REGULATION ON THE WHISTLEBLOWING CHANNEL

0. Introduction

The Regulation on the Whistleblowing Channel (hereinafter, the "**Regulation**") regulate the management and processing of communications received through the Whistleblowing System and the Protection of the Whistleblower (hereinafter, indistinctly, "**Whistleblowing System**" or "**System**") of Tubos Reunidos Group and all the companies comprising it[1] (hereinafter, the "Group", "TR Group") as a mechanism for receiving queries and information on breaches of the Code of Ethical Conduct and/or the Law.

The Management of Tubos Reunidos Group (hereinafter, the "Group" or "TR Group"), has developed a set of regulations in order to establish the guidelines, principles, guarantees and actions to be followed for the management of information received through the Whistleblowing Channel of the TR Group. The Regulation is an essential part of the Whistleblowing System.

1. Purposes

The Regulation on the Whistleblowing Channel define the guidelines and protocol to be followed by the Whistleblowing System Manager in the event of a Query or Complaint. Thus, the Regulation:

- Delimit the scope of the Whistleblowing System, both objectively and subjectively,
- Provide guidelines for action in the event of a Complaint or Query, establishing an appropriate guide for the management of such complaints or queries in terms of their analysis, internal investigation and resolution, and
- Provide the guidelines to be followed for the correct processing, investigation and resolution of the Complaints and Queries received.

2. Scope

2.1. Objective Scope

In accordance with the Corporate Policy on the Whistleblowing System and Protection of the Whistleblower, Staff and Third Parties may report knowledge or reasonable suspicion of breaches of the Code of Ethical Conduct or that may involve a breach of current legislation. In addition, the Whistleblowing Channel may also be used to raise doubts or queries in this regard.

The following issues should be reported through the Whistleblowing Channel:

- any suspicious fact, behaviour, action or activity within the organisation, regardless of its amount, which by its nature may constitute a breach of the Law, including in any case offences that may have criminal implications and in particular those that give rise to criminal liability for legal persons (public or private corruption, accounting and tax offences, fraud, urban planning or environmental offences, etc.) and/or which, in general, may constitute a breach of the current Tubos Reunidos Code of Ethical Conduct;
- Breaches of the TR Group's Criminal Liability Prevention Model or of any internal rules on ethics and compliance;
- Any other type of infringement that may involve criminal liability for the TR Group;

[1] Tubos Reunidos Group consists of Tubos Reunidos, S.A., as parent company, and the following companies: Tubos Reunidos Group, S.L.U., RDT, Inc., Tubos Reunidos Premium Threads, S.L., Tubos Reunidos Services, S.L.U., Tubos Reunidos América, Inc., CLIMA, S.A.U. and Aplicaciones Tubulares, S.L.U.; as well as all those in which the holding company holds at least 50% of the share capital.

- Acts or conduct that may have criminal implications;
- Serious or very serious administrative infringements;
- Infringements of labour law in the field of health and safety at work or against the Social Security or Tax Authorities; and
- Infringements of European Union law falling within the material scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law and the Spanish transposition act.

The Whistleblowing Channel is set up as the **sole channel for receiving information on breaches of the Code of Ethical Conduct and/or the Law**, and integrates all whistleblowing channels that may be established within the Company. All reports of workplace, sexual and/or gender-based harassment must be received through the Whistleblowing Channel and shall be processed in accordance with this Regulation on the Whistleblowing Channel and with the provisions of the applicable Harassment Protocol, and in all cases shall be subject to the guarantees and deadlines set forth in these Regulation.

The Whistleblowing Channel is reserved for consulting and/or reporting ethical breaches (understood as breaches of the Code of Ethical Conduct) and/or legal breaches (understood as breaches of administrative and/or criminal laws) and **is not set up as a means for communicating any conflict within the organisation.** Likewise, the **communication of matters relating to the interpretation of the Collective Bargaining Agreement in force falls outside this scope.**

Infringements of labour law in the area of health and safety at work and infringements involving financial loss to the Treasury or Social Security system are always considered to constitute a serious or very serious criminal or administrative offence and must therefore be reported and handled through the Whistleblowing System.

Any communications, provided they have been made in good faith and fall within the objective scope of the Regulation, shall, during the investigation process, benefit from the safeguards and guarantees of the Whistleblowing System.

2.2. Subjective Scope

A. The following persons may submit complaints and queries through the Whistleblowing Channel:
   - Employees,
   - Staff made available by Temporary Employment Agencies,
   - Trainees and trainee staff,
   - Volunteers,
   - Candidates who are in a selection process,
   - Former employees,
   - Legal representatives of workers,
   - Members of the administrative, management and supervisory bodies of the TR Group.

   All of them, hereinafter referred to as "**Staff**" of the TR Group. In any case, employees, interns and volunteers are reminded that they have a legal obligation to report in the event that they detect an infringement.

B. The following will also be able to lodge complaints and queries:
   - Shareholders or partners of the TR Group,
   - External collaborators, natural or legal persons,
   - Any person working for, or under the supervision or direction of, a customer, supplier, contractor or subcontractor of the TR Group.

   Hereinafter referred to as "**Third Parties**".

3. Means for submitting complaints and queries

What are the channels of communication for a complaint/query?

Below is a description of the channels of communication for complaints and/or queries available to the TR Group in relation to the matters described in section 2.1:

- **Whistleblowing Channel ("Channel"):** system for receiving information through which any infringement or query must be reported to the System Manager. It is available on the Group's website and at the date of publication of this regulation, it is the following email address:

  canaletico@tubosreunidosgroup.com.

- **Whistleblowing Hotline**: TR Group provides a telephone number through which any complaint or query may be communicated by means of a call, audio or message. The telephone number is available on the Group's website and at the date of publication of this regulation is as follows:

  667 412 930

- **Face-to-face meeting**: it is also possible to report any infringement verbally, by means of a request by the whistleblower for a face-to-face meeting with the Whistleblowing System Manager.

How do I file a complaint/query?

