Ethical Channel Protocol

Last update: May 2026

INDEX

INTRODUCTION

Minerva Insights Group (hereinafter also referred to as the "**Group**" or the "**organization**"), in order to promote its culture of ethics and compliance, has implemented an internal communication system, called the **Ethical Channel**, with the main purpose of promoting transparency, integrity and compliance with ethical and legal standards within the organization.

The Ethical Channel is, therefore, the means through which any person belonging to the organization or linked to it can report possible irregularities, inappropriate conduct, legal or ethical breaches, or any other activity that may be considered harmful to the organization or its stakeholders, thus allowing the early detection and correction of potential problems before they escalate into transcendental situations.

The potential sanction for inappropriate conduct may apply not only to the offender, but also to those who participate in, approve, facilitate, or conceal such conduct, provided that such liability is established in light of the specific circumstances of the case, the parties' roles and responsibilities, and applicable labor and legal regulations.

The foregoing is without prejudice to Grupo Minerva Insights promoting the good-faith reporting of potential irregularities through the Ethics Channel, based on reasonable grounds.

1. OBJECT

The purpose of this Protocol is to ensure the operation of the Ethical Channel, the basic principles by which it is governed, as well as the processing, management, investigation and response to communications received through it.

2. SCOPE OF APPLICATION

The Minerva Insights Group's **Ethical Channel** is applicable to all the companies that compose the Group.

All members of the **Group**, including any natural or legal person with whom they have or plan to have corporate, institutional and business relationships, such as associates, governing and representative bodies, advisory bodies, directors, employees, suppliers, outsourced service providers, collaborators, consultants and advisors (hereinafter "members"), will have at their disposal the Ethical Channel as a confidential channel.

The communications that can be made through the Ethical Channel are irregularities related to:

- ✓ Any conduct typified in the Penal Code and, in particular, those that could give rise to a direct or indirect benefit for the Group.
- ✓ Any actions or omissions that do not comply with European Union regulations in the following aspects:
    - ➢ Public procurement

- Financial services, products and markets
- Prevention of money laundering and terrorist financing
- Product Safety and Compliance
- Transport insurance
- Safeguarding the environment
- Radiation protection and nuclear safety
- Food and feed safety, animal health and animal welfare
- Public health
- Consumer protection
- Preservation of privacy, personal data, and security of networks and information systems
- Financial interests of the European Union
- Acts or omissions affecting the European Union market in terms of competition and aid granted by States, as well as infringements relating to the internal market in relation to acts that infringe the rules of corporation tax or with practices whose purpose is to obtain a tax advantage that distorts the object or purpose of the legislation applicable to corporation tax

✓ Any conduct that could constitute a serious or very serious administrative offence because it involves economic damage to the Public Treasury and/or Social Security.

✓ Any conduct or fact that could constitute sexual and/or gender-based harassment.

This Protocol is established to ensure that, in the event of any irregular action or potential action included in the established scope, the corresponding communication is treated impartially and confidentially, adopting the appropriate measures to protect the interests of the **Group** and its members.

3. BASIC PRINCIPLES

The principles that govern the operation and management of the Ethical Channel are the following:

✓ **Confidentiality**
Unequivocal commitment to guarantee confidentiality throughout the process, regarding the identity of the people who make use of it and the content of their communications and appearances.

✓ **Good faith**
Communications made through the Ethical Channel will be made honestly, with conviction as to the truth or accuracy of their purpose. Communications will be considered truthful, complete and accurate, even if, subsequently, it is verified that their content was equivocal.

✓ **Prohibition of retaliation**
It is guaranteed that there will be no retaliation or any type of negative consequences against anyone who communicates in good faith a possible misconduct or who assists with an investigation.

✓ **Proportionality**
All notifications received will be treated equivalently, regardless of who the sender is.

4. CHARACTERISTICS OF THE ETHICAL CHANNEL

The main characteristics of the Ethical Channel are the following:

- ✓ **Anonymity**
  The possibility of anonymous communications is guaranteed, understood as those that do not contain any reference to the reporting person.
- ✓ **Private Area**
  When a whistleblower reports any behaviour, action or fact that may constitute a crime, an infringement of European Union Law in the terms specified above, a serious or very serious administrative offence because it involves a breach of the Public Treasury and/or Social Security or, where appropriate, an infringement of Internal Regulations, the tool generates a code so that the whistleblower can:
  - ✓ Track the status of communication
  - ✓ Communicate with the Ethical Channel Manager via chat

5. DIFFUSION

In order for the Ethical Channel to be effective, it is important to ensure that all members of the organization:

I. Know about the existence of it.
II. Understand its purpose.
III. Are convinced of the advisability of informing the organization of possible irregularities or facts that may constitute a crime of which they may be aware.
IV. Know the rights that assist them.
V. Have confidence that communications will be handled objectively and fairly.

