INTERNAL INFORMATION SYSTEM POLICY + WHISTLEBLOWING CHANNEL

GRUPO FEDOLA

GF-JURIDICO

VERSION CONTROL

VERSION	DATE	RESPONSIBLE	COMMENTS
1.0	25/09/2019	Criminal Compliance	Definition and content of the Whistleblowing Channel Regulations in accordance with the Criminal Code
2.0	27/02/2023	Criminal Compliance	Adaptation to Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption
2.1	30/06/2023	Criminal Compliance	Review, update, and inclusion of annexes
2.2	15/01/2024	Criminal Compliance	Review and correction regarding data protection
2.3	08/03/2024	Criminal Compliance	Review and inclusion of the introduction and offences from Annex I of European Directive 2019/1937
2.4	18/11/2024	Criminal Compliance	Review and correction of errors

INDEX

1. - INTRODUCTION

This policy is approved in order to comply with **Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption**, which incorporates into Spanish law **Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019**.

This regulation governs, among other matters, the **Internal Information System** and the adequate protection against retaliation that natural persons who report any of the actions or omissions under European Union law, criminal law, labour regulations, etc., may suffer.

In this regard, since **2019**, Grupo Fedola had already implemented a reporting channel, called the **whistleblowing channel**, as a complement to its Code of Ethics, so that any employee would have a means of communication to report actions not in compliance with laws, regulations, or internal policies, potentially giving rise to criminal liability on the part of the company. This channel was already available on the website **www.grupofedola.com**. In compliance with **Article 7 of Law 2/2023**, this whistleblowing channel becomes part of the **Internal Information System**.

For all the above reasons, the Board of Directors of Grupo Fedola implements the **common internal information system** for the companies forming part of the Group (hereinafter, **IIS**). This system may be used as an alternative to other external channels if the reporting person so wishes, although the internal reporting channel is the preferred route for reporting any conduct that may be unlawful or irregular, within the objective scope of this policy.

2. - PURPOSE

The purpose of this policy is to determine the principles, rules, rights, and obligations of Grupo Fedola's internal information system.

In accordance with the provisions of **Article 11 of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption**, this internal information system is approved for the whole of Grupo Fedola. The companies that make up Grupo Fedola are the following:

GRUPO FEDOLA, S.L.
PREFABRICADOS TEIDE, S.L.
FERRETERIA HERMANOS LÓPEZ ARVELO, S.L.U.
FEDOLA, S.L.U.
BROKER FEDOLA CORREDURÍA DE SEGUROS, S.L.U.

PRICEMESA, S.L.U.
GF-TIC, S.L.U.

CAMULSE, S.L.U.
OFISABEL, S.L.U.
MASQUECARPAS, S.L.U.
GF HOTELES, comprising:
EXPLOTACIONES SANTONEL, S.L.
FELAHOTEL, S.L.
COSTA ADEJE GRAN HOTEL, S.L.
ISABEL FAMILY HOTEL, S.L.U.
NOELIA PLAYA, S.L.U.

3. - SCOPE

What conduct may be reported through the internal information system?

- **a)** Infringements of **European Union law**, provided they fall within the scope of the EU acts listed in the annex to **Directive 2019/1937 of the European Parliament and of the Council, of 23 October 2019**, and affect the financial interests of the EU or impact the internal market.
- **b)** Within the scope of the Spanish legal system, **criminal offences**, **serious and very serious administrative offences**, and **labour law infringements in the field of occupational health and safety**.

Reports received that fall outside the scope established in **Article 2 of Law 2/2023** and their senders shall remain outside the scope of protection granted by that law (**Art. 7.4**).

Who is entitled to report through the IIS?

- **a)** persons who are employees of Grupo Fedola;
- **b)** self-employed persons;
- **c)** shareholders, partners, and persons belonging to the management, administrative, or supervisory body of a company, including non-executive members;
- **d)** any person working for or under the supervision and direction of contractors, subcontractors, and suppliers.
- **e)** those whose employment or statutory relationship with Grupo Fedola has already ended, volunteers, interns, workers in training periods regardless of whether or not they receive remuneration, as well as those whose employment relationship has not yet begun, in cases where information on infringements was obtained during the selection process or pre-contractual negotiations.

4. -INTERNAL INFORMATION SYSTEM

The **IIS of Grupo Fedola** referred to in this policy is the preferred route for reporting the actions or omissions set out in section 3 above.

