



PROCEDURE OF THE AMPER GROUP INTERNAL INFORMATION SYSTEM

ELABORATION, REVISION AND APPROVAL

Prepared: Compliance	Revised: Ethics Committee	Approved: CEO
Date 26/03/2026	Date:22/04/2026	Date: 28/04/2026

Contents

1. INTRODUCTION.....	3
2. OBJECT	3
3. SCOPE.....	3
4. COMPETENCES AND RESPONSIBILITIES.....	5
5. COMMUNICATION VIAS OF THE INTERNAL SYSTEM OF INFORMATION AND REQUIREMENTS FOR THE PRESENTATION OF COMMUNICATIONS	6
6. AMPER COMMUNICATIONS PROCEDURE.....	6
7. INTEREST CONFLICT MANAGEMENT	15
8. REGISTRATION OF COMMUNICATIONS	16
9. DATA PROTECTION	16
10. EFFECTIVE DATE AND AMENDMENTS TO THE POLICY	18
11. VERSION CONTROL.....	19

1. INTRODUCTION

This Internal Information System Management Procedure (hereinafter referred to as the “Procedure”) is binding on AMPER S.A. and other entities under its control (in forward, jointly, “AMPER” “AMPER Group” or “Organization”) in accordance with the Internal Information System Policy (hereinafter referred to as “Policy”). For this purpose, “Amper” or “Amper Group” and “Amper Group” companies are all those companies, companies, branches, consortia, etc. in which Amper, S.A. is in a position of dominion or control in relation to another company because it is in one of the following situations: (i) owns directly or indirectly the majority of voting rights; (ii) has the power to appoint or remove a majority of the members of the administrative body; (iii) has the power, by virtue of agreements concluded with third parties, to dispose of a majority of voting rights; and (iv) has appointed a majority of the members of the administrative body with their votes. Without prejudice to the general aspects referred to therein, the operational annex to this procedure shall be drawn upon, which shall determine, in each country, the differences or specificities to be applied. The preparation of this complaint management procedure has been carried out taking into account the European legislation on the protection of the current informant, without prejudice to the fact that those national legal frameworks of application have been considered to incorporate the specifics that apply in each case. The Group guarantees the proper management of all communications received through the Complaints Channel which, in any event, will be examined and treated with the utmost respect and confidentiality, in accordance with the provisions and principles set out herein. In any event, the Panel may refer the investigation proceedings to a third party expert if circumstances so advise. All communications made through the Complaints Channel must be made in good faith. False or malicious communications or complaints may be punished, without prejudice to any civil or even criminal liability that may arise in accordance with the applicable legislation.

2. OBJECT

The Procedure regulates the aspects necessary to properly process the communications received through the Complaints Channel in all the societies in which the Group operates with the aim of ensuring the correct treatment of the information, the adequate protection of the informants in accordance with the provisions of the Internal Information System Policy and the applicable regulation and the proper management of the conflict of interest. The procedure is without prejudice to the provisions of the collective agreements and any other legal provision that may be applicable to AMPER, which shall remain in force.

3. SCOPE

3.1. SUBJECT SCOPE

This Procedure is binding on all directors, directors, employees regardless of their functional or hierarchical position (hereinafter referred to as the “Subject Person” or the “Personal”).

It shall also apply to persons who communicate information on offences obtained in the framework of an already completed employment relationship, as well as to persons whose employment relationship has not yet begun, in cases where information on offences has been obtained during the selection process.

In addition, it includes in the scope of application any person, natural or legal, who has obtained information about infringements in a professional context, or who works under the supervision and direction of contractors, subcontractors and suppliers (including Temporary Business Unions - UTE- or any other form of association) on behalf of AMPER.

Also, it will apply to those who provide their services in AMPER even if they are not part of the staff (through contract, scholarship). It is encouraged that AMPER’s external interest groups (hereinafter referred to as “Third Parties”) use AMPER’s Internal Information System for cases regulated in this Policy, as a communication mechanism regardless of other existing channels made available to them.

