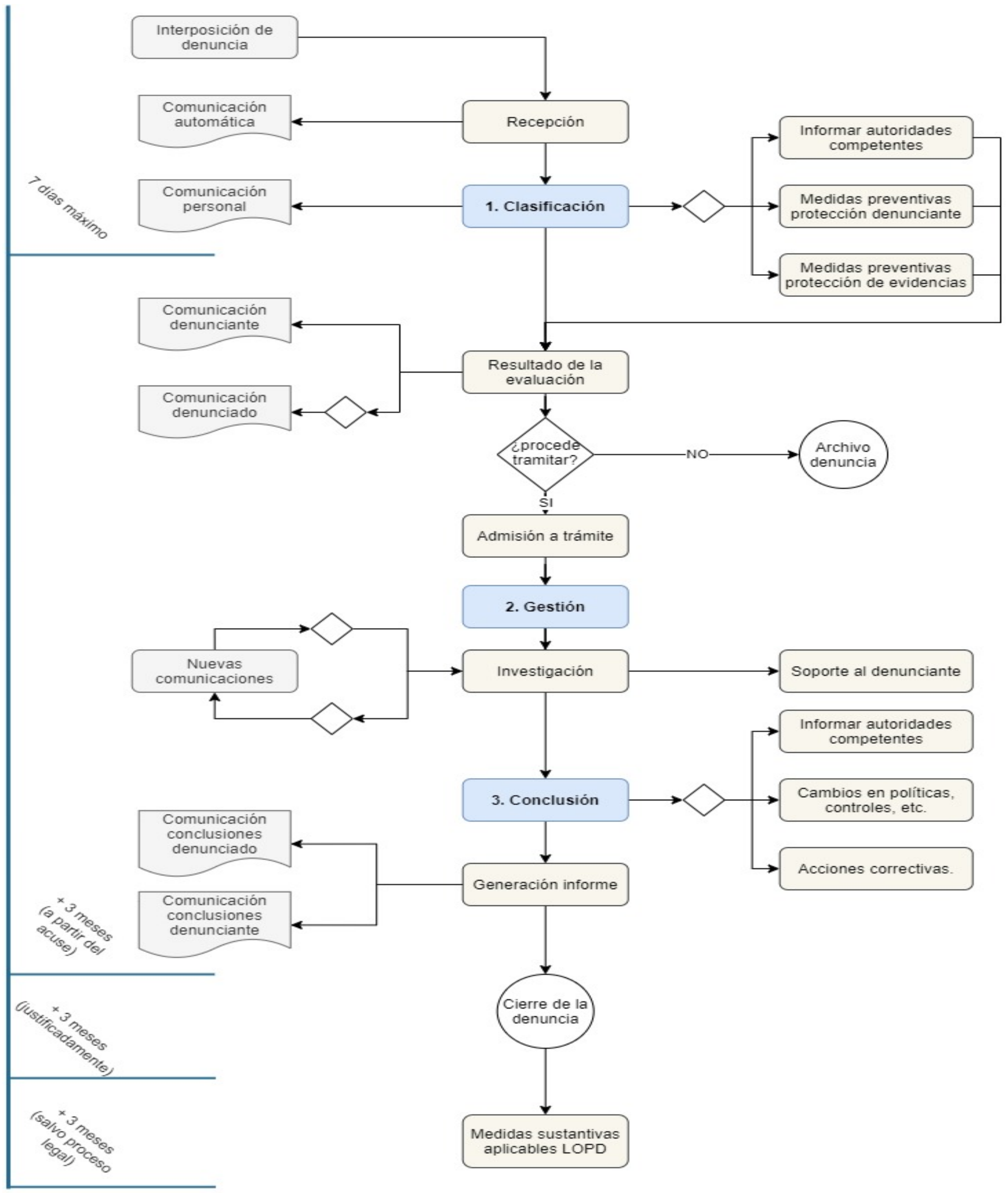
| | | | |
|---|---|---|---|
| | | is not possible, to the substitute manager who replaces them in accordance with section 4.7, i.e. **(1)** the Compliance Committee, **(2)** the Legal Department or **(3)** the Management Body. Only if it is impossible to contact any of the above three parties will the External Provider handle the communication.<br><br>7. If the option of verbal communication (in person, by telephone or by voice message) is enabled:<br>• It shall be noted that the communication will be recorded and a summary of the content of this Policy shall be provided, indicating where a copy can be found.<br>• The conversation will be documented by means of a recording in a secure, durable and accessible format, or by means of a complete and accurate transcript.<br>• Without prejudice to their data protection rights, the informant will be given the opportunity to check, rectify and accept the transcript of the message by signing it.<br>8. Whether or not the informant is identified, they will be advised to provide a means of maintaining communication or requesting additional information for the investigation.<br>9. It shall be recorded in the SII, assigning it a code.<br>10. Access to the SII is limited to:<br>• The internal person responsible for the system and, where applicable, the person who manages it directly and any external providers that may be appointed.<br>• Designated instructor<br>• HR manager in the area of disciplinary measures<br>• Head of legal services, if legal measures must be taken<br>• Data protection officer. | |
| 2 | **Acknowledgement of receipt** | 1. Within a **maximum of 7 working days** of receipt, the tool itself acknowledges receipt of the communication, if the informant identifies themselves. If it is anonymous and/or they have opted out of receiving communications, it does not. | External Supplier |
| 3 | **Admission or non-admission to proceedings** | 1. In all cases, the presumption of innocence, the right to be heard and the honour of the persons under investigation will be respected.<br><br>2. Once the information has been recorded, it will be checked to see if it exposes facts or conduct within the scope of application set out in this SII Policy.<br><br>3. Within a **maximum of 10 working days** from the date of registration, a decision will be made:<br>• **Whether to reject it** on the grounds of:<br>  ◦ Lack of credibility<br>  ◦ Facts that do not constitute an offence.<br>  ◦ Manifest lack of foundation or reasonable evidence that it was obtained through the commission of a crime. | Internal SII manager. |