The IIS consists mainly of the communication channel enabled for receiving reports falling within the scope of application, the **RSII**, and the procedure to be followed for processing those reports, called **"ANNEX I.- Internal Information System Procedure."**

4.1. - Basic principles of the internal information system

The Board of Directors of Grupo Fedola establishes the principles and rules for implementing reporting channels and managing internal investigation processes, highlighting the following:

- **Accessibility:** It allows all persons referred to in section 3 of this policy to communicate information on the infringements provided for in that section, in writing or verbally, and they may do so anonymously.
- **Integration:** The internal reporting channel established at Grupo Fedola is integrated into the IIS.
- **Security, confidentiality, and compliance with data protection regulations:** The IIS is designed, established, and managed securely, in such a way as to guarantee the confidentiality of the identity of the reporting person and of any third party mentioned in the report, and of the actions taken in the management and processing thereof, as well as the rights to privacy, personal life, honour, defence, and the presumption of innocence of the persons involved in the investigation process initiated as a result of a report made through the IIS, and data protection, preventing access by unauthorised personnel.

The identity of the reporting person, if known, as well as that of the third parties mentioned in the report, may only be disclosed to the judicial authority, the Public Prosecutor's Office, or the competent Administrative Authority במסגרת a criminal, disciplinary, or sanctioning investigation, after prior notice to the reporting person or the affected third party, provided that such circumstance does not compromise the investigation or ongoing judicial proceedings.

- **Diligence, speed, and effectiveness:** The actions aimed at verifying and clarifying the facts contained in the reports received must be carried out with the utmost diligence, speed, and effectiveness possible, taking into account the complexity of the facts, with the aim that Grupo Fedola should be the first to become aware of the possible irregularity, and always in accordance with the provisions of the IIS management procedure.

- **Proportionality, objectivity, and respect for the safeguards of the parties involved:** the actions carried out within the IIS shall be conducted in accordance with criteria of proportionality and objectivity, with the utmost respect for the law in force, recognising the rights of all parties involved and observing the safeguards expressly provided for in the IIS management procedure for the persons involved. Any act constituting retaliation against reporting persons is expressly prohibited.

The person affected by the report has the right to be informed of the facts attributed to them and to be heard at any time. Once informed, they may request to examine the information and documentation contained in the file created as a result of the processing of the report, although the necessary measures must be adopted to ensure that no information is disclosed that may reveal the identity of the reporting person.

- **Good faith:** this is an essential requirement for the protection of the reporting person, who must act in good faith and with an honest belief that serious harmful facts have occurred or may occur. This principle is opposed to actions such as sending false or distorted information, as well as information obtained unlawfully.
- **Publicity:** the information necessary for reporting persons to use Grupo Fedola's internal channel is provided clearly and is easily accessible, being included in this policy, which may be consulted on the website of all the companies forming part of Grupo Fedola, and more specifically through the following address:
  https://grupofedola.com/inicio/canal-denuncias/

4.2. Internal reporting channel

The internal reporting channel, integrated into the IIS, allows infringements under **Article 2 of Law 2/2023** to be reported in writing (**postal mail or electronic means**) or verbally (**telephone, voice messaging, or face-to-face meeting**, the latter within a maximum period of **7 days** at the reporting person's request). Within the Internal Information System, it is integrated through the **Whistleblowing Channel**.

Verbal reports shall be documented by means of **exact transcriptions**, which the reporting person may review, rectify, and accept. The reporting person shall be informed about the processing of their personal data in accordance with **Regulation (EU) 2016/679** and the external channels available for reporting to competent authorities or European institutions.

It is possible to make **anonymous reports**. Internal channels may also be enabled to receive information outside the scope of **Article 2**, although in such cases the

protection of the law shall not apply. The reporting person may indicate a secure means of receiving notifications.

4.3. IIS procedure

The IIS procedure regulates the management and processing of reports received through the internal reporting channel integrated into Grupo Fedola's IIS. This procedure is attached as **Annex I** to this policy.

In the case of reports relating to acts presumably constituting **moral harassment, sexual harassment, harassment based on sex, cyberbullying, or harassment based on sexual orientation, gender identity and/or gender expression**, they shall be raised and processed in accordance with the protocol applicable in each company.