3.2. SCOPE OF OBJECTIVE

- I. Through the different channels that are integrated into the Internal Information System, informants may communicate knowledge or motivated suspicion of irregular conduct in the following areas: Infringements, actions or omissions of European Union law provided that they fall within the scope of Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 or of any national transposition rule.
- II. The unlawful cases covered by the legal system that result from application in each of the jurisdictions in which we operate, which may include both criminal offences, as well as other offences such as administrative offences or in the area of safety and health at work, which will be dealt with in accordance with the regulations in force in the jurisdiction in which the act occurred, which implies that the guarantees defined in European and Spanish legislation on protection of the informant will not apply in all cases.
- III. Within the Spanish legal system, criminal offences, serious and very serious administrative offences and violations of labor law in the field of occupational safety and health.
- IV. Non-compliance with the Code of Conduct or other internal standards as essential rules of the Compliance System. The processing of communications relating to such non-compliance shall be carried out in accordance with the principles of action and commitment set out in this Policy.

4. COMPETENCES AND RESPONSIBILITIES

4.1. GOVERNING COUNCIL

The Board of Directors of AMPER has the competence to: – Approve the Policy and Procedure of the Internal Information System of AMPER, including its updates or modifications and – Designate the Head of the Internal Information System of AMPER, for the management and conduct of the investigations of the communications carried out.

4.2. RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM AMPER'S

Board of Directors appoints AMPER as the Head of the Internal Information System (hereinafter referred to as the “System Manager”) to the AMPER Ethics Committee, as a collegial body responsible for the management of the internal information system and the processing of research files.

He has the appropriate competence, integrity, authority and independence, as well as the resources necessary for the performance of his duties.

The following are details of the responsibilities attributed to the System Manager:

- **To ensure maximum confidentiality in relation to the identity of the informant**, the persons mentioned in the communication, the information communicated and the actions that take place as a result of the processing of the communication.
- **To maintain secure communication channels with the informant**, using the channel tool or any other means that, for this purpose, can be enabled according to the circumstances.
- **To ensure that the processing, instruction and resolution of communications or complaints** is carried out in accordance with the principles and guarantees provided for in the laws and the Policy, in a diligent manner and acting with full independence and impartiality.
- **To report periodically** to the Management Board through the Audit Committee, at least annually, and whenever necessary, as much information is required about the activity of the System, preserving in any case the confidentiality and security of the information, as well as the remaining guarantees and rights of the informants.
- **To update the Registry Book** with the information of the communications received.

Without prejudice to the above, any person of AMPER is obliged to collaborate with the System Manager on the terms set out in this Procedure. This collaboration includes, among other actions, meeting the requirements for information or documentation that are formulated, appearing and answering questions that may be asked if required, respecting the established deadlines, and maintaining confidentiality about the existence and content of any investigation. It shall also refrain from obstructing the submission or processing of

communications, from retaliating, or from communicating information knowingly of its falsity. In the event of any conflict of interest, it shall be managed in accordance with the established procedure.

5. COMMUNICATION VIAS OF THE INTERNAL SYSTEM OF INFORMATION AND REQUIREMENTS FOR THE PRESENTATION OF COMMUNICATIONS

For communication and in order to foster dialogue and active listening within the culture of normative and ethical compliance as a basic element of the Internal Information System, AMPER has the following channels of communication:

- Web: <https://www.grupoamper.com/formular-reports/>
- Postal mail: to the attention of the Compliance Management Amper Group: C/ Virgilio,2 (Edif. 4). Image City CP.28223, Pozuelo de Alarcón, Madrid).
- E-mail: committeeica@grupoamper.com,
- Face-to-face: face-to-face meeting with the Compliance Officer at headquarters C/ Virgilio,2 (Edif. 4). City of Image CP.28223, Pozuelo de Alarcón, (Madrid).