A. **COMPLAINTS:**

The submission of the complaint must comply with the following **formal** requirements:

- Reason for the complaint: detailed description of the facts or circumstances which, in the whistleblower's opinion, constitute a breach of the Code of Conduct or the Law.
- Possible persons involved (if known): name and surname(s), as well as any other data known and considered relevant to the identification of the alleged offender.
- Where appropriate, specific evidence to support the complaint: all documents available to support the belief that the offence described in the grounds for the complaint has been committed.
- Place and date.
- Acceptance of the Principles and Guarantees of the TR Group Whistleblowing Channel.

In addition, in cases where the report is not anonymous, only such information as necessary to identify the whistleblower will be requested.

In addition, the complaint must meet the following **material** requirements:

- Be made in good faith and relate to true facts, notwithstanding any inaccuracies or omissions that may be unintentionally made by the whistleblower.
- Deal with facts falling within the scope of the Whistleblowing Channel.
- Be submitted by Staff and/or Third Parties.

B. **QUERIES:**

The Whistleblowing Channel will receive and process queries or doubts relating exclusively to the TR Group's Code of Ethical Conduct, including queries regarding situations of potential conflict of interest, in accordance with the same. Queries must be made in good faith and contain, at least:

- Identification of the person making the query.
- Type of query that is going to be made:

1. Doubt or query about the Code of Ethical Conduct: Possible interpretations of the same, clarifications, doubts about situations such as the acceptance of gifts, or
2. Query about potential conflict of interest.

- Description of the query, detailing the reasons for the same.

4. Whistleblowing System Manager.

The Management Body of the TR Group, as the body responsible for the Whistleblowing System, has designated the Secretary of the Board and Chairman of the IMB as the natural person responsible for the System (hereinafter, the "**System Manager"**).

The System Manager must carry out his or her functions independently and autonomously from the rest of the entity's bodies, and may not receive instructions of any kind in the exercise thereof. Likewise, he/she must have all the necessary means to carry out the functions entrusted to him/her.
The powers and responsibilities attributed to this figure are detailed below:

- It is the responsibility of the System Manager to ensure the confidentiality of the identity of the person who uses the Whistleblowing Channel and chooses to identify him/herself. The identity of the whistleblower who identifies himself/herself shall not be disclosed to the reported person without his/her consent, without prejudice to the provisions of the previous section.
- The System Manager shall endeavour to maintain a secure means of communication with the whistleblower, using the Whistleblowing Channel or any other means that may be made available for this purpose depending on the circumstances.
- The System Manager shall ensure that the handling, investigation and resolution of complaints or enquiries is carried out in accordance with the law and the principles of the Policy, acting with full independence and impartiality.
- The System Manager shall report regularly to the Board of Directors, at least annually, although he/she is free to call a meeting of the Board of Directors to deal with this matter whenever necessary. The System Manager shall periodically report any information required on the operation and management of the System, preserving in all cases the confidentiality and security of the information, as well as the other guarantees and rights of users established in this Regulation.
- The System Manager shall keep the Register Book up to date with the information on the communications received.
- The System Manager shall ensure that the deadlines established for the handling, processing and filing of complaints and/or communications received are met.
- The System Manager shall ensure that acts constituting retaliation, including threats of retaliation and attempts of retaliation against persons making a communication under this Regulation are prohibited.

In order to carry out the ordinary functions deriving from the Whistleblowing System, the System Manager may rely on additional human and material resources, provided that compliance with the principles set out in the Corporate Policy on the Whistleblowing System and the Protection of the Whistleblower is guaranteed, especially the duties of confidentiality and secrecy. When so deemed by the System Manager, he/she may be supported by the Secretary of the Independent Monitoring Body (IMB), by internal areas of the Group such as Human Resources or Legal Counsel, as well as by any other figure he/she deems appropriate.
Without prejudice to the foregoing, any person in the TR Group, individually or collectively, has the duty to collaborate with the System Manager under the terms of this Regulation for the management of the Whistleblowing Channel.
Both the appointment and the removal of the System Manager shall be notified to the Independent Authority for Whistleblower Protection (AAI), or, where appropriate, to the competent authorities or bodies of the autonomous communities, within the following ten (10) business days.

5. Processing of queries and complaints. Guarantees.

A. COMPLAINTS

5.1 Receipt and registration of the complaint

The **System Manager** shall be responsible for receiving complaints made through the Whistleblowing Channel, as well as any other communication of breaches that fall within the scope of the Whistleblowing Channel.
Once the complaint has been reported, the System Manager will register it and assign it a correlative identification code.
The submission of a report shall generate an acknowledgement of receipt, which must be sent to the whistleblower within seven (7) calendar days of receipt of the complaint, unless this could jeopardise the confidentiality of the information. By sending the acknowledgement of receipt, the whistleblower shall be informed of the receipt of the complaint and the registration number given to the same.
Personal data provided through the Whistleblowing Channel will be processed by the TR Group for the management of the communication received through the Whistleblowing Channel and for the performance of any investigation actions necessary to determine the existence, if applicable, of the facts reported in the complaint. Any personal data collected will be processed in full compliance with the applicable data protection regulations and the **Whistleblowing Channel Privacy Policy**, which is attached as **Annex I** to the Regulation.

Special features of face-to-face complaints
Complaints made through a face-to-face meeting with the System Manager will be documented by recording (if the whistleblower gives permission) or through a complete and accurate transcript of the conversation. At this meeting:

- The whistleblower may be accompanied, if he/she so wishes, by a lawyer or an employee representative.
- To ensure due confidentiality of the investigation, attendees will be informed, in writing, of their duty of secrecy and confidentiality, as well as of all legal information on Data Protection.
- The transcript shall be signed by those present at the meeting. If for any reason the whistleblower or any of those present do not wish to sign the minutes, it shall be so recorded and the investigation shall continue.

Finally, the recording or transcript of the conversation will be attached to the Channel Record Book and the investigation file will continue as set out in the following sections.

5.2 Admissibility

Decision on admissibility or inadmissibility
Once the complaint has been registered, a preliminary analysis of the facts reported and the formal elements of the complaint must be carried out by the System Manager.
If, after such analysis and assessment, the complaint does not meet the minimum requirements for processing by the Whistleblowing Channel, it will not be admitted for processing and the whistleblower will be informed of this circumstance.
The decision to admit or, as the case may be, reject the complaint must be reasoned and communicated to the whistleblower.