The existence of the Ethical Channel will be communicated to the members of the Group through an internal communication indicating the place, the way to access it and its subsequent steps.

6. MEANS OF COMMUNICATION

Minerva Insights Group makes the following means available to all its members to carry out communications:

- **Website**: https://report.uhy-fay.com/grupominerva

- **Postal address:** UHY Fay & Co. C/ Serrano, 1. 28001 Madrid. Spain

  (ref. Ethical Channel - "Confidential and Personal")

(UHY Fay & Co. is the external responsible for the management of the Ethical Channel of Minerva Insights Group)

For communication made through the postal address, a form is available that is attached to this programme as Annex II, which is optional.

7. BODIES IN CHARGE OF THE MANAGEMENT OF THE ETHICAL CHANNEL

- External Manager of the Ethical Channel

To ensure the objectivity, transparency and impartiality of the process, the management of the tool has been entrusted to an independent third-party expert. The functions of the independent external third party with respect to the Ethical Channel will be as follows:

- ✓ Reception of communication.
- ✓ Acknowledgement of receipt to the informant within a maximum period of seven days.
- ✓ Processing and informing the Internal Manager of the Group's System.
- ✓ Preparation of a preliminary report.

- Internal System Manager

In order to safeguard independence and impartiality, the investigative function of the **Minerva Insights Group's Ethical Channel** is assumed by the **Group's Compliance Officers, as Internal Managers of the System**.

The mission of the Internal System Manager in the Ethical Channel is to **control and investigate** all communications made through it. Its functions are as follows:

- ✓ Archiving or admission for processing of the communication, as appropriate.
- ✓ Research.
- ✓ Preparation of a report of conclusions and proposal for a resolution.
- ✓ Communication with the parties.
- ✓ Preparation of a follow-up report on the proposed measures and the safeguarding of the principle of non-discrimination.
- ✓ Monitoring potential retaliation.

- Board of Directors:

The Board of Directors of the parent company is ultimately responsible for the Ethical Channel and, as such, is responsible for deciding on the files originated as a result of valid communications that have been the subject of its own investigation process through the following procedure:

- ✓ Reception and study of the report of conclusions and proposal for resolution.
- ✓ Issuance of final resolution.

8. SCHEME OF OPERATION OF THE ETHICAL CHANNEL

The management procedure of the Ethical Channel is articulated in the following phases:

8.1 PROCESSING OF THE COMMUNICATION

- **Availability:** the Ethical Channel is operational 24 hours a day, 365 days a year.
- **Content of the communication:** the informants must **detail the events** and specify the **approximate date** on which they occurred, as well as the **Group company in which the events occurred**.
- **Identification of the informant:** it is expected that it is the informant who decides whether or not he wants to identify himself, since anonymous communications are foreseen.
- **Follow-up of the communication:** in the event that the informant decides to use the online tool**,** after making the communication they will obtain a tracking code to access the private area, and receive through this channel the acknowledgement of receipt of the same within a **maximum period of 7 days**. In the private area, the whistleblower will be able to monitor the status of their communication and, if they wish, use the chat enabled to communicate with the external Manager of the Ethical Channel.

  In the event that the respondent decides to use the postal address provided, he or she must fill in Annex II of this Protocol and send it by post to the address C/ Serrano, 1; 28001 Madrid (Spain) for the attention of UHY Fay & Co., the external Manager of the Management of the Ethical Channel of Minerva Insights Group. If the informant identifies himself in the communication, he or she will receive, within 7 days, an acknowledgement of receipt from the external Manager of the Ethical Channel, which is not the case for anonymous communications.

8.2 ADMISSION FOR PROCESSING

Upon receipt of the communication, the independent third-party expert shall register the communication and send an acknowledgement of receipt of the communication to the informant within **7 days** of receipt.