In the event that any communication, information or complaint falling within the material scope of this Procedure is communicated by means other than those previously provided, it shall be forwarded by the person receiving it immediately and confidentially to the Compliance Officer of AMPER, refraining from sharing this information with persons outside the management of the Complaints Channel.

Finally, information concerning the existence of competent authorities in each country in which the Group operates in order to receive communications as an external channel of communications will be incorporated through annexes approved by the person responsible for compliance of the Group.

6. AMPER COMMUNICATIONS PROCEDURE

AMPER has implemented a complaint channel to be accessed from any electronic device with Internet connection, available at the following link: <https://www.grupoamper.com/formulario denuncias/>

The purpose of the channel is to allow any interested party to communicate, anonymously if he so wishes, all conduct within the objective scope of the Internal Information System specified in the Policy and Procedure.

6.1. FORMULATION OF THE COMMUNICATION

The person who decides to make a communication must provide the maximum available information on the reported facts with the same information, including expressly:

- Identifying data (name and surname), although anonymous communications will be admitted.
- Identification of the company of the Amper Group in which the alleged infringement or non-compliance took place.
- The type of link that the informant maintains with AMPER, in accordance with paragraph 3 of the Policy and Procedure of the Internal Information System.
- The date or dates on which the reported acts were committed as offenders (even if by approximation).
- The person/s who, if any, was affected by the communication.
- A complete and precise description of the facts. – Existence of witnesses, and, where appropriate, a list of the same.
- Person or collectivity, who is considered to be liable for the conduct.
- If possible, documents, data and other sources of evidence or information that, if any, could permit the investigation of the facts.

Any communication must be made in good faith and deal with certain facts, without prejudice to the inaccuracy or omission that the informant may inadvertently commit.

6.2. RECEPTION OF COMMUNICATION

The System Manager will carry out the management of communications.

Once the communication, information or complaint has been made, it will be registered in the tool support for the management of complaints, assigning it a unique access code.

The submission of the communication or complaint shall generate an acknowledgement of receipt, which shall be sent to the informant within seven (7) calendar days of receipt of the complaint, unless this may endanger the confidentiality of the information. By sending the acknowledgement of receipt, the informant shall be informed of the receipt of the complaint and the registration number assigned.

In the event that any information is received by a means other than that established in the Internal Information System, from AMPER, confidentiality shall be ensured and, to the extent possible, that its treatment is in accordance with the provisions of this Procedure.

The Channel will have a secure and restricted-access database in which all communications or complaints received, date of receipt, identification code, status and action taken thereon will be recorded and updated.

Personal data that can be collected will be processed with respect to the data protection regulations that result from application and in accordance with the terms provided for in the AMPER Privacy and Data Protection Policy.

6.3. VERBAL COMPLAINTS

When communications or complaints are received orally, the informant will be offered the opportunity to formulate, ratify, expand or clarify the complaint at a face-to-face meeting within seven (7) days of receipt.

In this case, the informant shall be requested to have the oral communication recorded, informing him of the processing of his data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Organic Law 3/2018 of 5 December 2016 on the Protection of Personal Data and Guarantee of Digital Rights.

It offers the possibility of communicating normative breaches, at the request of the informant, through a face-to-face meeting with the natural person responsible for the internal information system that can be requested at the following email address: committeeica@grupoamper.com

In case of making the communication by face-to-face meeting, the physical person responsible for the internal information system will document it as follows, with the consent of the informant:

- by recording the conversation in a safe, durable and accessible format or through a complete and accurate transcript of the conversation. In the case of communications or complaints in person by means of a meeting:
 - The informant may attend accompanied, if he wishes, by a lawyer or a representative of the workers.
 - To ensure the proper confidentiality of the investigation, those attending this meeting shall be informed in writing of their duty of secrecy and confidentiality, as well as of all legal information relating to data protection.
- The transcript shall be signed by those present at the meeting. Without prejudice to the rights of the informant in accordance with the data protection regulations, you will be given the opportunity to check, rectify and accept the transcript of the conversation by your signature. If, for any reason, the informant or any of those present does not wish to sign the minutes, the minutes shall be recorded and the proceedings shall continue.