Where the facts reported may arguably constitute a criminal offence, they must be brought to the attention of the **Public Prosecutor's Office** or the **European Public Prosecutor's Office**, as appropriate.

4.4. External channels

Without prejudice to the preferred route of the aforementioned internal channel for reporting possible breaches covered by the whistleblower protection law, Grupo Fedola informs that reports may also be made to the **Independent Whistleblower Protection Authority (A.A.I.)**, or to the corresponding regional authorities or bodies, regarding any actions or omissions included within the scope of application, whether directly or following prior communication through the corresponding internal reporting channel.

5. - PERSON RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM (RSII)

In accordance with the provisions of **Article 5.1 of Law 2/2023, of 20 February**, the Board of Directors of Grupo Fedola is responsible for the implementation of the IIS and for the processing of personal data. The **RSII** designated by the Board of Directors is the person holding the position of **Head of the Legal Department of Grupo Fedola**, who shall perform their functions independently and autonomously with respect to the rest of the entity's bodies. In addition, they are entrusted with the diligent management of the internal information system and the proper handling of the reports received.

Both the appointment and dismissal of the RSII shall be notified to the **Independent Whistleblower Protection Authority** or, where appropriate, to the competent

authorities or bodies of the autonomous communities, within the scope of their respective powers.

The RSII shall diligently assume, in the absence of a conflict of interest, responsibility for resolving the procedures initiated as a result of the information received through the established internal channel, ensuring the adequacy of the procedure. In the event of a **conflict of interest, absence, or illness**, the functions shall be performed by the person holding the position of **Criminal Compliance**, who, in the exercise of that function, shall be subject to the same obligations and principles as the RSII.

6. - PROTECTION MEASURES AND SAFEGUARDS

6.1. Conditions for protection

Protection is granted to those who report infringements under **Article 2**, provided that:

- They have reasonable grounds to believe that the information is true, even if they do not provide conclusive evidence.
- The report complies with the legal requirements.

6.2. Exclusions from protection

Protection is not granted to those who report information:

- Rejected by the internal channels or inadmissible.
- Relating to personal conflicts between individuals.
- Already publicly available or based on rumours.
- Outside the scope of application of the law.

6.3. Extension of protection

- To legal representatives of employees in support functions for the reporting person.
- To natural persons related to the reporting person (**colleagues, family members, etc.**) who may suffer retaliation.
- To legal persons related to the reporting person in an employment context.
- **Cases of anonymity:** if an anonymous reporting person is later identified and meets the legal requirements, they shall also be protected.
- **Reports to the EU:** persons who report infringements to European Union institutions shall have the same protection rights as those using external channels.

6.4. Prohibition of retaliation

Retaliation consists of acts or omissions prohibited by law that result in unfavourable treatment, placing the affected person at a disadvantage in the employment or professional sphere because they are a reporting person or have made a public disclosure. These include:

1. Employment measures, such as dismissal, suspension, non-renewal or early termination of contracts, demotions, denial of promotion, changes to working conditions, or failure to convert temporary contracts into permanent ones, unless justified by reasons unrelated to the report.
2. Personal harm, such as financial or reputational damage, intimidation, harassment, or ostracism.
3. Negative evaluations or references regarding performance.
4. Disclosure of harmful information, such as inclusion on blacklists limiting access to employment.
5. Denial of rights, such as leave, permits, or training.
6. Discrimination or unfair treatment.

Affected persons may request protection within **two years** following the retaliatory act, with the possibility of extending this period exceptionally, upon justification.

6.5. Support measures

a) **Advice:** Free and independent information on procedures, resources, protection against retaliation, and the rights of the reporting person.
b) **Assistance:** Effective support from the competent authorities and certification of protection under the law.
c) **Legal assistance:** In criminal proceedings and cross-border civil proceedings in accordance with EU regulations.
d) **Financial and psychological support:** In exceptional cases, assessed by the Independent Whistleblower Protection Authority.
e) **Compatibility with the Legal Aid Law** for representation in judicial proceedings.