Information to affected parties

- **Communication to the whistleblower**: if the complaint is accepted for processing, the decision will be communicated to the whistleblower who identifies himself/herself and provides some means of communication (e-mail, telephone number, etc.) within seven (7) calendar days or the shortest possible time, provided that this does not jeopardise the investigation itself.
  The possibility to **maintain communication with the whistleblower** and, if deemed necessary, to request additional information from the same, is explicitly foreseen.

- **Communication to the reported person**: likewise, the person who has been the subject of the complaint, provided it is admitted, shall be informed by the System Manager of the receipt of the complaint, of its admission for processing, and of the fact of which he/she is accused in a succinct manner (including the actions or omissions attributed to him/her, and his/her right to be heard within a maximum period of one month from its receipt. However, it will be necessary to assess, on a case-by-case basis, whether informing the same of the lodging of the complaint within such deadline could jeopardise the proper conduct and success of the investigation. In this case, if it is decided not to inform the person concerned at the initial stage of the investigation, this decision shall be duly documented and justified.

Whistleblowers shall be expressly informed that their identity will in any case remain confidential. Under no circumstances shall the person complained against be informed of the identity of the whistleblower.

5.3 Examination of the complaint

5.3.1 Opening of the file and appointment of the examiner

Upon the System Manager's decision to open a file, the examination of the complaint submitted shall begin, carrying out all those actions and queries as deemed necessary for the purpose of ascertaining the accuracy and truthfulness of the information received, as well as aimed at clarifying the facts, with full respect for the presumption of innocence and the honour of the persons affected.
The System Manager shall, as a general rule, be the Examiner. However, when there are well-founded reasons for doing so and in view of the nature and seriousness of the complaint, the System Manager may delegate the examination of the complaint to an **external expert** to collaborate in the investigation and analysis of the documentation and evidence obtained.

Likewise, the System Manager may be assisted by the Secretary of the IMB in the management and processing of files opened as a result of consultations and/or complaints.
However, the System Manager shall supervise the management and investigation of complaints that he or she does not directly handle, and shall at all times provide support, assistance and advice to them.

5.3.2 Investigation of the alleged facts

For the investigation and study of the relevant complaint, appropriate persons and internal or external means available shall be designated and used, always respecting the fundamental rights of the whistleblower. Likewise, all information and documentation that the System Manager considers appropriate at any given time for the investigation of the complaint may be requested from the whistleblower, the reported person or other employees. All directors, officers or employees of the TR Group have the duty to cooperate in good faith in the investigation.

Likewise, due confidentiality shall be maintained of the identity of the subjects involved and, most especially, of the whistleblower, protecting their identity at all times in order to avoid leaks. Thus, only the System Manager and the person who directly deals with it may access the data, the head of Human Resources or the duly designated competent body, only when disciplinary measures may be taken against an employee, the head of Legal Counsel only when legal measures may be taken, and the persons in charge of the processing of personal data that may be designated by the System Manager.

In no case shall the right of full access to the file and, in particular, to the initial communication or to any documents from which suspicion or disclosure of the identity of the whistleblower may arise be granted. Thus, the identity of the whistleblower shall be known only to the designated investigating team.

Thus, save for such exceptions as provided for by law, the identity of the whistleblower shall not be provided to any third party. So, the whistleblower's identity may only be provided to the judicial authority, the Public Prosecutor's Office or the competent administrative authority, within the framework of a criminal, disciplinary or sanctioning investigation. In addition, TR Group persons who, due to their functions, may have access to and knowledge of the reports submitted and the identity of the whistleblowers, have the duty to maintain due confidentiality and professional secrecy, both with regard to the identity of the whistleblower and the content of the report.

5.3.3 Issuing the Report

Once all the proceedings have been concluded, the Examiner shall issue an Investigation Report with the procedures carried out, which shall be delivered to the System Manager, unless the latter has been designated as the File Examiner.

This report will include:

- Facts of the complaint
- Evidence taken in the investigation of the case.
- Results of the proceedings.
- Allegations by the reported person.
- Assessment of the alleged facts.

The System Manager, in view of the Report derived from the investigation, shall draw up and issue a **Resolution** regarding the complaint made, in which he/she shall decide on:

a. **The dismissal of the complaint**. The System Manager shall close the complaint and the actions carried out when, after the appropriate investigation, he/she considers that the facts reported have not been sufficiently proven, or that they do not constitute an infringement included in the objective scope of the Whistleblowing Channel, or
b. **The proposal of the disciplinary measures to be adopted**. When the facts reported have been sufficiently proven and, furthermore, constitute an infringement included in the objective scope of the Whistleblowing Channel, the System Manager will:
    - Prepare a Resolution in writing, duly justified, including potential disciplinary measures to be taken depending on the seriousness of the infringement.
    - Forward the complaint, the documented results of the investigation and the Resolution to the TR Group's Human Resources Department, if disciplinary action is necessary; to the Legal Counsel, if legal action is necessary; and/or to the department in charge of handling the response action in the event that the reported person is external to the Organisation, and

c. **Measures for the protection of the whistleblower**: When the alleged facts have been proven and constitute any of the offences included in the objective scope of Act 2/2023, the System Manager will promote the application of the measures for the protection of the whistleblower enforced during the process of processing the complaint, taking into account the circumstances of each specific case.

The System Manager shall immediately forward the information relating to a complaint and its relevant file to the Public Prosecutor's Office when the facts that he/she considers proven in the investigation could be indicative of a criminal offence.

In any case, the System Manager shall inform those making the communication through the Whistleblowing Channel, in a clear and accessible manner, of the existence of the external information channels before the competent authorities and, where appropriate, before the institutions, bodies or agencies of the European Union.

Complaints in bad faith and those that do not fall within the objective scope of Act 2/2023 will not be covered by the protection measures contained therein.

If the complaint relates to a member of the Board of Directors or of the Executive Committee, the proposed Resolution shall be submitted by the System Manager, prior to its issuance, to the Chairman of the Board of Directors. If the same relates to the Chairman of the Board of Directors, the proposed Resolution shall be submitted through the Secretary to the Appointments and Remuneration Committee of the Board of Directors.

