



TECNICAS REUNIDAS

Internal Reporting Channel Policy

CONTENTS

1	PURPOSE.....	3
2	SUBJECTIVE SCOPE OF APPLICATION.....	4
3	MATERIAL SCOPE OF APPLICATION	5
4	PROJECTION OF THE POLICY WITH THE TR GROUP.....	6
5	TR GROUP INTERNAL REPORTING CHANNEL MANAGER.....	6
6	TR GROUP INTERNAL REPORTING CHANNEL PRINCIPLES	7
7	SCOPE OF PROTECTION	9
	7.1 PEOPLE WHO MAY NEED PROTECTION.....	9
	7.2 CONDITIONS FOR PROTECTION.....	9
8	CONSEQUENCES OF A BREACH	10
9	MONITORING, SUPERVISION AND UPDATING.....	10
10	IMPLEMENTATION OF THE POLICY	10
11	DISSEMINATION	11
12	APPROVAL AND ENTRY INTO FORCE	11

Internal Reporting Channel Policy

1 PURPOSE

The purpose of Spanish Law 2/2023, of 20 February, regulating the protection of people reporting regulatory violations and corruption matters ("**Law 2/2023**"), which transposed into the Spanish legal system Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, on the protection of persons who report breaches of Union Law (the "**Directive**"), is to protect people who, in an employment or professional context, detect certain regulatory violations and report them using the internal information channels that must be set up for such purpose, granting adequate protection against any type of retaliation.

For these purposes, and in accordance with said Law, TÉCNICAS REUNIDAS, S.A. ("**TÉCNICAS REUNIDAS**" or the "**Company**") has implemented an Internal Reporting Channel ¹ (the "**Internal Reporting Channel**" or the "**System**") including **(i)** this Internal Reporting Channel Policy (the "**Policy**") which sets forth the general principles and premises of the System, the aims of which essentially focus on protecting informants and, for such purpose, establishing the requirements that must be fulfilled by the information channels, as well as **(ii)** the Internal Reporting Channel Management Procedure (the "**Procedure**") which implements it under the terms established by applicable laws.

Likewise, the Internal Reporting Channel established by this Policy and which implements the Procedure is part of the Compliance Management System in effect for all Técnicas Reunidas group companies ("**TR Group**" or the "**Organization**"), which has had a Whistleblowing Channel since the year 2016. The TR Group Internal Reporting Channel meets an essential purpose in enforcing the Group's commitment to regulatory compliance and the principles and values of its Code of Conduct.

The purpose of this Policy is to implement the principles guiding and inspiring the functioning of the Internal Reporting Channel as the preferential means for reporting any violations that fall under the material scope of application of the TR Group Internal Reporting Channel (see point 3).

In this context, the TÉCNICAS REUNIDAS Board of Directors has been allocated the powers to determine and approve the Company's general policies and strategies². Exercising such powers and in accordance with the Directive, the TÉCNICAS REUNIDAS Board of Directors is responsible for implementing the foundation for the Internal Reporting Channel with the approval of this Policy and the Procedure implementing it.

¹ Article 5.1 of Law 2/2023.

² Article 5.1. (x) of the Técnicas Reunidas Board of Directors Regulations.

2 SUBJECTIVE SCOPE OF APPLICATION

This Policy applies to and is mandatory for all people within the Organization. This means all people included in governing bodies, executives, management, employees, whether temporary or working under collaboration agreements, volunteers within the Organization and all other people under the hierarchical supervision of any of the foregoing³. Moreover, the Policy is applicable to business partners which shall mean any part – except those working within the Organization – with whom it has or expects to establish any type of business relationship⁴, and third parties engaging in relations with the TR Group.