6.6. Protection measures

a) **Exemption from liability:** the reporting person shall not be considered to have breached disclosure restrictions if acting on reasonable grounds, except in cases of criminal liability. This also applies to labour representatives subject to confidentiality.
b) **Access to information:** there shall be no liability for acquiring or accessing reported information if this does not constitute a criminal offence.
c) **Presumption of retaliation:** in judicial proceedings, if the reporting person proves harm after reporting, it shall be presumed to be retaliation, and the burden of proof shall lie with the person who adopted the harmful measure.
d) **Protection in judicial proceedings:** reporting persons shall not be held liable for protected reports and may justify their action as necessary to reveal infringements.
e) **Rights of the affected persons:** guarantee of the presumption of innocence, defence, restricted access to the case file, confidentiality of identity, and confidentiality of the data in the proceedings.

These measures seek to ensure a safe and protected environment for reporting persons.

6.7. Protection measures for the person affected by a report

During the proceedings, the persons affected have the right to the **presumption of innocence, defence, access to the case file, confidentiality of their identity, and protection of the data and facts related to the case**, in the same way as reporting persons.

7. - INFORMATION RECORD BOOK

The **RSII** shall keep a **record book** of the reports received and the investigations carried out. This register shall preferably be kept on media that guarantee its integrity, confidentiality, and non-manipulation, and it is not public; only judges and courts may access it in the context of judicial proceedings. Accordingly, the RSII shall ensure the availability of the documentation in order to respond to requests from judicial authorities and public bodies or entities protected by the applicable regulations. Personal data related to reports and investigations shall only be kept for the necessary period, which in no case may exceed **ten years**.

Once the proceedings have concluded, the **RSII** shall issue a report to be recorded in the record book and containing at least:

1. A statement of the facts reported together with the identification code of the report and the date of registration
2. The classification of the report for the purpose of determining its priority in processing
3. The actions carried out in order to verify the truthfulness of the facts
4. The measures adopted, where appropriate
5. The conclusions reached and the assessment of the evidence supporting them
6. Closing date

8. - PERSONAL DATA PROTECTION

8.1. Legal framework for the processing of personal data

The processing of personal data within the framework of this law is governed by:

- **Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data**
- **Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights**
- **Organic Law 7/2021, of 26 May, on the protection of personal data processed for the purposes of preventing, detecting, investigating, and prosecuting criminal offences and enforcing criminal penalties**

8.2. Limits on processing

Only necessary data shall be collected; irrelevant or accidentally obtained data shall be deleted immediately. Special categories of personal data shall be erased without being recorded or processed.

8.3. Lawfulness of processing

The lawfulness of processing is based on the existence of an **internal information system (IIS)**. Public disclosures are also protected if specific GDPR conditions are met.

8.4. Information to data subjects

Data subjects must be informed about the processing of their data and the right to keep their identity confidential. The person mentioned in a report shall not be informed of the identity of the reporting person.

8.5. Preservation of data

Data shall be kept only for as long as necessary to decide whether to open an investigation. If no investigation is initiated within **3 months**, the data shall be deleted or anonymised.

8.6. Access to data in the IIS

Access shall be limited to the **RSII**, Human Resources, legal services, and data protection officers. The data may be shared with third parties if necessary for sanctioning or criminal proceedings.

8.7. Identity of the reporting person

Their identity shall be confidential and may only be disclosed to judicial, prosecutorial, or administrative authorities in criminal investigations. Before any disclosure, the affected person shall be informed, unless doing so would prejudice the investigation.

ANNEX I.- IIS MANAGEMENT PROCEDURE

1. - PROCEDURE FOR REPORTING IRREGULAR ACTIONS

1.1. Identification of an irregularity

The **Internal Information System (IIS)** allows any person connected to the company to report, anonymously or with identification, knowledge of unlawful acts, irregularities, or omissions. These reports shall be managed by the **Person Responsible for the IIS (RSII)**, who shall investigate and take measures to prevent similar future conduct.

Reports may concern breaches of legal obligations, internal protocols, the Code of Conduct, or facts of an unlawful or criminal nature.

The following are included within its scope: infringements of **European Union law**, the **Spanish Criminal Code**, or infringements affecting the financial interests of the EU; serious or very serious criminal or administrative infringements, such as those causing financial harm to the Public Treasury and Social Security; and labour law infringements in the field of occupational health and safety.

The IIS does not require technical legal knowledge of the facts reported, as the **RSII** shall be responsible for determining their legal or administrative nature.

1.2. Communication/Receipt of the report

The internal reporting channels shall be available **24 hours a day, 365 days a year**, guaranteeing the utmost confidentiality. They are set out below in order of preferred use, without prejudice to the will of the reporting person:

a) Corporate app **"Fedola Conecta"**, exclusive to employees of all the companies.
b) IT tool available in the **"whistleblowing channel"** section of the corporate website;
c) Email: **canaldedenuncias@grupofedola.com**.