The maximum period for completing the investigation and responding to the investigation proceedings may not exceed three (3) months from the receipt of the communication or, if no acknowledgement of receipt was issued to the whistleblower, three months from the expiry of the seven-day period after the communication was made, except in cases of particular complexity requiring an extension of the period, in which case the period may be extended by up to a maximum of three additional months.

B. QUERIES

5.4. Receipt and registration of the query

The query will be received by the System Manager and, like the complaints, will be assigned a correlative identification code.

The System Manager will analyse whether the query meets the minimum requirements necessary to be processed by this means.

5.5. Processing of the query.

The System Manager will analyse the queries received and, in case of doubt, will refer them to the Independent Monitoring Body (IMB) for a response.

5.6 Resolution of the query

With regard to the queries received, the System Manager shall issue and forward the resolution adopted to the persons concerned. Such resolutions may lead to improvements in the Code of Ethical Conduct, in order to keep it up to date and to improve its content and proper understanding.

5.7. Powers of the Examiner.

The Examiner formally appointed by the System Manager, provided that the applicable legislation so permits, shall have access to and may obtain from each of the departments, offices, directors, managers, employees and companies of the TR Group all the information and documentation necessary for the proper performance of his or her duties.

The Examiner, whether internal or external, and his or her investigating team, if any, shall have access to all premises, offices, files and documents of the organisation, in so far as this is necessary for the investigation and proportionate to its purpose. If necessary for the purposes of the investigation, the investigating officer may order a search of the computers and e-mails of the persons under investigation. The Examiner shall ensure proportionate use of this power.

All directors, officers and employees of the organisation have the duty to respond diligently, fully and truthfully to all questions concerning the performance of their professional activities within the TR Group and to provide such cooperation as may be requested by the Examiner. Intentional or grossly negligent provision of untruthful or incomplete information shall be considered an offence subject to disciplinary action.

In addition, the Examiner may seek the collaboration or advice of external professionals, who shall address their reports to the System Manager.

To the extent possible, and only where this does not affect the effectiveness of his work, the Examiner shall endeavour to act in a transparent manner, informing, where appropriate, the directors and professionals concerned of the subject matter and scope of his investigations.
The System Manager and the Examiner may request information from the other TR Group bodies and personnel on those aspects that are necessary for the exercise of their functions of effective management of the Information System, in particular on the following:

- Financial and accounting situation.
- Status of preventive measures.
- Status of disciplinary files handled by HR, if any.
- Any other affecting the Code of Ethical Conduct or the Prevention Model.

6. Conflict of interest and whistleblower protection

6.1. Conflict of interest

A conflict of interest exists when the objectivity of the person who has to take a decision on the complaint is compromised by his or her relationship with the whistleblower, the reported person, or the reported facts. The conflict of interest may be:

- **Direct**, when such person is the subject of the complaint
- **Indirect,** when, without being the reported person, objectivity is at risk of being compromised for other reasons, such as:
  - The existence of a relationship of affection or kinship with the reported person:
    - Manifest friendship or enmity with the whistleblower or the reported person or, if more than one, with any one of them.
    - Relationship by marriage or similar effective or kinship relationship with the whistleblower or the reported person or, if more than one, with any of them.
  - The presence of personal interests (e.g. financial or career development) that may be compromised by the investigation of the alleged facts.
  - The existence of vicarious liability (e.g. for inaction) in relation to the facts reported.
  - The direct team relationship between the whistleblower and the reported person.

Measures to avoid conflict of interest:

- In the event that the complaint is directed against the System Manager, or if there is any conflict of interest, the System Manager shall abstain from intervening in the processing of the case (except in the event that he/she is the reported person) and it shall be submitted to the Board of Directors for the purpose of deciding internally on its processing and possible sanction, following the procedure established in this Regulation.
- If the System Manager or any of the persons involved in the handling and processing of complaints is likely to incur a conflict of interest upon becoming aware of information related to the objective scope, the complaint shall be addressed by the System Manager to any member of the IMB who is not subject to a conflict of interest, who shall act in accordance with the provisions of this Regulation, assuming the functions of the System Manager that have been defined.
- In those cases in which the complaint is directed against a member of the Executive Committee, the System Manager shall have external advice for the processing and resolution of the case, following the procedure established in this Regulation.
- In those cases in which the complaint is directed against a member of the Board of Directors, the System Manager shall have external advice for the processing and resolution of the case, following the procedure established in this Regulation.

6.2. Whistleblower protection

Acts constituting retaliation, including threats of retaliation and attempts of retaliation against persons who make a bona fide communication as provided for in this Regulation and comply with the conditions set out in this Regulation, are expressly prohibited.
However, the prohibition of retaliation shall not preclude appropriate disciplinary action where the internal investigation establishes that the allegation is false, and that the person who made the allegation was aware of its falsity and acted in bad faith.

The conditions, measures and deadlines for the protection of whistleblowers against retaliation are regulated in the **Non-Retaliation Protocol** (Annex II to this Regulation).

7. Data protection

TR Group undertakes to treat at all times the personal data received through the Whistleblowing Channel as absolutely confidential and in accordance with the purposes set out in this Regulation, and will adopt the necessary technical and organisational measures to guarantee the security of the data and avoid its alteration, loss, unauthorised processing or access, taking into account the provisions of the legislation on the protection of personal data.

The specifications regarding the processing and protection of personal data received through the Whistleblowing Channel are set out in **Annex I - Whistleblowing Channel Privacy Policy** of the Regulation.

8. Adoption, publication and entry into force

This Regulation was approved by the Board of Directors of Tubos Reunidos S.A. on 25 May 2023 for application to the entire Tubos Reunidos Group.
The Board of Directors promotes and approves this Regulation in compliance with its duty to establish the necessary bases for an adequate and efficient management of the Whistleblowing System and to promote compliance with the principles and guarantees set out in the Corporate Policy on the Whistleblowing System and the Protection of the Whistleblower.

This Regulation shall be published on TR Group's corporate website and intranet. In addition, they will be sent to the TR Group Staff and communicated, to the extent applicable, to those Third Parties with which the TR Group has relations.

This Regulation shall be reviewed, updated, approved and disseminated on a regular basis and whenever it becomes necessary to make any amendments.

ANNEX I.- WHISTLEBLOWING CHANNEL PRIVACY POLICY
ANNEX II.- NON-RETALIATION PROTOCOL.