The various protection measures provided for throughout this Policy shall be implemented, as corresponds, with all Informants, related Third Parties and People affected by any communication received through the System. In this context:

- The figure of **Informant**⁵ includes all people who report any violation including not only public servants or employees but also all self-employed workers, shareholders, participants and members of administrative and management bodies, the people who work for or under the supervision of business partners, volunteers, interns and trainee workers as well as all people whose employment or statutory relationship has ended or has not yet begun.
- The figure of related **Third Parties**⁶ includes all people within the TR Group who assist the Information at any time throughout the process, as well as related people who may suffer retaliation such as colleagues or family members. It also includes legal entities for which or with which the informant works or with which they maintain any type of relationship in an employment context or in which they hold a significant interest⁷.
- The figure of the **Person affected by the communication**⁸ includes the people who in a communication are said to have engaged in an action or omission (constituting a violation under the scope of application of the TR Group Internal Reporting Channel).

³ Article 3 of Law 2/2023.

⁴ Section 1 (x) of the Criminal Compliance Policy.

⁵ Article 3.1 of Law 2/2023.

⁶ Article 3.4 of Law 2/2023.

⁷ Article 3.4 of Law 2/2023.

⁸ Article 5.10 of the Directive.

3 MATERIAL SCOPE OF APPLICATION

The TR Group has implemented an Internal Reporting Channel through which Informants may report any actions or omissions constituting violations occurring in an employment or professional context⁹ relating to the following areas¹⁰:

- **Violations of European Union Law** relating to the following areas, among others: public procurement, the financial sector, the prevention of money laundering and terrorism financing, product safety and conformity, transport safety, environmental protection, protection from radiation and nuclear safety, the safety of food and feed, animal health and wellbeing, public health, consumer protection, the protection of privacy and personal data, and network and information system security, the EU's and the internal market's financial interests¹¹.
- **Serious or very serious criminal or administrative violations.**
- **Occupational health and safety labor law violations.**
- **Violations of the TR Group's Code of Conduct** or any other Policy implemented in accordance with the TR Group Compliance Management System.

Information on the violations mentioned will be collected by the System Manager through a single digital platform enabling written communications¹², which may be accessed via the following link:

<https://canaletico.tecnicasreunidas.es/tecnicasreunidas>

Through the System, the Informant may also, if deemed necessary, request an in-person meeting in order to submit their notification¹³.

⁹ Article 3 of Law 2/2023.

¹⁰ Article 2 of Law 2/2023.

¹¹ Includes the violations set forth in: (i) the Annex to EU Directive 2019/1937, particularly in Part I, B, on financial services, products and markets and the prevention of money laundering and terrorism financing; (ii) article 325 of the Treaty on the Functioning of the European Union (TFEU) concerning the fight against fraud; or, (iii) when they affect the internal market as set forth in article 26 of the TFEU.

¹² Article 5.2.c) of Law 2/2023.

¹³ Article 7.2 of Law 2/2023.

The TR Group Internal Reporting Channel allows submitting communications with a name or anonymously¹⁴ and it is managed through a digital tool that complies with applicable law on protecting Whistleblowers and the use of information channels.

Notwithstanding the foregoing, and depending on the subject of the communication, the investigation thereof may be referred to internal bodies and departments with the corresponding powers with regard to such matter.

4 PROJECTION OF THE POLICY WITH THE TR GROUP

This is a corporate Policy and thus applicable to all TR Group companies. The various companies within the Organization shall carefully read it and implement this Policy, and therefore, the general principles of the Internal Reporting Channel provided for therein through their own governing bodies.

5 TR GROUP INTERNAL REPORTING CHANNEL MANAGER

The TÉCNICAS REUNIDAS Board of Directors shall designate, dismiss or terminate the Internal Reporting Channel Manager (the “**System Manager**” or the “**Manager**”) pursuant to the options available under Law 2/2023¹⁵.

Any such appointment or termination shall be communicated to the corresponding Authorities before the deadline legally established, specifying (in cases of a termination), the reasons justifying such action.

The Manager must diligently manage the Internal Reporting Channel within the TR Group pursuant to the provisions of this Policy and the Procedure and, in particular, the adequate management and processing of all investigations initiated following any communication received.

The Manager shall perform all duties independently and autonomously with respect to any TR Group body or request. He/she may not receive any type of instructions in the exercise of his/her duties and must have the personal and material resources necessary to complete them.

The System Manager will exercise his/her duties with respect to the various TR Group companies, making all appropriate decisions for such purpose.