Finally, the recording or transcription of the conversation will be attached to the application of the Channel and/or the file associated with the communication and will continue the processing of the communication as set out in the following paragraphs.

Notwithstanding the above, in cases where the entity operates in jurisdictions other than those of the Member States of the European Union, the processing of communications or

verbal complaints shall be in accordance with, in addition to the aforementioned Spanish European and domestic legislation, the local legislation in force in the field of the protection of informants, the protection of personal data, industrial relations and any other sectoral rules which result from application in each territory. To this end, the Head of the Internal Information System, with the support of the relevant local advisers, shall undertake a preliminary analysis of the regulatory framework of each jurisdiction in which the entity carries out its activity, with the aim of identifying specific requirements that could complement, reinforce or, where appropriate, prevail over the provisions contained in this proceeding, applying in any case the highest standard of protection for the informant. Where local legislation establishes additional or divergent obligations over those provided for in Law 2/2023, Directive (EU) 2019/1937 or European data protection rules, the necessary organisational and technical measures shall be taken to ensure simultaneous compliance with all applicable regulatory frameworks, documenting such adaptations and incorporating them as specific annexes to this procedure.

6.4. FORMAL ANALYSIS OF THE COMMUNICATION

Once the communication or complaint has been registered, a preliminary assessment of the facts communicated and the formal elements of the complaint shall be made.

Prior to the decision to allow the complaint to be processed, additional information may be sought for prior assessment. If such information is to be provided by the informant, the informant shall have a period of three (3) working days from the time it is required to do so. Such communication shall take place through the tool or by any other means allowing the processing to be recorded.

Depending on the subject matter of the communication, a prior assessment of the communication may be requested from other areas of the Organization in cases where it considers it appropriate.

If, after the prior assessment, it is considered that the communication is related to matters regulated through specific procedures, the informant shall be acknowledged to receive the communication and shall forward it to the person responsible in these cases. Thus, these communications will be processed in accordance with the provisions of the aforementioned protocols or procedures which, in any case, will have the guarantees and deadlines provided for in Law 2/2023 or in any other regulation that results from application, depending on the jurisdiction affected by the alleged communication.

Access to information for the prior assessment of a communication or complaint shall entail the signature of the corresponding confidentiality commitment and declaration of absence of conflict of interest by all persons accessing it, which in any case shall be the minimum necessary to carry out such assessment.

Once the communication is categorized, it will be carefully analyzed and it will be verified that it contains all the fields necessary for the corresponding investigation to be started.

Otherwise, or if the communication has any defect that prevents its proper processing, a request for a request for information will be made to the informant through the tool. In the case of cases in which a judicial decision or administrative file is pending, the communication shall be suspended, without prejudice to the investigation of the facts raised therein and the issuance of relevant generic recommendations.

6.5. ADMISSION TO COMMUNICATION

On the basis of the previous assessment made, a decision shall be taken on the admission or inadmissibility of the communication or complaint. The decision of admission or inadmissibility to process shall be notified to the informant and recorded in the Channel support tool.

The Internal Information System Manager of the Amper Group ensures the proper processing of communications received that will be analyzed and treated with the utmost confidentiality and confidentiality. In this way, the identity of the informant will only be known to the responsible person or instructor who would have been appointed. No right of full access to the file and, in particular, to the initial communication or to any documents from which the identity of the informant may be suspected or disclosed shall be granted, unless required by law and/or by law.

Once the communication has been analyzed, the System Manager will decide on the admission or inadmissibility of the communication.

Inadmissibility of communication, information or complaint shall be exercised in the following cases:

- When the facts reported are not covered by the objective scope of the policy and procedure of the internal information system.
- When the facts reported are not credible.
- When communication, information or complaint is manifestly unfounded because it does not meet the minimum requirements for its processing, or when there are reasonable indications that the evidence was obtained through the commission of an offence.
- When communication, information or complaint does not contain new and significant information on violations compared to a previous communication in respect of which the corresponding procedures have been concluded, unless new factual or legal circumstances exist that justify a different follow-up.
- When the loss of the object of the communication, information or complaint occurs because the cause of the communication has been remedied prior to its admission to the proceedings.