****

ANNEX I. WHISTLEBLOWING CHANNEL PRIVACY POLICY

1. Purpose

The purpose of this Privacy Policy is to provide information on the processing of personal data for the handling and investigation of complaints or queries submitted through the Whistleblowing Channel of the companies belonging to Tubos Reunidos Group (which forms part of its "Whistleblowing System" or "System").
The System is designed and set up in accordance with the provisions of the applicable regulations on data protection, and in particular:

- 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 (hereinafter referred to as the "General Data Protection Regulation", or "GDPR");
- Special Act 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (*Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, hereinafter, "LOPD");
- Act 2/2023 of 20 February regulating the protection of persons who report regulatory infringements and the fight against corruption; and
- Other European and Spanish implementing legislation that may be applicable.

2. Who is the controller of your personal data if you use the Whistleblowing Channel?

The controller of personal data collected within the framework of the System will be the parent company of Grupo Tubos Reunidos in Spain, Tubos Reunidos S.A., given that it is the company of the Person Responsible for deciding on the admission for processing of any complaint or query, the steps in the investigation procedure, and the closure of the investigation. Further information on the composition of Tubos Reunidos organisation may be found on the corporate website: www.tubosreunidosgroup.com.

In this regard, this Policy applies to Tubos Reunidos Group and to all the companies that comprise it, as well as to all directors, officers, employees or persons who, directly or indirectly, have a relationship with TR Group, regardless of their functional or hierarchical position (hereinafter, the "Staff").

In addition, the scope of application of the System includes any person, natural or legal, who has had, has or may have a professional relationship, or a relationship within the framework of a professional context, with TR Group, including its shareholders (hereinafter, the "Third Parties").

pdatos@tubosreunidosgroup.com is the e-mail address that whistleblowers may use to consult any matter strictly concerning the processing of their personal data, as well as to exercise their data protection rights.

3. What personal data do we collect?

Personal information about the whistleblower and the reported person, as well as about third parties involved in the events that have been the subject of a query or complaint (e.g. potential witnesses), may be processed through the Whistleblowing Channel.

In this respect, it is not possible to define beforehand which categories of personal data will be processed through this communication channel, given that it will depend on the information that any of the parties involved wishes to provide, whether the whistleblower when making the complaint, or the reported persons when defending themselves, or even

potential witnesses participating in any investigation process initiated. In any case, Tubos Reunidos may receive such personal data:

- directly from the data subject (provided at the time of the complaint or query, when making any allegations, or at any other time during the investigation); and

- indirectly, from any of the persons - natural or legal - involved in the investigation; or by Tubos Reunidos companies, when said person works or provides services in -or for- any of them.

In cases in which Tubos Reunidos receives personal information from a data subject indirectly, such data subject will be informed immediately, with an indication of the origin and the categories of data being processed.
Finally, whistleblowers wishing to disclose their identity must provide Tubos Reunidos their current and accurate personal data, so that the information contained in its systems is updated and error-free (in particular, the data through which Tubos Reunidos can contact them for any question related to the information submitted).

4. What types of issues are dealt with or managed in the Whistleblowing Channel?

Communications that should be made through the Whistleblowing Channel include, among others, any knowledge or suspicion of conduct that may involve non-compliance with current legislation and/or Tubos Reunidos' Code of Ethical Conduct. Likewise, the Whistleblowing Channel is also available for raising doubts or queries regarding ethics and compliance.

By way of example, the following matters should be reported:

- Any breach of the Code of Ethical Conduct.
- Non-compliance with Tubos Reunidos' Compliance and Criminal Risk Prevention Model ("Compliance Model") or with any internal regulations on ethics and compliance.
- Acts or conduct that may have criminal implications.
- Serious or very serious administrative infringements.
- Labour law Infringements in the field of health and safety at work, or against social security or tax authorities.
- Infringements of European Union law falling within the material scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law and the Spanish transposition law.

5. For what purpose and on what legal basis do we process personal data?

For legal purposes, it is hereby stated that the processing of the data collected through the System is intended for the following purposes, each of them with their corresponding legitimate basis:

a) **Compliance with Act 2/2023 on Whistleblower Protection.**
Firstly, we will process the information (provided by the whistleblower or collected in the framework of an eventual investigation) in order to (i) manage and investigate the complaints/queries made about potential breaches of our Code of Ethical Conduct or the Law, and (ii) adopt the legally established protection measures to prevent possible retaliation, in strict compliance with the provisions of Act 2/2023, of 20 February, on the Protection of Whistleblowers.

The whistleblower may submit the complaint verbally via the telephone number provided for this purpose, or in a face-to-face meeting. All verbal communications (made in a face-to-face meeting, by telephone or voice message) must be documented in one of the following ways, subject to the whistleblower's consent:

- recording of the conversation in a secure, durable and accessible format, or
- full and accurate transcript of the conversation

The whistleblower shall be given the opportunity to verify, rectify and accept, by signing, the transcript of the conversation.

b) **Attention and response to possible queries, due to the legitimate interest of the person making the query.**
If it is not a complaint but a query, Tubos Reunidos will process the information received in order to attend to, manage and duly respond to it. The above will be carried out based on the legitimate interest of Tubos Reunidos, as a legitimate basis, which does not prejudice or harm the privacy of the person making the query, and also of the latter, who also has a legitimate interest in obtaining a due response.

c) **Prevention of criminal risks, as a Public Interest mission.**
On the other hand, the personal data collected will also be processed for the fulfilment of a mission carried out in the public interest, such as the prevention, detection and discovery of possible risks and breaches that may occur and which may generate criminal liability for any of the Tubos Reunidos entities.

d) **Having evidence of the correct functioning of the Criminal Risk Prevention Model, in the legitimate interest of Tubos Reunidos.**
In addition, personal data may be processed within the framework of this system on the basis of Tubos Reunidos' legitimate interest in having evidence of the correct functioning of its Criminal Risk Prevention Model.
In accordance with the European General Data Protection Regulation 2016/679, and both for that described in this section d) and in section b) above, Tubos Reunidos has drawn up the relevant "balancing test", an internal analysis that confirms the origin and relevance of such legitimate interest.
Tubos Reunidos Group shall keep a confidential, non-public **Register Book** of complaints and queries received, and of the internal investigations to which they give rise, which shall only be handed over to a judge and upon reasoned request.

e) **Other legally binding uses**
Finally, in some cases, personal data may also be processed in order to comply with certain legal obligations that may be imposed on us. Where possible, we will inform you of this and of the applicable law in each case.