The exchange of information between the various TR Group companies for adequate coordination and the best performance of their duties shall be acceptable¹⁶.

¹⁴ Article 7.3 of Law 2/2023.

¹⁵ Article 8 of Law 2/2023.

¹⁶ Article 11.3 of Law 2/2023.

6 TR GROUP INTERNAL REPORTING CHANNEL PRINCIPLES

The general principles guiding and inspiring the Internal Reporting Channel so as to ensure adequate functioning thereof and guarantee the rights of the people involved in the communications are as follows:

- (i) **Principle of Zero Tolerance.** The Internal Reporting Channel is a manifestation of the principle guiding the TR Group on zero tolerance and absolute rejection for the commission of any violation of the laws in effect or its ethical principles and values. In this context, there is an obligation for all people belonging to the Organization to report any conduct that may be considered a violation.
- (ii) **Principle of Effectiveness.** The communications received involving violations of European Union Law, serious or very serious administrative or criminal violations or violations of Occupational Health and Safety labor laws shall be effectively handled in all cases.
- (iii) **Prohibition on Retaliation.** Taking any type of retaliation against Informants or related Third Parties for reporting something through the TR Group Internal Reporting Channel is absolutely prohibited. This prohibition includes threats and attempted retaliation.

Retaliation shall mean any action or omission prohibited by the law or which directly or indirectly involves unfavorable treatment putting the victim at a particular employment or professional disadvantage simply due to their status as an informant or due to their collaboration with the handling of any information.

Retaliation includes but is not limited to the following:

- The suspension of an employment contract, dismissal or extinction or non-renewal of an employment agreement – unless done as part of the regular management powers in accordance with labor laws.
 - Damages, including reputational damages, economic losses, coercion, intimidation, harassment or ostracism.
 - Negative references with respect to professional performance.
 - Inclusion on blacklists or the dissemination of information within a certain sector which hinders their access to jobs or promotions.
 - The rejection or cancellation of a license or training certification.
 - Discrimination or unfavorable or unfair treatment.
- (iv) **Principle of Independence.** The procedures leading to the various communications shall be governed by the utmost objectiveness and independence, with the Organization establishing the corresponding principles and rules of action to prevent any conflicts of interest.

- (v) **Principle of Personal Data Protection and Confidentiality.** The Internal Reporting Channel is set up in accordance with personal data protection requirements.

The TR Group undertakes not to process any personal data not absolutely necessary to understand the actions or omissions constituting a violation reported in the communications recorded in the Internal Reporting Channel and which, furthermore, are not legally justified as required. Any unnecessary data will be deleted.

Likewise, the System is designed and managed in such manner so as to guarantee the confidentiality of the identity of the Informant – anonymity if so desired by the Informant –, the People affected and any Third Party mentioned in any communication, as well as of the actions taken to manage and process them.

- (vi) **Principle of Respect.** The management and processing of communications shall be carried out in respect of and guaranteeing all rights and protection measures applicable to Informants, related Third Parties and the People affected by any communication pursuant to the laws in effect and, in particular, this Policy.

The People affected shall have the following rights:

- The Right to Honor.
- The Right to the Presumption of Innocence meaning no one may ever be penalized without first proving the veracity of the events included in a communication.
- The Right to Defense, meaning all those affected must be informed of the actions or omissions they are accused of in the time and manner deemed appropriate to guarantee the proper results of the investigation. At the same time, they shall be given the opportunity to be heard at any time in order to offer an explanation for the situation communicated, summoned for an interview or asked to provide clarifications to better understand the events.
- The Right to Access to the Case File under the terms provided for by applicable laws and, in all cases, respecting the principle of confidentiality set forth above.
- Protection for Informants, withholding their identity and guaranteeing the confidentiality of the events and data involved in the procedure.

- (vii) **Principle of Objectiveness and Integrity.** The provisions set forth in this Policy shall be in all cases guided by the principles of absolute objectiveness and integrity. Likewise, the Organization will not permit the use of the System for motives that are illegitimate, personal or contrary to good faith.