<table>
<tr><td></td><td></td><td>
<ul><li>If it does not contain new and significant information about previously reported infringements for which the corresponding proceedings have been concluded, unless there are new factual or legal circumstances ( ) that justify a different course of action.</li></ul>
Rejection shall be notified with reasons, unless it is an anonymous report and/or the informant has waived the right to receive communications.
<ul><li><u>If admitted</u>. Admission shall be notified, unless the communication is anonymous and/or the informant has waived the right to receive communications, stating the reasons. Likewise, the communication shall be immediately forwarded to the Public Prosecutor's Office if the facts contain clear indications of a crime.</li></ul>
4. Throughout the process of admitting or rejecting the communication, any persons who may have a conflict of interest with the content of the communication shall be excluded.
</td><td></td></tr>
<tr><td>4</td><td>Investigation</td><td>
1. Once the complaint has been accepted for processing, the investigator will send the acceptance report to the External Provider, who will change the status of the communication to "Under Investigation".<br><br>
2. The investigator will categorise the report in coordination with the categorisation made by the whistleblower.<br><br>
3. The investigator may seek support from the Compliance Committee, the Legal Department and the Director of Human Resources, as well as from specialist staff on an exceptional basis, during the investigation.<br><br>
4. They shall take the necessary steps to verify the veracity of the facts.<br><br>
5. Ensure that the person affected by the information:
<ul>
<li>is informed of this and of the facts reported in a succinct manner; is informed of the actions or omissions attributed to them, and is heard at any time. Such communication shall take place at the time and in the manner deemed appropriate to ensure the successful completion of the investigation, if their contribution at the outset may facilitate the concealment, destruction or alteration of evidence.</li>
<li>be informed of the processing of their personal data.</li>
<li>be able to submit written statements. This information may be provided during the hearing</li>
<li>an interview, with respect for the presumption of innocence, inviting them to present their version of events and to provide any evidence they deem appropriate.</li>
<li>access to the file without revealing the identity of the informant, being able to be heard at any time, and appearing assisted by a solicitor.</li>
<li>Under no circumstances shall the identity of the informant be disclosed to the persons concerned, nor shall access to the communication be granted.</li>
</ul>
</td><td>SII Manager or Designated Instructor</td></tr>
</table>