6. To which recipients will your personal data be communicated?

As a general rule, Tubos Reunidos shall not transfer the personal data it collects through the system to any third party. Therefore, it may only be accessed by staff who, due to their functions, responsibilities and duties, are duly and previously authorised:

- The System Manager and whoever manages the system directly.
- The Human Resources Manager or the duly designated competent body, only when disciplinary measures against an employee may be appropriate.
- The Legal Counsel, only when legal action may be appropriate.
- The data processors that may be appointed by the System Manager.

If, as a result of the investigation process, it is resolved to adopt legal or disciplinary measures against the reported party, the System Manager shall pass on the strictly necessary information to the Tubos Reunidos company with which the reported party has a contractual relationship (employment, commercial or otherwise), in order to carry out and execute the relevant legal actions.

Personal data may also be provided to third parties where Tubos Reunidos has a legal obligation with such parties: for example, Courts and Tribunals, Security Forces and Bodies or any competent Public Body, upon request.

Likewise, Tubos Reunidos may have the collaboration of third party service providers, who may have access to such personal data and who will process them in their name and on their behalf, as a consequence of the provision of contracted services. In relation to the above, Tubos Reunidos follows strict criteria for the selection of suppliers in order to comply with its data protection obligations. Thus, in order to regulate the conditions of privacy in which these possible third-party suppliers will act, Tubos Reunidos will impose on them, among others, the obligations to apply appropriate technical and organisational measures; to process personal data for the agreed purposes and only in accordance with the documented instructions of Tubos Reunidos; and to delete or return the data once the provision of services has been completed.

The above is indicated because Tubos Reunidos may contract the provision of services with third party suppliers that carry out their activity, by way of example and without limitation, in the following sectors: legal consultancy, multidisciplinary professional services companies, or companies that provide technological or IT services.

In such cases of involvement of a third party supplier, the latter shall:

- strictly and punctually follow the documented instructions given by Tubos Reunidos;
- not use such data for any other purpose;
- implement the necessary security measures - technical and organisational - to ensure the confidentiality of the information to which it has access; and
- not communicate to third parties the data to which it has access, not even for storage purposes.

7. International data transfers

As a general rule, all personal data collected within the framework of the Channel will be stored and processed in the European Union, in strict compliance with the GDPR. However, as Tubos Reunidos is an international group, there is the possibility that in specific situations, data may be processed outside the EU: specifically in the countries listed on its corporate website www.

In these cases, and in order to guarantee in any case the protection of data subjects' data also in such countries, the parent company of Tubos Reunidos will use the appropriate or suitable guarantees (in particular, it will sign the appropriate standard contractual clauses with the international companies of the group).

8. Security and confidentiality measures. Possibility of whistleblower remaining anonymous.

Tubos Reunidos shall ensure that all necessary technical and organisational measures are adopted to preserve the security of the data collected, in order to protect them from potential unauthorised disclosure or access.

In this respect, whistleblowers may decide whether or not to identify themselves when making a complaint. Anonymous reporting is therefore permitted. In any case, maximum confidentiality will be guaranteed as to the identity of the whistleblower who initially or finally wishes to identify himself/herself.

In addition, and as a measure to guarantee the confidentiality of the whistleblower, it is noted that the exercise of the right of access by the reported person will not entail access to the identity of the whistleblower.

The identity of the whistleblower may only be disclosed to the administrative and judicial authorities, where legally appropriate, for the proper handling of any administrative or judicial proceedings that may arise from the complaint lodged. In this regard, it is hereby stated that the identity of the whistleblower will only be known to the persons in charge of managing the System and investigating the complaint, as well as to the areas that are strictly necessary for the investigation of the facts and resolution of the complaints made.

Finally, persons who, by reason of their duties, have knowledge of the complaints made, are personally bound to keep secret all information to which they have access.

9. How long do we keep personal data?

Personal data shall not be collected if their relevance is not obvious. The personal data collected (through the complaint filed and, where appropriate, within the framework of any eventual investigation) may be kept (i) for the time necessary to decide on the appropriateness of initiating an investigation into the reported facts, (ii) where appropriate, for the duration of the relevant investigation and, finally, (iii) for the duration of the exercise of the relevant legal actions. In the case of a simple query, for the time necessary to handle, process and respond to the same.

If it is proven that a complaint or part of it is not truthful, or relates to matters that should not be reported through the Whistleblowing Channel, it will be immediately deleted, unless such lack of truthfulness may constitute a criminal offence. Communications that have not been followed up may only be recorded in the Register Book in an anonymised form.

In any case, after three months have elapsed from the receipt of the complaint without any investigation having been initiated, the complaint shall be deleted, unless the purpose of keeping it is to leave evidence of the operation of the channel.

Finally, and after all of the above, the data collected will be kept in order to comply with eventual legal obligations that may apply, as well as to meet potential claims and liabilities, keeping them duly blocked, and for the statutory maximum periods, at the disposal of the Judiciary and Law Enforcement Bodies, and potential Competent Public Administrations.

As a general rule, personal data relating to complaints and investigations shall not be kept for a period of more than 10 years.

10. How can you exercise your data protection rights?

Individuals whose personal data may be processed in the framework and context of the Reporting System have the following data protection rights:

a) The right to obtain confirmation as to whether or not their personal data are being processed at Tubos Reunidos - within the framework of the management of the System - and to access, rectify, limit the use of their data or, where appropriate, request their erasure, on the terms established by law, when, among other reasons, the data are no longer necessary for the management of the System.

b) In accordance with the provisions of the aforementioned Act 2/2023, in the event that the person to whom the facts described in the communication refer exercises the right of opposition or limitation, it shall be presumed, unless there is evidence to the contrary, that there are compelling legitimate reasons that justify the processing of their personal data.

c) When the affected persons exercise their rights of access, rectification, erasure, opposition, limitation of processing, and the right not to be subject to automated individualised decisions, they must be duly accredited and request this by e-mail to the address pdatos@tubosreunidosgroup.com.

d) Likewise, you may file a complaint with the Spanish Data Protection Agency, especially when you have not obtained satisfaction in the exercise of your rights, through the electronic headquarters at www.aepd.es.