After the registration of the communication, the independent external third party shall submit to the Group's internal System Manager a preliminary report, which shall include all the information contained in the communication. After this, the Group's Internal System Manager must carry out an initial analysis to determine whether or not it justifies initiating an internal investigation:

- ❑ **No:** if after the preliminary assessment it is considered that the matter is not justified, the communication will be archived, documenting the reason for the decision to dismiss it, and notifying the informant in those cases in which it is possible.
- ❑ **Yes:** (see section internal investigation).

If the communication includes the Internal System Manager, the latter shall expressly refrain from assessing the communication and shall immediately inform the Board of Directors of the Group's parent company. The failure of the Internal System Manager to abstain when the communication received affects or may affect, directly or indirectly, constitutes a very serious misconduct within the disciplinary system.

8.3 INTERNAL INVESTIGATION

Once the communication has been admitted, the Internal System Manager will carry out the investigation in accordance with the principles established in the organization's regulations and will order the opening of the corresponding internal investigation as soon as possible, in such a way as to demonstrate the company's commitment to regulatory compliance, in order to:

- ✓ To clarify the facts communicated,
- ✓ Identify those responsible for the reported conduct, and
- ✓ To compile the relevant evidence for its discovery, observing all the rules and guarantees enshrined in this Protocol.

To initiate the internal investigation, the Internal System Manager will open a file, to which the corresponding number of proceedings will be assigned. This file must contain documentary evidence of all the actions carried out, attaching to it all the evidence or steps obtained in the course of the investigation.

8.3.1 Planning

The investigation will be initiated as soon as possible in such a way as to demonstrate the Group's commitment to regulatory compliance. Before starting the research, the following aspects will be planned and considered:

- Applicable regulations or conventions: whether any obligation or limitation is imposed that should be known before starting the investigation.
- Limitation period, if the alleged facts reported are time-barred or will soon prescribe in accordance with the provisions of the Workers' Statute.
- Protection of personal data applicable to the Ethical Channel.
- Specialized assistance: consider whether the matter requires a specialist/third party.
- Assessment of whether provisional measures should be adopted[1].

---

[1] At the initiative of the Internal System Manager, the adoption of precautionary measures may be agreed.
The adoption of such measures must be agreed in writing and the following must be set out in detail:

a. the reasons and needs that lead to the adoption of the precautionary measures,
b. the duration of the same, and
c. the identification of the measures adopted.

The adoption of precautionary measures will be exceptional and the least burdensome measure will always be chosen from among the most effective, necessary and useful to achieve the aims pursued. The adoption of these measures must be brought to the attention of the person(s) directly or indirectly affected by them.

8.3.2 Deadlines

The maximum period in which the research must be carried out may not exceed **3 months** from the receipt of the communication.

However, in cases of special **complexity** that require an extension of the term, it may be extended to a maximum of **another three additional months**.

The Internal System Manager will authorise the extraordinary extension of the aforementioned maximum period, issuing a justified resolution to this effect. This agreement will be incorporated into the corresponding file.

However, the exceptional extension that may be agreed upon must be proportional to the nature and difficulty of the facts under investigation and may not be extended for longer than strictly necessary for the correct and due investigation and discovery of the facts.

8.3.3 Principles of internal research

During the investigation, the fundamental rights recognized by the country's Constitution of the person or persons to whom the facts communicated refer, the workers of the companies that compose the Group and the other persons involved, directly or indirectly, affected by the facts that are the subject of communication must be respected.

It is important to remind those who are the subject of an investigation or participate in the investigation of the following principles:

- As a general rule, violations of fundamental rights and guarantees occurring in the course of an internal investigation shall constitute a serious or very serious infraction, as the case may be, in accordance with the whistleblower protection regulations applicable at the local level.
- The goal of an investigation is to establish the facts. The fact that an investigation is carried out does not presuppose that there has been a violation of the Internal Regulations or the legislation in force.
- Employees are expected to cooperate in the investigation of the facts.
- Being interviewed during an internal investigation or otherwise collaborating should not be stigmatized.
- Research is a confidential matter and confidentiality must be maintained. Information about the research may only be shared with those people who have a strict need to know about it.
- There will be no stigma in being investigated if at the end of the investigation it is proven that the facts were unfounded.
- The express prohibition of all types of reprisals and attempts to do so.
- The communicator must be informed at the time of establishing the first contact that:
    - The identity will be kept confidential at all stages of the process, although it may be necessary to disclose the identity to the persons involved in the investigation or in the subsequent judicial proceedings initiated as a result of the investigation

- No retaliation of any kind will be allowed for having interposed the communication

- The interviewee may be asked to submit a written statement based on his or her knowledge of the facts. If this is not possible, ask if you would be willing to sign a statement based on the notes taken during the interview.