In addition to the electronic means listed above, reports may also be made by the following means:

d) By **registered post with acknowledgement of receipt**, addressed to Grupo Fedola, **Calle Candelaria, Edificio Olympo, No. 28, 1st floor, Postcode 38002, Santa Cruz de Tenerife**, for the attention of the **RSII**.
e) By **telephone**, via the main offices of Grupo Fedola, number **922 151499**, dialling **extension number 4** corresponding to the **Legal Department** and the role of the **RSII**.
f) By **face-to-face meeting**, requested in advance through any of the means described above.

All internal channels guarantee the confidentiality of reports, but the **only channel that guarantees anonymity**, understood as the ability to report without being identified by any means, is the IT tool available on the website.

In the case of reports relating to facts presumably constituting **moral harassment, sexual harassment, harassment based on sex, cyberbullying, or harassment based on sexual orientation, gender identity and/or gender expression**, they shall be raised and processed in accordance with the applicable protocol in each company. Without prejudice to the foregoing, employees may also submit a harassment report directly through the internal reporting channel, as may any other reporting person referred to in section 3 of the IIS policy, in which case the **RSII** shall forward the report to the person responsible for handling harassment complaints according to the applicable protocol. The investigation procedure and the subsequent determination of whether or not a harassment situation exists shall be governed by the procedures established in each protocol of the Group companies.

The internal reporting channel shall be made known through Grupo Fedola's website and the **"Fedola Conecta"** corporate application.

However, at the request of the reporting person, it may also be submitted by means of a **face-to-face meeting within a maximum period of seven days** from the filing of the report.

Access to and/or use of the IIS implies full and unconditional acceptance of the operating rules contained in this policy; that is, the user/reporting person has read, understood, and consented to them.

Verbal reports, including those made through a face-to-face meeting or by telephone, shall be documented, with the prior consent of the reporting person, by means of a **complete and accurate transcript** of the conversation made by the personnel responsible for handling it.

Without prejudice to the rights corresponding to them under data protection regulations, the reporting person shall be offered the opportunity to review, rectify, and accept the transcript of the conversation by signing it.

1.3. Minimum reporting requirements

As far as possible, the report shall contain the following information:

1. Identifying data of the reporting person, unless they choose to make the report anonymously.
2. Contact details of the reporting person, in order to clarify any questions during the investigation and to keep the reporting person informed.
3. A description of the suspected event as specifically as possible, detailing:

   a. What the potentially irregular conduct consists of.
   b. The persons allegedly involved.
   c. Approximate dates of commission of the acts.
   d. The means by which the possible unlawful conduct was carried out.
   e. The area of the organisation affected.
   f. Does anyone in the organisation know about the facts?
   g. Has the matter previously been reported?

The **RSII** may contact the reporting person again if necessary, to obtain further information or for them to provide documentation. If the report falls outside the objective scope of the IIS, the **RSII** shall close the report, informing the reporting person of that closure. For this reason, it is important that the reporting person provide some method of communication for that purpose.

1.4. Anonymity

Grupo Fedola's IIS allows reports to be made **anonymously**.

However, Grupo Fedola encourages the reporting person at least to provide a means of communication so that any information necessary to clarify the facts can be requested and a communication channel can be established between the **RSII** and the reporting person.

Notwithstanding the above, when a report is submitted (**whether anonymous or not**), Grupo Fedola ensures that the internal reporting procedure shall be carried out in a secure manner that guarantees the confidentiality of the identity of the reporting person and other related information.

2. - REPORT MANAGEMENT PROCEDURE

2.1. Receipt of the information

In order to obtain all the necessary data to assess the information and take appropriate action, the report must meet the minimum requirements established in the previous section. In this regard, to ensure proper data collection, the **RSII** must make sure to obtain as much information as possible from the reports and, where appropriate, attempt to contact the reporting person to obtain all the data that may be needed.

2.2. Registration and classification of the report

Once the report has been received, it shall be assigned a **unique identification code** and classified in order to prioritise the reports received according to the following categorisation criteria: **minor, serious, very serious, or inadmissible**.