7 SCOPE OF PROTECTION

7.1 PEOPLE WHO MAY NEED PROTECTION

Through the Information System, the TR Group offers protection to good faith Informants against any harm they may suffer due to communicating possible violations they gain knowledge of as well as to related Third Parties. Likewise, the TR Group offers protection to anyone who has publicly disclosed one of the violations that fall under the application of the Internal Reporting Channel ¹⁷.

Moreover, protection shall be provided under the terms legally established to People affected by any Communication.

7.2 PROTECTION CONDITIONS

If the Informant were to submit a communication through the TR Group Internal Reporting Channel or make a public disclosure, the protection offered by the Organization shall be conditioned on the good faith submission or disclosure¹⁸ pursuant to the provisions of this Policy and the Procedure. Good faith is assumed to exist when there are reasonable motives to think the information referred was accurate at the time of the communication or public disclosure, even when not conclusive proof is provided, and said information falls under the scope of application of this Policy.

Communications will be considered submitted in bad faith when they are done by stealing the identity of the Informant or detailing events that are known to be untrue or involve people that have had no relationship with such events, even when such events are true.

Expressly excluded from the protection offered by the TR Group are:

- (i) Any information included in communications that have been rejected previously by the very Internal Reporting Channel or by an Independent Protection authority for any of the following reasons:
 - When the events mentioned lack credibility.
 - When the events mentioned do not constitute any type of violation of the laws included under the scope of application of this Policy.
 - When a communication manifestly lacks grounding or there are rational indications of the commission of a crime.
 - When the communication has no new and significant information on violations in comparison with a prior communication with respect to which the corresponding procedures have been concluded unless there are new factual or legal circumstances justifying other follow-up.

¹⁷ Article 35 and seq. of Law 2/2023.

¹⁸ Preamble of Law 2/2023 and the Whereas Clauses of the Directive.

- (ii) Information related to claims regarding interpersonal conflicts or those solely affecting the Informant and the people mentioned in the communication or disclosure.
- (iii) Information already fully available to the public or mere rumors.
- (iv) Information referring to actions or omissions not included in Section 3 above.

If an Informant makes a public disclosure¹⁹, the protection offered by the Organization will be further subject to the legally established protection conditions.

8 CONSEQUENCES OF NON-COMPLIANCE

All people under the scope of this Policy have an obligation to comply with it. If a serious breach hereof is identified, it may and must be reported to the Organization through the Internal Reporting Channel with the sanctions that may apply based on the matter subject of the breach or the person who has committed the violation.

9 MONITORING, SUPERVISION AND UPDATING

Pursuant to the duties allocated to the Audit and Control Commission, it must monitor and supervise the application and implementation of this Policy and the Procedure implementing it without prejudice to any powers reserved to the Company's Board of Directors.

On the other hand, the System Manager is responsible for updating this Policy when appropriate or in view of organizational changes, changes in the control structure, activities developed and/or changes in the law or case law. He/she must also inform the Audit and Control Commission before referring any proposal, where applicable, to the Board of Directors.

10 IMPLEMENTATION OF THE POLICY

As part of his/her duties and without prejudice to the monitoring and supervision powers attributed in this Policy and the Procedure to the Audit and Control Commission, the System Manager may draw up any implementing rules or guides to this Policy and the Procedure deemed necessary to ensure proper functioning of the Internal Reporting Channel , always first informing the Audit and Control Commission.

¹⁹ Article 28 of Law 2/2023.

11 DISSEMINATION

This Policy shall be delivered and is available to all people who are a part of the TR group, as well as all business partners and third parties by means of the publication thereof on the TR Group intranet system and the Organization's website under a separate and easily identifiable section of the homepage.

The TR Group undertakes to disseminate and disclose the necessary information to all personnel so they may be aware of the Organization's Internal Reporting Channel , its principles, guarantees and obligations, as well as the preventive purpose thereof.

12 APPROVAL AND ENTRY INTO FORCE

At its meeting on 28 June 2023, the Board of Directors unanimously agreed to approve this Policy. That date shall be considered its date of entry into force.