8.3.4 Investigative measures

Within the framework of the investigation, all legally lawful and valid actions may be used to investigate the facts that are the subject of the report.

The selection and practice of such actions will be governed by the principle of proportionality. The measure must be:

- ✓ Exceptional (there must be no other less burdensome investigative actions to achieve the objective pursued).
- ✓ Necessary (without its practice, research could be compromised).
- ✓ Suitable (it must serve the purposes of the investigation).

Among others, the following will be lawful means of investigation:

- Interview with the informant, if possible, which must be preceded by the corresponding reading of the rights and guarantees that assist him.
- Interview with witnesses, which must be preceded, in any case, by a warning of their obligation to be truthful in their statements.
- Interview of the person under investigation, which must be preceded by the corresponding reading of the rights and guarantees that assist him or her and the right to make written allegations.
- Examination of documentation, merely exemplifying:
    - Bills
    - Travel expense settlements
    - Correspondence
    - Contracts
    - And any other document that may evidence the irregular conduct
- Recovery and analysis of information contained in electronic devices, through the use of software and hardware tools that preserve the integrity of the evidence, with absolute respect for current legislation. In any case, in order to proceed with the access and analysis of electronic devices, the following circumstances must be met:
    - The employee must have been clearly informed about the nature of the control that the Group may carry out over electronic devices;
    - The employee must be given details of the scope of such supervision, that is, tell him whether the flow of communications or the content of the communications will be inspected, whether all or only part of them will be inspected, whether such a measure will be limited in time, the persons who will have access to said information, the spatial limits of surveillance;

- All this must be done prior to the implementation of the measure

8.3.5 Rights of the investigated party

- ✓ The right to be informed as soon as possible as a result of a communication lodged against him.
- ✓ Right to judicial protection and defence, access to the file.
- ✓ The right to be informed of whether the interview will proceed.
- ✓ Right to the presumption of innocence.
- ✓ Right to legal assistance.
- ✓ Right to make written submissions.
- ✓ The right to be informed of the resolution or archiving of the communication.

8.3.6 Rights, guarantees and obligations of the whistleblower

- ✓ Right to information. In any case, the informant will be informed, whenever possible, about:
  - ➢ Initiation of the internal investigation as a result of your communication,
  - ➢ Development of the processing of the communication,
  - ➢ Concluding report of the internal investigation,
  - ➢ The decision of the Internal System Manager on the accreditation of the communication and,
  - ➢ Where appropriate, of the measures adopted
- ✓ Guarantee of confidentiality. The content of the communication, including the personal data of the informant, may be known exclusively to the body in charge of managing the communication. This guarantee is aimed at preventing any possible retaliation.
- ✓ Obligation to tell the truth about the facts communicated.

8.4 RESEARCH REPORT

Once the internal investigation has been completed, the Internal System Manager will submit a written report with the conclusions reached.

This report must include, where appropriate, in addition to the full content of the file initiated:

- The procedures used for their investigation.
- The documented results of the research.
- The corrective measures to be established.
- Allegations of the investigated party and the evidence provided by him that he deems appropriate.
- Corresponding proposal for a sanction for the person or persons responsible for them, in accordance with the applicable labour legislation in force and the sanctioning regulations of the Group's companies.

8.5 COMPLETION OF THE INVESTIGATION

In view of the result of the internal investigation carried out and the report issued as a result of the same, the Internal System Manager will decide, within a **maximum period of 10 working days** from the date of issuance of the conclusions report, whether or not it considers the reported infringement and the persons responsible to be proven.

❑ Non-accreditation of the facts that are the subject of the report.

If it is understood that the facts that are the subject of the communication have not been proven, the Internal System Manager will order the file to be archived, leaving a written record of the reasons on which such decision is based.

❑ Communication in bad faith.

If the result of the investigation determines that the informant filed the communication, complaint or claim in proven bad faith, the management of the organization will determine what type of disciplinary measure should be adopted against the informant.

❑ Accreditation of the facts to be reported.

If it is understood that the facts that are the subject of the report are proven, the Internal Manager of the System will transmit the report of conclusions to the Board of Directors so that it can adopt the appropriate measures with respect to the people under investigation.