| | | | |
|---|---|---|---|
| 5 | **Completion of proceedings and response to the informant** | 1. Maximum time limit for completing proceedings and responding to the informant: **3 months from the date the information is** recorded. Except in particularly complex cases that require an extension (up to a maximum of 3 additional months).<br><br>2. The above is subject to specific cases for which other deadlines are legally established (such as sexual harassment and gender-based harassment in the workplace).<br><br>3. Whatever the decision, it will be communicated to the whistleblower, unless they have waived this right or the communication is anonymous.<br><br>4. Once the investigation is complete, a report will be issued containing:<br>• The facts reported, the identification code of the report and the date of registration.<br>• The classification of the report for the purposes of determining whether or not it is a priority for processing<br>• The actions taken to verify the veracity of the facts and conclusions, the assessment of the proceedings and the evidence supporting them<br><br>5. The decision will include one of the following options:<br>• Closure of the file, notifying the informant and the person concerned. Such closure may be based on a finding of lack of plausibility or lack of evidence or non-compliance with the communication received.<br>• Or, if the facts of the communication are proven to be true, thereby evidencing a breach or violation of regulations, the adoption of the relevant measures in accordance with labour legislation and other applicable civil and commercial obligations shall be proposed.<br><br>6. The whistleblower shall be entitled to the protection of the law unless the investigation concludes that the information should have been rejected for the reasons set out in section 3.3 above.<br><br>7. Referral to the Public Prosecutor's Office if, despite initially finding no evidence of a crime, such evidence is found during the investigation.<br><br>8. Once the investigation has been completed and the relevant decision has been taken regarding the report received, the System Manager shall be responsible for sending the closing report to the External Provider, who shall change the status to "completed". | SII Manager/Designated Investigator |
| 6 | **Retention and destruction of personal data** | 1. Personal data that is not necessary for the knowledge and investigation of the reported facts will not be processed and, where appropriate, will be immediately deleted, as will personal data relating to conduct not covered by the scope of the law. If the report includes special categories of personal data, it will only be processed when strictly necessary to investigate the facts; otherwise, it will be deleted immediately.<br><br>2. If it is proven that the information provided, or part thereof, is not true, it will be deleted as soon as this circumstance becomes known, unless the lack of truthfulness may constitute a criminal offence, in which case the information will be kept for the time necessary for the legal proceedings to be processed. | SII Manager and External Provider |

| | | | |
|---|---|---|---|
| | | 3. The personal data of the complainant, as well as that of employees and third parties, will only be kept in the SII for the time necessary to decide whether to initiate an investigation into the reported facts.<br><br>4. Three months after the data is entered, it will be deleted from the reporting system, unless the purpose of retaining it is to leave evidence of the functioning of the SII, in which case it must be blocked. | |

**Flowchart**



## 5.4 Closure of the Communication

The SII Manager must complete the investigation of the communication within three months of receiving the communication or, if no acknowledgement of receipt was sent to the whistleblower, within three months of the expiry of the seven-day period after the communication was made, except in cases requiring an extension of the period for an additional three months.

Once the investigation has been completed, the SII Manager will issue the corresponding closing report indicating their conclusions and the measures agreed upon (informing the authorities, adopting disciplinary or legal measures and/or improvement actions) and will communicate this to the whistleblower and the persons under investigation, proceeding to close and archive the communication.

# 6. PERSONAL DATA PROTECTION

| | |
|---|---|
| **Data controller** | Zennio Avance y Tecnología, S.L., with registered office in Toledo (Spain), acting as the data controller for its own Internal Information System (SII) and that of the Zennio Group's subsidiaries. |
| **Data processor** | Independent external provider that manages the Ethical Channel platform, in accordance with the data processing agreement (Art. 28 GDPR). |
| **Data** | Identification and contact details of the whistleblower, if not anonymous; details of persons involved or mentioned in the report; and additional data provided in the investigation (documents, emails, etc.). |
| **Purpose** | To manage communications received through the SII: reception, verification of conflicts of interest, analysis, investigation, resolution and archiving. |
| **Legal basis** | Compliance with a legal obligation (Art. 6.1 c GDPR) and mission of public interest (Art. 6.1 e GDPR), in accordance with the LPI. |
| **Recipients** | Competent judicial or administrative authorities; internal managers appointed by Zennio (SII, Compliance Committee, Legal Department or Administrative Body); external provider of the Ethics Channel. |
| **International transfers** | Not envisaged. If necessary, standard contractual clauses or other mechanisms under Art. 44–49 GDPR will be applied. |
| **Retention period** | 3 months if no investigation is initiated. For the time necessary for the ongoing investigation and, subsequently, blocked for the time during which liability may be claimed, up to a maximum of ten years (Article 26 of Law 2/2023). |
| **Security measures** | Secure web platform (HTTPS), restricted access, enhanced contractual confidentiality measures, data blocking, password access, omission of names of individuals in reports, etc. |

| | |
|---|---|
| **Rights** | Access, rectification, erasure, restriction, objection and portability, by sending a request todpo@zennio.com . You may also lodge a complaint with the Spanish Data Protection Agency (www.aepd.es). |