11. Information to the parties involved

The parties involved in the queries or complaints received and/or processed shall be duly informed of the processing carried out with regard to data protection. In order to carry out the above, Tubos Reunidos shall provide the necessary mechanisms to ensure that potential users of the Whistleblowing Channel are aware of and have at their disposal, in a simple, accessible, understandable and, of course, free of charge manner, the aforementioned information on data protection.

Likewise, each time a complaint or query is made, Tubos Reunidos shall inform the persons involved of the collection and subsequent processing of their personal data. However, the manner in which the above is carried out shall be managed on a personalised basis. Thus, in order to reinforce and guarantee compliance with this duty to inform, the following measures shall be taken (depending on whether it is the whistleblower, the reported party or a third party involved):

- Whistleblower: If the whistleblower identifies himself/herself when submitting the complaint, he/she will also be informed of the processing of his/her data in the communication sent to acknowledge receipt of the submission of his/her complaint or query, with a link to this Privacy Policy. Exceptionally, this personalised notification will not be made if the whistleblower has used a common or shared email account, or one that is accessible to more people in the organisation.

- Reported Person: As a general rule, the reported person shall be informed of the lodging of a complaint against him/her within a maximum of one month after its receipt. However, it will be necessary to assess on a case-by-case basis whether informing him/her of the lodging of the complaint against him/her within this time limit could jeopardise the proper conduct and successful outcome of the investigation. In this case, if it is decided not to inform the person concerned at the initial stage of the investigation, such decision shall be duly documented and justified.

- Any other stakeholder involved in the complaint or consultation: Finally, third parties involved in the complaint or query will be informed prior to their participation in the process: for example, a potential witness will be informed prior to his or her interview or statement being taken.

12. Dissemination of the Privacy Policy

This Policy shall be incorporated as an annex to the Whistleblowing Channel Regulation, and it shall be published as part of the same on the corporate website and on the corporate intranet, and shall be reviewed, updated, approved and disseminated from time to time and whenever any changes need to be made.

13. Development, monitoring and control.

The TR Group's Independent Monitoring Body (IMB) in compliance matters is responsible for the development and periodic review of this Policy, supervising its implementation and submitting to the Board of Directors any observations or proposals for modification and improvement that it deems appropriate.

14. Adoption, publication and effectiveness.

At its meeting held on 25 May 2023, the Board of Directors of Tubos Reunidos, S.A. approved this Whistleblowing Channel Privacy Policy, to advance in the adoption of the best Compliance practices. The Policy is an annex and an integral part of Tubos Reunidos Group's Whistleblowing Channel Regulation.

******

ANNEX II. PROTOCOL PROHIBITING RETALIATION

Pursuant to the provisions of Tubos Reunidos Group's Corporate Policy on the Whistleblowing System and the Protection of the Whistleblower (hereinafter, the "**Policy**"), as well as the Whistleblowing Channel Regulation (hereinafter, the "**Regulation**"), Tubos Reunidos Group (hereinafter, "**TR Group"**) will not tolerate retaliation (including threats and attempted retaliation) against any whistleblower for raising a complaint, communication or any concern in good faith, or for cooperating in the investigation of any complaint, and will use its best efforts to prevent, prosecute and punish such conduct.

1. Purpose

The main purpose of this Protocol for the Prohibition of Retaliation (hereinafter the "**Protocol**") is to protect whistleblowers who make a report or complaint through the reporting channels included in the TR Group Whistleblowing System from potential retaliation, including threats of retaliation and attempted retaliation.

The Protocol also establishes a framework of protection and guarantees for whistleblowers within the organisation, which respects the provisions of Act 2/2023 regulating the protection of persons reporting regulatory violations and the fight against corruption (hereinafter **Act 2/2023**), and which can effectively address situations of risk and protect whistleblowers in good faith from retaliation.

2. Scope of application

This Protocol is applicable to and protects against possible reprisals all whistleblowers who report in good faith serious or very serious criminal or administrative offences, according to Spanish law, committed by action or omission within the TR Group organisation, and who do so through the internal (Whistleblowing Channel) or external (External Reporting System) mechanisms regulated in Act 2/2023.

In addition, the protection measures provided for in this Protocol shall also apply to:

- Natural persons who, within the framework of the TR Group organisation, assist the whistleblower in the process.
- Natural persons who are related to the whistleblower and who may suffer reprisals, such as co-workers and family members (ascendants and descendants, spouses or common-law partners, and siblings).
- Legal persons for whom the whistleblower works or with whom he/she has any other type of relationship in an employment context or in which he/she has a significant interest. For these purposes, an interest in the capital or in the voting rights attaching to shares or equity is deemed to be significant when it confers the person holding the same the capacity to influence the legal person in which it has the interest.

3. Concept of retaliation

Acts constituting retaliation against whistleblowers who meet the requirements set out in this Protocol are prohibited. For the purposes of this Protocol, "retaliation" means any act or omission that is prohibited by law, or that directly or indirectly results in unfavourable treatment placing the persons subjected thereto at a particular disadvantage compared with another person in the employment or professional context, solely because of their status as whistleblowers, or because they have made a public disclosure, and provided that such acts or omissions occur during the investigation procedure or within two years of the termination of the investigation procedure or of the date on which the public disclosure was made. An exception shall be made where such act or omission can be objectively justified by a legitimate aim and the means of achieving that aim are necessary and appropriate.

Retaliation includes, but is not limited to, retaliation in the form of:

a. Suspension of the employment contract, dismissal or termination of the employment relationship, or other relationship provided for in the bylaws, including the non-renewal or early termination of a temporary employment contract after the trial period, or early termination or cancellation of contracts for goods or services, or the imposition of any disciplinary measure, demotion or denial of promotion and any other substantial modification of working conditions and the failure to convert a temporary employment contract into a permanent one, in the event that the employee had legitimate expectations that he/she would be offered a permanent job; unless these measures are carried out as part of the regular exercise of the TR Group's management powers under the relevant labour or employee statute legislation, or due to circumstances, facts or breaches that are accredited and unrelated to the submission of the communication;
b. Damage, including reputational damage, or economic loss, coercion, intimidation, harassment or ostracism;
c. Negative evaluation or references regarding work or professional performance;
d. Blacklisting or dissemination of information in a particular sectoral area, which hinders or prevents access to employment or the contracting of works or services;
e. Refusal or revocation of a licence or permit;
f. Refusal of training;
g. Discrimination, or unfavourable or unfair treatment.