- When the information is already fully available to the public or constitutes mere rumors.
- When there is subjective incompetence of the channel to know the facts communicated in the terms established in the Policy and Procedure of the Internal Information System.

If communication is not admissible, the reasons shall be succinct and the informant shall be informed as soon as possible by informing him of his inadmissibility.

The person who has made the complaint, additional information or clarifications may be requested when deemed necessary in order to conduct the admissibility analysis or the investigation itself.

In the event of admission to proceedings, the decision shall be communicated to the informant by means established to maintain communication with the informant. If this is not technically possible, the decision shall be communicated by another form of alternative communication provided. Following that decision, the Ethics Committee shall be informed of the decision. The Ethics Committee consists of: the Chief Executive Officer, who may delegate to a head of the CEO's Office; the Corporate Financial Director; the Director of Persons and the Legal Director; and a secretary of the Ethics Committee, a position performed by the person Responsible for Compliance Function as set out in the Compliance Policy.

In the event of admission to the complaint, the decision shall be communicated to the informant who identifies and provides any means of communication (e-mail, telephone number, etc.) or through the complaint channel tool, provided that it does not compromise the investigation itself. All of this, unless the person renounced the right to receive notifications. Likewise, the designated channel will be used to allow the receipt of additional information that may be requested from the informant, depending on the case. In addition, if the communication is admitted, the person who has been the subject of a complaint shall be informed by the Head of the System within a maximum period of 15 calendar days from the receipt of the complaint concerning (i) the receipt of the complaint, (ii) the fact of which he is accused in a succinct manner, (iii) the departments and third parties which, if necessary, may be the addressee of the complaint and (iv) how to exercise their rights in the area of data protection, for which purpose it shall be established in the Privacy Policy. However, no communication shall be made to the person concerned if the complaint is not admissible and when, at an early stage of the investigation, it is concluded that there has been no breach or violation by the person concerned.

Finally, if there is a risk that the notification to the complainant would compromise the investigation, that communication may be postponed until the risk is removed.

6.6. RESEARCH PHASE

6.6.1. DESIGNATION OF INSTRUCTOR

The admission to the proceedings of the complaint will result in the opening of the investigation file. Once the complaint has been admitted, the person responsible for the system, or to whom they delegate, shall designate the investigator within five (5) working days and shall require them to initiate the investigation procedure.

In the event of an investigation and prior verification that there is no conflict of interest of the rest of the members of the Ethics Committee confirm, an instructor shall be appointed who may be internal or external, single-person or multi-person, depending on the needs of the case. In addition, the Ethics Committee may take precautionary measures with a view to protecting the informant, preventing further illicit activity, preventing the destruction of evidence and causing serious or irreparable harm. Other persons designated for this purpose (e.g. human resources officers, members of the legal or audit department, external advisers, etc.) may also participate in the investigation where necessary. In situations of harassment, the provisions of the internal regulations that are applicable to the prevention and action in the event of workplace, sexual and/or sex harassment shall be applied. In any event, the System Manager will oversee the management and investigation of communications that are instructed by the former and will provide them with their support, assistance and advice at all times.

6.6.2. GENERAL PRINCIPLES OF INSTRUCTION

Throughout the investigation file, respect for and compliance with the principles and guarantees enshrined in the Internal Information System Policy shall be ensured.

In any case, the instructor will always increase the confidentiality of the persons involved and, especially, of the informant, protecting his identity. In this way, the identity of the informant will only be known to the instructor who would have been appointed. It may not grant the right of full access to the file and to the initial communication or to any other documents from which the identity of the informant may be suspected or disclosed. The right of defense and the right to be presumed innocent and the honor of persons affected by information, complaint or communication shall be guaranteed. The person complained of has the right to know of the actions or omissions attributed to him by means of succinct communication of the facts and to be heard at any time, in such manner as is deemed appropriate to ensure the good end of the case.

and must be informed of the possibility of being assisted by a lawyer. In no case shall you be informed of the identity of the informant or have access to communication.