Each case will need to be carefully reviewed, and several factors must be considered including:

- The seriousness of the proven facts.
- The concurrence of aggravating or mitigating circumstances.
- The employment file of the accused employee.
- How similar situations have been managed in the past to ensure consistency.
- The provisions of the legislation and the applicable Collective Agreement.

Regardless of the decision taken by the Internal System Manager in relation to the completion of the investigation, this decision must be documented.

If, as a result of the investigation, the violation of the law or the Internal Regulations is proven, **Minerva Insights Group** will carry out a review and update of the existing protocols, measures and controls, in order to implement the necessary improvements and in order to prevent new breaches from occurring again.

Likewise, **Minerva Insights Group** may reinforce the training previously provided to its members in order to prevent new breaches of the law or the Internal Regulations from occurring again.

8.6 RESOLUTION

The Board of Directors of the Group's parent company, responsible for the decision-making function, and after the reported facts have been accredited, will formulate, in relation to the report of conclusions and the proposals for sanctions, where appropriate, a resolution within **fifteen days** from the receipt of the aforementioned report.

This resolution will be sent to the Internal Manager of the System, so that he or she can communicate said resolution in writing to the parties.

As a result of the research that has been carried out and the final assessment and evaluation of the respective results, the following may be proposed:

a) Filing of the complaint.

(b) Adoption or promotion of appropriate measures, namely:

i. Changes in the Company's control processes and methods or policies;

ii. Corrections or adjustments to documents;

iii. Reports to the competent regulatory authorities;

iv. Termination of contractual relationships;

v. Initiation of disciplinary proceedings or loss of membership in a corporate entity;

vi. Initiation of judicial or criminal proceedings or measures of a similar nature

All disciplinary actions must be duly documented. If the disciplinary measure imposed is not dismissal, the situation should be monitored to identify possible signs of retaliation, as well as possible recurrent behavior on the part of the sanctioned employee.

8.7 COMMUNICATION TO THE PARTIES

❑ **Communication with the informant**

Minerva Insights Group may inform the person who has communicated the results of the investigation within the deadlines established for this purpose, and where appropriate, may be informed about whether measures are being adopted, without going into unnecessary details. Likewise, the informant must be reminded of what to do in the event that he suffers any type of retaliation or if he notices the repetition of events similar to those already reported. Finally, it is necessary to insist on the confidentiality of the investigation.

❑ **Communication with the investigated employee**

Minerva Insights Group must inform the person under investigation of the result of the investigation. If it is considered appropriate to impose a sanction, this requires following a series of formalities (written communication to the sanctioned worker indicating the infraction, the sanction imposed and the effective date of the same, among others).

Likewise, the sanctioned person must be warned that no reprisals will be tolerated. Where appropriate, it shall also be noted that the commission in the future of acts similar to those which have been the subject of this file will entail additional disciplinary measures. Finally, to reiterate once again the confidentiality of the investigation.

- **Communicating with witnesses**

It is not necessary to inform witnesses about the details of the investigation.

In no case will the Internal System Manager be obliged to provide the details of the investigation or to deliver a copy of the investigation report to any person who has participated in the investigation.

9. PROTECTION OF THE WHISTLEBLOWER AND THOSE TO WHOM THE REPORTED FACTS RELATE

In accordance with the whistleblower protection regulations applicable at the local level, governing the protection of persons who report regulatory infringements and the fight against corruption, Grupo Minerva Insights guarantees, in all cases, the highest level of confidentiality with respect to the content of communications, except where the applicable legislation provides that such information must be made available to the competent judicial, administrative, or law enforcement authorities.

Anyone who, in good faith, informs the Group of any circumstance, fact or communication through the Ethical Channel will not be subject to retaliation, discrimination or disciplinary sanction, and if it is confirmed that such persons have been subjected to retaliation, the perpetrators of the same will be subject to investigation and, where appropriate, sanction.

If it is shown that the whistleblower has acted in bad faith in his or her communication, the corresponding sanctioning measures will be adopted in this regard.

10. PROTECTION OF PERSONAL DATA

The personal data provided during the communication and obtained as a result of its processing and internal investigation, will be processed only for the management and control of the Ethical Channel, for which purposes the following will have exclusive access:

a) The person responsible for the System and whoever manages it directly.
b) The head of human resources, only when disciplinary measures could be taken against an employee.
c) The person in charge of the legal services of the entity or body, if appropriate the adoption of legal measures in relation to the facts reported in the communication.

d) The data processors that may be designated.
e) The Data Protection Officer (if assigned).