Both the **admission for processing** of the report and, where applicable, its **dismissal and the reason for it**, shall be communicated to the reporting person within a maximum period of **3 months**.

The data provided through the internal reporting channel shall be included in a personal data file, which shall be processed in accordance with the **General Data Protection Regulation** and the applicable regulations.

If different reports of irregularities are received concerning the same facts or facts linked to the same person affected by the report, the **RSII** may combine the different cases, assigning to the group of files the number of the oldest file.

In a preliminary analysis, the **RSII** may propose measures relating to urgent reports, proposing where appropriate measures to mitigate the risk materialised or liable to materialise, and measures to preserve evidence.

2.3. Admission procedure

Once the information has been recorded, the **RSII** must check whether it describes facts or conduct falling within the material scope of application.

After carrying out this preliminary analysis, the **RSII** shall decide whether to **admit** or **reject** the report within a period not exceeding **ten working days** from the date of entry in the information register. The information may also be forwarded immediately to the **Public Prosecutor's Office**.

a) **Reject the report**, in any of the following cases:

1º When the facts reported are entirely implausible.
2º When the facts reported do not constitute an infringement of the legal system.
3º When the report is manifestly unfounded or there are reasonable indications that it was obtained through the commission of a criminal offence. In the latter case, in addition to rejection, a detailed account of the facts considered to constitute a criminal offence shall be sent to the Public Prosecutor's Office.
4º When the report does not contain any new and significant information on infringements compared to a previous report in respect of which the corresponding procedures have been concluded, unless new factual or legal circumstances justify different follow-up.

5º When the information affects classified information or information declared secret or reserved.

The rejection shall be communicated to the reporting person within the following **five working days**, unless the report was anonymous and the reporting person had waived the receipt of communications.

b) **Admit the report for processing**

Admission for processing shall be communicated to the reporting person within the following **five working days**, unless the report was anonymous and the reporting person had waived the receipt of communications.

c) **Immediately forward the information to the Public Prosecutor's Office** when the facts may arguably constitute a criminal offence, or to the **European Public Prosecutor's Office** if the facts affect the financial interests of the European Union.

2.4. Conduct of the investigation

Once all relevant information about the reported facts has been obtained from the reporting person and the report has been admitted for processing, the **RSII** shall entrust the investigation of the report to the **investigation committee**, whose composition shall vary depending on the structure of the company to which the report relates, as shall its members, which shall vary depending on the business unit affected.

When convening the committee, the **RSII** must exclude those members who are in a conflict of interest in view of the content of the report. In such cases, they shall be replaced by the person holding an equivalent position or by their direct hierarchical superior.

It must also assess the possible **outsourcing of the investigation** when the facts reported affect persons performing especially sensitive functions in the organisation, such as members of **Senior Management** or the **Governing Body**.

2.5. Investigation procedure

The file must be opened within a maximum period of **5 working days** and acknowledgement of receipt must be given to the reporting person within a maximum period of **7 working days**.

The opening of the file shall take place in an individualised file, with the identification of the reporting person, if identified, and of the person affected by the report, the risk situation reported, and its classification as conduct contemplated in criminal legislation.

At all times, the committee shall attempt to carry out the investigation using its own resources and, if this is not possible, shall request the assistance of other departments or operational areas. If the participation of other departments is necessary, their assistance shall be requested and they shall be required to comply with the duty of confidentiality.

, whenever it considers it necessary, the investigation committee may rely for the processing and investigation of the report received on **external independent advisers or experts**, who shall also be bound by the duty of confidentiality.

The investigation committee shall issue a **proposed resolution** preferably within **2 months** from the opening of the file, with the possibility of a further **one-month extension** if necessary, subject to a reasoned decision duly communicated to the person affected by the report, in cases where the file has not been considered secret in view of the seriousness of the facts investigated.

The investigation committee shall agree on the carrying out of the necessary steps to clarify the facts, keeping documentary evidence of each and every action taken.

The result of this investigation shall be reflected in a **conclusions report**.