6.6.3. INSTRUCTION

The Instructor shall carry out all such actions or checks as he deems necessary for the investigation of the facts reported. To this end, the following actions will be carried out, among others:

- **Documentary analysis.** The instructor shall analyses in detail the information and/or documentation provided by the informant, affected person or witnesses. It may also require as much additional information and/or documentation of a professional nature as necessary, always on the basis of criteria of proportionality and reasonableness.
- **Testimonies.** The investigator must give the persons concerned a hearing, including in any case the informant, affected person and witnesses. All of them must be aware of the rights, guarantees and duties of the parties.

Interviews shall be duly documented, either by recording (on request and authorization of the data subject) or by record of the meeting held. In the latter case, the minutes of the rights, guarantees and duties of the parties, signed by all attendees, will be attached.

- **Technical or expert opinions or reports.** At any time during the instructional phase, the instructor may seek an opinion or technical report, both from other AMPER professionals and from outside experts in the field, which shall respect the principles set out in the System Policy. Such external opinions or reports shall be attached to the Research Report.

6.6.4. REPORT

Upon completion of all investigative proceedings and proceedings, the Instructor shall issue an Investigation Report, which shall include, at least:

- Facts reported in the communication or complaint
- Diligencies practiced in the investigation of the file
- Arguments of the person complained of
- Results of the proceedings carried out
- Assessment of the reported facts
- Conclusions

6.6.5. TIME FOR INSTRUCTION

The instruction may not exceed the maximum period of three (3) months from the receipt of the communication. In cases of particular complexity requiring an extension, this period may be extended to three additional (3) months, by decision of the Head of the Internal Information System.

6.7. PROPOSAL FOR RESOLUTION

In the light of the investigation report, the Head of the System shall issue a motion for a resolution containing, at least:

- The filing of the communication or complaint, in the event that, following the appropriate investigation, it is considered that the facts complained of have not been sufficiently established, or that they are not constituting an infringement within the objective scope of the Internal Information System. In this case, and where appropriate, it shall be agreed that the information should be transferred to other areas of the organisation for its management; where the proceedings carried out do not sufficiently demonstrate the commission of the offence: when the person or persons responsible have not been identified; when the infringement has been concluded at any time, that the offence has been prescribed;
- The declaration of non-compliance, in which case the following measures may be taken:
 - or Corrective measures: When the commission of any non-compliance within the scope of this Procedure has been established;
 - or Proposal for the initiation of disciplinary proceedings: When the facts reported show signs of constituting an offence subject to disciplinary sanctions, the person responsible for the internal information system shall inform the Directorate of AMPER or person authorized in the case, where appropriate, the initiation of disciplinary proceedings;
 - or Referral to the supervisory body: Where the facts may be indistinguishable as constituting an offence that may affect the criminal responsibility of the legal person;
 - or Referral of information to the Ministry of Public Prosecution, or equivalent competent authority in the relevant jurisdiction: Where the facts may constitute offences, provided that other fundamental rights are not affected.
 - o Referral of the information to the European Public Prosecutor's Office (or, where it is not competent or outside the EU, to the equivalent competent authority in the relevant jurisdiction): Where the facts affect the financial interests of the European Union, provided that other fundamental rights are not affected.
 - o Referral of information to other competent authorities or bodies, where appropriate, in accordance with current regulations.

Regardless of whether or not the facts of the communication have been established or whether or not there has been any evidence of non-compliance, improvement measures may be agreed upon when, within the framework of the investigation, the advisability of implementing any improvement to prevent future non-compliances is identified.

The report shall be submitted to the decision-making body which may vary depending on the seriousness of the facts and the persons involved. The designated body may be: director of the organisation, the Audit and Control Committee or the Management Board. Once the

case has been collected and examined, it shall take such penalties and/or measures as it deems appropriate in a reasoned manner.