4. Retaliation risk assessment

When a communication is received through the Whistleblowing Channel enabled by the TR Group, the risk of eventual retaliation against the whistleblower and other parties involved shall be assessed, by way of example but without limitation, by considering the following assessment criteria established by best practices:

- What is the likelihood that the confidentiality of the whistleblower's identity and/or reported data is ensured?
- Who else has knowledge of the complaint and/or the facts?
- Does the nature of the information reported reveal the identity of the whistleblower?
- Is the whistleblower particularly concerned about retaliation, and is there evidence that retaliation has already been taken or are there immediate threats of retaliation?
- Is the whistleblower involved in the offence or is the offence directed against him/her?
- Does the complaint involve multiple types of violations?
- How did the whistleblower obtain the reported information?
- What is the whistleblower's relationship to the reported subject and to the organisation?

Based on the assessment of the risk of retaliation, strategies and actions to prevent retaliation against the whistleblower and other persons involved will be implemented on a case-by-case basis.

The retaliation risk assessment shall be monitored and reviewed by the System Manager, documenting the results of each reassessment.

5. Measures to protect against retaliation

In order to protect whistleblowers, the System Manager shall apply the protection measures that may be appropriate. In particular, by way of example and without limitation:

- **Anonymity and confidentiality**: whistleblowerd may, at their free choice, identify themselves or submit their complaint anonymously. In any case, it is guaranteed that all reports received will be treated confidentially and in accordance with the data protection regulations in force, protecting both the identity of whistleblowers who wish to identify themselves and the identity of the facts, data and information provided relating to natural and legal persons.

As a measure to guarantee the confidentiality of the identity of whistleblowers who choose to identify themselves, the TR Group expressly states that the whistleblower's identification data are not included in the scope of the right of access that can be exercised by the reported person. Therefore, as a general rule, the identity of the whistleblower will not be known.

Likewise, all persons who, by reason of the functions they perform, have knowledge of the communications that are made, are obliged to maintain professional secrecy regarding the identity of the whistleblower and any information or data to which they have access, and failure to comply with this duty is a very serious infringement.

- **Development of training and communication actions** on protection measures against retaliation aimed at TR Group employees and its third parties.

- **Prohibition of retaliation** against the person reporting in good faith, such as dismissal, non-renewal, early termination of the employment relationship, reputational or economic damage, performance evaluations that are not commensurate with the work performed, among others.

- **Regular monitoring of the whistleblower's situation:** the System Manager will monitor the working conditions of whistleblowers who form part of the Staff and meet the conditions for protection against retaliation. To this end, the System Manager will hold regular meetings with them to gain first-hand knowledge of their employment situation, requesting, where appropriate, any documentation deemed necessary during the processing of the complaint and, especially, after it has been filed, in order to verify that there has not been any condition or behaviour that could entail retaliation.

Where appropriate, temporary or permanent measures to protect the reporting person (e.g. physical change of workplace or location, change of area/department or change of job, change of supervisor or manager, change of reporting line, etc.) should be considered.

If it is found that retaliation has indeed taken place against the whistleblower or other persons involved, in addition to taking appropriate disciplinary action against the perpetrators of such reprisals, the necessary and available measures shall be taken to restore the whistleblower to the situation prior to the harm suffered (e.g. restoration of the employee to his/her original job/salary/responsibilities; access to internal promotion/training/benefits and rights denied; offer of apologies; compensation for damages; etc.).

For the development of the aforementioned actions, the System Manager will also be supported by the Secretary of the IMB.

If the whistleblower is a **Third Party**, to the extent applicable, the System Manager will monitor the business relationship, if any, with the reporting third party to ensure that there is no retaliation, such as early termination or cancellation of contracts.

Any person who, while falling within the scope of this Protocol and meeting the conditions for protection, suffers retaliation, threats of retaliation or attempted retaliation as a result of reporting a complaint through the Whistleblowing System, shall be entitled to seek protection from the competent Authorities, in addition to the protection of the TR Group.

The System Manager shall record the actions taken as part of his or her regular monitoring function, as well as the results obtained.

6. Conditions for protection

Subjects covered by the scope of application of this Protocol who report offences shall be subject to the protection regime provided for in this Regulation provided that:

a. The communication or complaint has been submitted in compliance with the requirements set out in the Whistleblowing Channel Regulation and
b. The whistleblower acts in good faith and has reasonable grounds to believe that the information reported is true at the time the complaint is made, even if the whistleblower has not been able to provide conclusive evidence.

On the other hand, those subjects who report on the issues below are expressly excluded from protection:

a. Information that is already fully available to the public;

b. Issues contained in queries or complaints that have been rejected as inadmissible;
c. Information related to complaints about interpersonal disputes, or involving only the whistleblower and the reported person;
d. Mere rumours;
e. Information related to infringements outside the objective scope of the Channel; or
f. Information that is already fully available to the public.

7. Breaches of the retaliation prohibition protocol

If you meet the necessary conditions to be a beneficiary of the protection established in this Protocol, if you have suffered or are suffering retaliation, you should immediately inform the System Manager through the Whistleblowing Channel, using any of the following channels:

E-mail: canaletico@tubosreunidosgroup.com
Telephone line: **(+34) 667412930**
Request for a **face-to-face meeting with the System Manager**

for the latter to carry out the appropriate verification actions, together with the adoption of the measures deemed necessary to put an end to them.

In any case, if it is concluded, after the appropriate investigation, that the whistleblower entitled to protection has been the victim of retaliation as a result of reporting, the relevant disciplinary procedure shall be activated against the person or persons who have exercised such retaliation in contravention of the provisions of this Protocol.

This Protocol is an annex and an integral part of Tubos Reunidos Group's Whistleblowing Channel Regulation approved by the Board of Directors of TRSA on 25 May 2023.

****