Lawfulness of the processing of personal data.

The processing of personal data will be understood to be lawful based on the provisions of Article 6.1.c) of Regulation (EU) 2016/679 and 8 of Organic Law 3/2018, of 5 December, and 11 of Organic Law 7/2021, of 26 May.

This procedure guarantees the exercise of the rights established in Organic Law 3/2018 (Protection of Personal Data and guarantee of digital rights), in 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 and in the additional regulations in force on the matter, both in terms of the information that must be provided in the different communications, and in terms of the specific information referring to the processing of the data and the possible exercise by the affected party of their rights.

The owners of the personal data may exercise their rights by letter addressed to the address at Rua Padre Luís Aparício, nº 10, 1º, Lisboa CP 1150 248 Lisboa (Portugal).

However, the exercise of such rights will not proceed in the following cases:

a. When the person under investigation exercises his or her right of access, the identification data of the informant will not be communicated to him/her.
b. When the exercise of these rights is projected with respect to a communication related to the prevention of money laundering and terrorist financing, in which case the provisions of Article 32 of Law 10/2010, of 28 April, on the prevention of money laundering and terrorist financing will apply.

The personal data contained in communications shall be retained in the channel for as long as necessary to carry out the investigative proceedings provided for under the whistleblower protection regulations applicable at the local level. Once such proceedings have concluded, the personal data contained in the communications shall be deleted and the communications shall be retained in a blocked state outside the Ethics Channel, in order to preserve evidence of the system's operation. Should no investigative proceedings have been initiated within 3 months of the communication, the personal data shall likewise be deleted and retained outside the Ethics Channel.

ANNEX I

DECLARATION OF CONFORMITY PROTOCOL WHISTLEBLOWING CHANNEL

I have received, read, and understood the Ethical Channel Management Protocol from Minerva Insights Group.

To this end, I fully accept the responsibility to comply with the ethical principles and guidelines set out in the Protocol.

I also understand the importance of using the Ethical Channel to report irregularities, inappropriate conduct, legal or ethical breaches, or any other activity that may be considered harmful to the Group or its stakeholders, and I undertake to make appropriate and confidential use of this resource.

In... to....... of........................ of 202....

____

Signature and full name

ANNEX II

COMMUNICATION FORM	
INFORMANT DATA	Name and surname
	Email
GROUP COMPANY TO WHICH THE INFORMANT BELONGS	
DATE OF COMMUNICATION	
APPROXIMATE DATE OF EVENTS	
DESCRIPTION OF REPORTED FACTS	Describe what your communication consists of, the company where the act was committed, who are the people involved, which areas of the entity are affected, means that have been used to carry out the conduct and all relevant data that you consider.
EVIDENCE	

In accordance with 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, and Organic Law 3/2018 of 5 December 2018 on the

Protection of Personal Data and guarantee of the digital rights of MINERVA INSIGHTS GROUP, S.A., as the party responsible for the data provided, informs of the following points relating to the processing of the data:

Responsible: MINERVA INSIGHTS GROUP, S.A., with CIF 517188627 and address at Rua Padre Luís Aparício, nº 10, 1º, Lisboa CP 1150 248 Lisboa (Portugal). **Purpose**: to manage your communication, take appropriate corrective action and, if necessary, inform you of the outcome of the procedure. **Legitimation**: legal obligation (Art. 6.1.c) GDPR). **Conservation**: The personal data of the communications will be kept in the channel for as long as necessary to carry out the investigative measures provided for in Law 2/2023 of 20 February. Once the proceedings have been completed, the personal data will be deleted from the communications and these will be kept blocked outside the Ethical Channel, to leave evidence of the operation of the system. If no investigation actions have been initiated after 3 months have elapsed since the communication, the personal data will also be deleted and stored outside the Ethical Channel. **Data transfer**: No data will be communicated to third parties, except by legal obligation. Likewise, it is reported that the data will be processed in a lawful, loyal, transparent, adequate, pertinent, limited, accurate and updated manner. **Exercise of rights**: You may exercise your rights of access, rectification, limitation of processing, deletion, portability and opposition to the processing of your personal data, as well as the consent given for the processing of the same, by sending your request to the address at Rua Padre Luís Aparício, nº 10, 1º, Lisboa CP 1150 248 Lisboa (Portugal). You may also contact the Supervisory Authority.