The reports shall be sent to a Book-Register of the information received and of the internal investigations which they have given rise to, guaranteeing, in any case, confidentiality requirements. Such registration shall not be made public and only at the reasoned request of the competent judicial authority, by order, and in the course of and under the supervision of judicial proceedings, the contents of the said registration may be accessed in whole or in part. Personal data relating to the information received and internal investigations shall be kept only for such period as is necessary, in accordance with what is indicated for this purpose both for each applicable regulation and for the operational annexes incorporated into this Procedure.

6.8 COMMUNICATION

During the processing of the file, at least the following communications will be made:

- **Communication to the Informer:** In case of admission to the process of communication, complaint or information, the decision will be communicated to the informant who identifies and provides some means of communication (e-mail, telephone number, platform, etc.) or, through the channel tool, provided that it does not compromise the investigation. The latter may be informed of the final decision. All of this, unless the person renounced the right to receive notifications. It shall be understood that he has resigned when attempting to contact AMPER without success.
- **Communication to the respondent:** Whoever has been the subject of a complaint, provided that he is admitted, shall be informed by the System Manager, or the person to whom he delegates, within a maximum period of fifteen (15) calendar days from the receipt of the complaint about (i) the receipt of the complaint, (ii) the fact that he is accused in a succinct manner, (iii) how to exercise his rights in the area of data protection, for which he shall apply the provisions of this Procedure and the Privacy Policy. The latter may be informed of the final decision.

7. INTEREST CONFLICT MANAGEMENT

There is a conflict of interest when the objectivity of the person making decisions on a communication is compromised by his/her relationship with the informant, with the respondent, with the persons concerned or with the facts.

In the event that the complaint was directed against the Head of the System, or there was a conflict of interest between them or any other persons who have to intervene in the processing of the file, they shall refrain from intervening in the processing and resolution of the file (except where appropriate in their capacity as a complaint), and shall inform the

rest of the members of the Ethics Committee or, alternatively, the Secretary of the Board of Directors).

The conflict of interest may be:

- **Direct**, when the complaint is made.
- **Indirect**, when, without being the person complained of, objectivity is at risk of being compromised by other reasons, such as:
 - The existence of a close personal relationship or family connection with the person reported.
 - A clear friendship or hostility toward the reporting person or the person reported, or, where there is more than one, toward any of them.
 - A connection through marriage, a relationship similar to marriage, or a family relationship with the reporting person or the person reported, or, where there is more than one, with any of them.
 - The presence of personal interests (e.g., financial interests or career-development interests) that could be affected by the investigation of the reported facts.
 - The existence of indirect responsibility (e.g., due to inaction) in relation to the reported facts.
 - A direct reporting-line or team relationship with the reporting person or the person reported.

In this case, the information relating to the file shall be restricted to the person involved in the conflict of interest. In any event, the provisions of the internal rules on conflicts of interest shall apply.

8. REGISTRATION OF COMMUNICATIONS

The Head of the Internal Information System shall maintain an up-to-date register, preferably in digital format, with the communications made and the procedures followed in connection with them.

The persons authorized to manage the Internal Information System may record, in the Canal management tool, the information received and the internal investigations that have resulted in ensuring compliance with the requirements defined by each regulatory framework that may result from application.

9. DATA PROTECTION

The data provided through the means of communication enabled shall be processed by guaranteeing the confidentiality of the information received and only those persons who have been designated to carry out these functions shall have access to it. However, access by

other persons, or even their communication to third parties, shall be lawful where necessary for disciplinary action to be taken, or upon request of the judicial authority, prosecutor or administrative authority competent in the context of a criminal, disciplinary or sanctioning investigation.

In such cases, the informant shall be informed of this before revealing his identity, unless such information could compromise the investigation or judicial proceedings or if the decision of a Court, Court or Authority is made otherwise.