The actions that must always be carried out are:

1. Request confirmation from the reporting person, where communication with them is possible, and obtain relevant additional information, such as documents or testimonies.
2. Summon internal or external persons involved to inform them of the existence of the report, take written statements from them, and request useful additional information, such as documents or testimonies.
3. Inform the affected areas or business units of the opening of the file, requesting the information necessary to clarify the facts.
4. Conduct an interview with the person or persons affected by the report, allowing them to be accompanied by a person of trust. The person affected by the report shall be informed of the actions or omissions attributed to them and shall have the right to be heard at any time.
5. The proposed resolution must include a detailed report of the steps taken, as well as those that could not be carried out. In addition, conclusions must be presented as to whether a criminal offence or conduct prohibited by current law, compliance policies, or other organisational policies has been committed, as well as the persons allegedly responsible.
6. The conclusions report shall be communicated to the person affected, who shall have a maximum period of **10 days** to submit their allegations. Once the allegations have been analysed, the **RSII** shall issue its final proposed resolution to the **Board of Directors**.

2.6. Resolution of the report

Once the conclusions report (hereinafter, the **"report"**) has been prepared, the investigation committee may adopt the following decisions:

a) File the report and close the investigation, if it is considered that irregular conduct has not been proven or that the information, despite the reporting person having been asked to expand it, does not meet the requirements of truthfulness and clarity.

b) Submit the report to the company's management, which shall decide, where appropriate, on the imposition of the corresponding disciplinary sanctions on the basis of the report drawn up.

c) Submit the report to the **Board of Directors of Grupo Fedola**, which shall decide whether or not to initiate the corresponding judicial or administrative actions, including criminal or disciplinary/sanctioning actions, where appropriate.

If a criminal offence has been committed, a possible failure in the controls implemented for the prevention of criminal offences shall be assessed and improvement actions proposed.

The report must contain the steps carried out and those that could not be carried out, and the conclusions as to whether a criminal offence or prohibited conduct has been committed and as to the persons allegedly responsible.

The reporting person and the investigated person shall receive a notification with a brief explanation of the steps taken and the conclusion of the file. The confidential nature of the information and the rights of the persons involved shall be respected at all times.

2.7. Closure of proceedings

Once all investigative actions have been completed, the investigating committee shall issue a **report-proposal** with the following content:

1. A statement of the facts reported together with the identification code of the report and the registration date.
2. The classification of the report for the purpose of determining its priority in processing.
3. The actions taken in order to clarify the facts.
4. The conclusions reached during the investigation and the assessment of the steps and evidence supporting them, indicating the proposed actions to be taken.

Following this report, the **RSII** shall adopt one of the following decisions:

- **Closure of the file**, which shall be notified to the reporting person and the affected person. In such cases, the reporting person shall be entitled to the protection provided by law, unless, as a result of the actions carried out during the investigation phase, it is concluded that the information, in light of the information gathered, should have been rejected because one of the grounds provided for in this procedure applied.
- **Referral to the Public Prosecutor's Office** if, despite no initial indication that the facts might constitute a criminal offence, this becomes apparent during the investigation. If the offence affects the financial interests of the European Union, it shall be referred to the **European Public Prosecutor's Office**.
- **Submission of all proceedings to the Board of Directors of Grupo Fedola** for the adoption of such measures as they consider appropriate, where applicable.

This conclusions report shall be filed and kept by the **RSII** in the **record book**.

3. - PREPARATION OF THE ANNUAL REPORT

The **RSII** shall prepare an **annual report** to assess the operation and effectiveness of the **Internal Information System (IIS)**, including data such as:

- **Total number of reports received**
- **Classification of reports** (**minor, serious, very serious, inadmissible**)
- **Reports closed without investigation** for not meeting minimum requirements
- **Reports closed after investigation** because they did not constitute irregular conduct
- **Investigated reports that resulted in disciplinary action**, distinguishing whether they involved judicial proceedings
- **Typology of irregular conduct detected**
- **Business areas affected by the reports**

The **RSII** shall establish annual improvement objectives to optimise the IIS and investigation processes. The report is used for the monitoring and continuous improvement of the system.

ANNEX II.- FORM FOR REPORTING INFORMATION RELATING TO LAW 2/2023, OF 20 FEBRUARY, REGULATING THE PROTECTION OF PERSONS WHO REPORT REGULATORY INFRINGEMENTS AND THE FIGHT AGAINST CORRUPTION

Instructions for submission:

- Please make sure to complete all relevant information.
- If additional documentation is included, attach it together with this form.
- Send the form to the channel enabled by the organisation to receive reports in accordance with **Law 2/2023** and the **internal information system policy**.
- The internal reporting channel guarantees the confidentiality of the information and of the reporting person, in compliance with the applicable regulations.