The necessary measures shall be taken to preserve the identity and to ensure the confidentiality of the data relating to the persons concerned by the information provided. The data shall be kept in the information system for a maximum of 3 months thereafter, and may be retained only for the purpose of providing evidence of the operation of the crime prevention model and of exercising or defending legal action.

In no case shall personal data which are not necessary for the knowledge and investigation of the actions or omissions referred to in this procedure be processed and, where appropriate, immediately deleted.

In addition, all personal data that may have been communicated and that relate to conduct that is not covered by the law shall be deleted.

If the information received contains personal data included in the special categories of data, it shall be deleted immediately, without registration and processing. Information on files that have been archived without investigation may only be kept anonymously. AMPER S.A. as parent company of the Amper Group and entity to which the Head of the Internal Information System belongs, will be considered as responsible for the processing of personal data derived from the use of the internal information system and the processing of internal investigations.

Your identification data are as follows:

- Name: AMPER S.A.
- CIF: A28079226
- Address: calle Virgilio, 2, edificio 4, Pozuelo de Alarcón (28223) Madrid.
- E-mail: protecciondedatos@grupoamper.com

If you would like to know more about the processing of your data and your rights recognised in the European Data Protection Regulation, please consult our Privacy Policy on our website <https://www.grupoamper.com>

In relation to the processing of personal data carried out within the framework of the Internal Information System, the Amper Group will at all times apply the data protection

rules that result from application in the relevant territory and each specific data stream (including, where appropriate, rules with extraterritorial scope), without prejudice to maintaining the European standard — Regulation (EU) 2016/679 and its development rules — as a reference framework for the design of controls, risk assessment and the adoption of technical and organisational measures. When several schemes are in place, the specific requirements of the applicable legislation will be implemented and, in addition, efforts will be made to align the treatments with the principles and safeguards of the European standard to the extent that they are compatible with local government.

10. EFFECTIVE DATE AND AMENDMENTS TO THE POLICY

The Internal Information System procedure shall enter into force on the day following its approval by the Board of Directors of AMPER.

This Procedure shall, in its interpretation and application, be in accordance with the following elements:

- i. Directive (EU) 2019/1937, Law 2/2023 and other implementing legislation;
- ii. The doctrine and jurisprudence of the Court of Justice of the European Union and the national courts;
- iii. Circulars, reports or guides issued by the Independent Information Protection Authority (A.A.I.) or by equivalent authorities according to the jurisdiction in which the Panel operates
- iv. The interpretative criteria which, within the framework of the above, will be set by the compliance body of AMPER.

This Procedure shall be reviewed in the event of any possible improvements or changes in regulations, organizational changes or any other justification. T

he update of this procedure was approved by the Chief Executive Officer of AMPER S.A. on 13 May 2026.

11. VERSION CONTROL

This document will be updated to the established periodicity and whenever significant changes occur. In addition, it must always be in conformity with the relevant provisions in force.

Version	Summary of changes	Date
1.0	Initial version	14/02/2020
2.0	Modification consists of the creation of a complaint form, thus eliminating the communication of complaints through an email address. An e-mail address of the Ethics Committee was also created.	14/06/2022
3.0	Amendment in April 2023, following the adoption of Law 2/2023 of 20 February, regulating the protection of persons reporting on normative violations and the fight against corruption. This amendment consists of the adaptation of the internal complaint channel established in accordance with the legal requirements.	04/2024
4.0	Review after the appointment of the Head of the Internal Information Systems in accordance with Law 2/2023 of 20 February, regulating the protection of persons who report normative violations and the fight against corruption and the review of the procedure. Update of the means by which a complaint can be lodged Update of paragraph 4 following the appointment of the Head of the Internal Information Systems. - Adaptation of paragraph 6 in the area of data protection.	30/01/2025
5.0	Review of the procedure after the appointment of the Ethics Committee as Head of the Internal Information System and inclusion of the following sections: scope of application, competences and responsibilities, conflict of interest management.	28/04/2026