1. Reporting person's details (if you wish to remain anonymous, leave this section blank)

Full name: _____
ID/NIE (if applicable): _____
Contact telephone number: _____
Email: _____

2. Communication channel chosen for case follow-up:

☐ **Email**
☐ **Telephone**
☐ **Other (please specify): _____**

3. Relationship of the Reporting Person with the organisation or affected entity:

☐ **Employee**
☐ **Collaborator**
☐ **Supplier**
☐ **User**
☐ **Other (please specify): _____**

4. Details of the entity and/or person affected by the report:

Name of the entity/organisation: _____
Name of the area/department: _____
Person(s) involved (if known): _____

5. Description of the regulatory infringement or act of corruption

(**Describe in detail the facts you wish to report. Include dates, places, and any relevant information.**)

6. Evidence or attached documents (if any):

☐ **Additional documentation attached**
☐ **I do not have evidence at this time**

7. Declaration of the Reporting Person:

I declare that the information provided in this form is truthful and has been collected and communicated in good faith, within the framework of **Law 2/2023**, in order to report possible regulatory infringements or acts of corruption.

Signature of the reporting person: _____
Date: _____

Legal Notice

This form is protected by **Law 2/2023**, and its improper use may give rise to legal liability. Reports made in bad faith or with defamatory intent are subject to legal sanctions.

ANNEX III CONFIDENTIALITY PROTOCOL

1. OBJECTIVE

The objective of this protocol is to ensure the confidentiality and protection of reporting persons when the report is made through channels that are not integrated into the IIS.

2. RESPONSIBILITY OF STAFF

All staff of the organisation are responsible for maintaining the confidentiality of internal reports and protecting the identity of reporting persons. This includes employees, managers, and any other person who may receive or have access to information related to a report.

3. PROCEDURE IN CASE OF RECEIPT OF REPORTS THROUGH UNOFFICIAL CHANNELS

If a staff member receives a report through an unofficial channel, they must:

a) Not disclose the identity of the reporting person. It is important not to reveal the identity of the reporting person to any other person, including other staff members.
b) Forward the report to the designated person responsible. The staff member must immediately forward the report to the **RSII**, providing all details and documentation received.

c) The **RSII** shall inform the reporting person about the correct procedure, whenever possible. Likewise, they shall inform them that the report has been received and that the proper process is being followed for its handling.

d) Follow-up and monitoring. The **RSII** shall monitor the report and take the necessary measures to ensure that the proper report management process is followed.

4. INFORMATION AND AWARENESS

All employees shall be informed about the importance of confidentiality and the proper use of internal reporting channels, in order to promote a culture of trust and respect towards reporting persons.

DO YOU KNOW GRUPO FEDOLA'S INTERNAL INFORMATION SYSTEM?

For more information, please consult the
INTERNAL INFORMATION SYSTEM POLICY,
available on the website **www.grupofedola.com**

In compliance with **Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption**, the company has implemented the **Internal Information System (IIS)**, comprising several communication tools. The IIS is available to employees and collaborators of Grupo Fedola companies so that they may report to the company any matter of which they are aware concerning criminal, administrative, labour, European Union law infringements, or any other kind of unlawful conduct.

It is a **private communication channel**, active **24 hours a day, 365 days a year**, with a guarantee of **maximum confidentiality** and in compliance with the regulations in force.

Reports or complaints may be addressed to the **Person Responsible for the IIS (RSII)** of the organisation, that is, the person holding the position of **Head of the Legal Department of Grupo Fedola**. The means for making reports through the IIS are:

Kaloyan Simeonov
INTERNAL INFORMATION SYSTEM

Email: canaldedenuncias@grupofedola.com

Registered post with acknowledgement of receipt, addressed to Grupo Fedola, Calle Candelaria, Edificio Olympo, No. 28, 1st floor, Postcode 38002, Santa Cruz de Tenerife, for the attention of the **RSII**.

Telephone, via the main offices of Grupo Fedola, number **922 151499**, dialling **extension number 4** corresponding to the **Legal Department** and the role of the **RSII**.

Group corporate application
(**Whistleblowing Channel section**).

Website. Whistleblowing channel tool available on Grupo Fedola's website.

Please note that if the IIS receives information concerning facts constituting **harassment of any kind**, these shall be processed through the **specific procedure applicable to such cases**.