CIRSA

OPERATING POLICY OF THE ETHICS HOTLINE CHANNEL

2023

1. INTRODUCTION

1.1. Justification of the reforms

Ethics, integrity, respect for legality, transparency and honesty are principles that are defended by the CIRSA Group, thus rejecting any possible irregular action. Our activity is designed so that each person who forms part of the Company strictly complies with current legislation, at all times and in each place where this activity is carried out. Likewise, as set out in the Group's Code of Conduct, strict compliance with the Company's own commitments and obligations with regard to relations with customers, suppliers, partners and the environment in general is upheld. This is the basis for avoiding any possible wrongdoing that would have a strong impact on the reputation and the business itself.

Within the framework of the compliance culture that prevails throughout the Group and as part of the continuous improvement plans being implemented on Compliance policies, a new platform has been incorporated into the Company's Internal Information System, also known as the Ethics Hotline Channel. This tool enables the Group to continue to comply with the new European directives and state regulations, to reinforce its high level of regulatory compliance and to maintain a firm commitment to society in general, since the platform enables the anonymous - if desired - and confidential reporting of any potentially significant irregularities that may occur within the company or on its behalf.

This compliance is one of the factors that allows the Company to be one of the leading companies in the sector and a benchmark at the business level.

1.2. Regulatory context

The need for the existence of an Ethics Hotline Channel appears as an essential element of the Compliance and Regulatory Risk Prevention Models. Thus, and in accordance with the provisions of Article 31 bis, paragraph 5, subparagraph 4 of the Criminal Code: "the organisation and management models (...) shall impose the obligation to report possible risks and breaches to the body responsible for monitoring the functioning and compliance of the prevention model". Similarly, paragraph 5 of section 5 of Article 31 bis of the Criminal Code establishes the need for a Disciplinary System in matters of Compliance, by literally stating that "(...) the organisation and management models (...) shall establish a disciplinary system that adequately sanctions non-compliance with the measures established by the model". Both issues are addressed in the development of this Policy in order to effectively meet the requirements of the legislator.

From the point of view of the CIRSA Group's internal regulations, this Policy must be considered an integral part of the Group's Global Compliance Management System and a key element in defining the principles and structuring the Group's Internal Information System. CIRSA wishes to make it clear that the Operating Policy of the Ethics Hotline Channel is not intended to replace the competencies of the ordinary management of the channel in the countries where it operates. Relationships between them must therefore be based on complementarity, coordination and collaboration, in order to achieve the best result.

From the point of view of the content and structure of this Policy, it follows the guidelines imposed by the following regulations:

Firstly, it is due to Circular 1/2016 of the State Attorney General's Office, of 22 January, on the criminal liability of legal persons in accordance with the reform of the Criminal Code executed by Organic Law 1/2015, which states that in order for company employees to be able to warn of potentially unlawful conduct, it is necessary to have adequate internal regulations that specifically protect the Whistleblower.

It also complies with ISO 37001 on Bribery and Corruption Management Systems, which makes special reference to the process to be followed in the investigation of Alerts, pointing out the need to develop internal processes for Alerts that guarantee: (i) the effectiveness of the actions carried out, (ii) the capacity of the persons in charge of the investigation, (iii) the necessary reflection of the involvement and cooperation of other areas and (iv) the confidentiality of the Alert, the investigation and the resolution.

For its part, Standard 37301 for Compliance Management Systems establishes the need for Alert channels. Thus, in the section on raising concerns, it states literally: "even where not required by local regulation, organisations should consider developing an Alert mechanism that allows for anonymity or confidentiality, through which employees and agents of the organisation can report or seek guidance in terms of non-compliance with compliance without fear of retaliation". In addition, this standard makes specific reference to the requirements and recommendations included in the ISO 37002 Standard for Whistleblowing and Irregularities Management Systems - on Whistleblowing Channels -, which has served as the basis for the development of this Policy.

It is also worth highlighting the relevance of data protection legislation in this area, as well as the protection of whistleblowers, especially after the protection of the whistleblower with Directive (EU) 1937/2019 of 23 October 2019, on the protection of persons who report breaches of EU law and, similarly, the recent approval of Law 2/2023 of 20 February, regulating the protection of persons who report breaches of regulations and the fight against corruption. This regulation ensures that Whistleblowers can report, internally and to the authorities, any potential breach of European law within an organisation through channels that ensure the safety of the Whistleblower, without fear of retaliation from the company.

For this reason, in accordance with the requirements established in the aforementioned regulations and for the effective implementation of the internal Alert channels -ordinary and alternative- within the CIRSA Group's Internal Information System, this Ethics Hotline Channel Operating Policy provides for the development of the scope and content of the procedures and processing of Alerts. In this respect, the following requirements are established:

1) Alerts can be issued in writing, as well as by analogue and digital means, and also in person if the Whistleblower so wishes;
2) Communications or Alerts can be anonymous;
3) Prompt handling of all Alerts (including anonymous ones);
4) Acknowledgement of receipt of the Alert within 7 days;
5) Allows for the ad hoc designation by the Compliance Body of an Investigation Team, effective until the case is terminated, as well as the designation of a case manager who will process the Alerts and maintain communication with the Whistleblower. If necessary, it will be responsible for requesting additional information and providing a response;

6) Establishment of a general deadline of 3 months to reply to the Whistleblower on the processing of the Alert, starting from the acknowledgement of receipt;
7) Establishment of the duty to inform employees or third parties of the existence of these information systems ("Ethics Hotline Channel").

Furthermore, it makes it clear that the processing of personal data arising from the application of this regulation shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights. Similarly, access to the personal data contained in the Ethics Hotline Channel must be limited within the scope of their competences and functions exclusively to those persons who - regardless of whether or not they belong to the entity - have internal monitoring and compliance functions (the person in charge and the manager of the Channel, the human resources manager or the duly designated body, only when disciplinary measures could be taken and/or the person in charge of the legal services if legal measures should be taken in relation to the facts related to the facts described in the report), the head of human resources or the duly designated body, only when disciplinary measures may be taken and/or the head of the legal services of the entity if legal measures may be taken in relation to the facts described in the communication), or to the data processors that may be designated and to the data protection officer. This is without prejudice to access by other persons or to the possible disclosure of data to third parties or to the authorities where this is necessary for disciplinary measures or for the conduct of legal proceedings. And, notably, it also states that the identity and confidentiality of the data corresponding to the persons affected must be preserved, especially the data of the person who would have reported the facts if he or she had not done so anonymously.

Finally, with regard to the possibility of filing Anonymous Alerts, we refer to Supreme Court Ruling 272/2020, of 6 February, which highlights and validates the use of Anonymous Alerts for the detection of possible criminal wrongdoing that can be corroborated, as in this procedure, by the subsequent internal and police investigation. Thus, the Criminal Chamber notes that: "(...) Importance is attached to the Alert made and in which, with the non-existence of an internal regulatory compliance programme, it is of notable interest that in the period of the proven facts a mechanism of 'ad intra' action is carried out within the company, recently regulated in the so-called 'internal whistleblowing channel', also known as 'whistleblowing', and which has been included in the recent 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 EU law". Currently transposed into Spanish law through Law 2/2023, of 20 February, which regulates the protection of persons who report regulatory infringements and the fight against corruption.

2. AIM

The CIRSA Group, in order to move forward with its commitment to establish a strong culture of compliance and information or communication, beyond any legal obligation, based on values and principles, recognises the importance of adopting an internal operating regulation (hereinafter the "Policy"). These rules comprise the Group's Code of Conduct and the Organisation, Management and Control Model. The aim of this is to provide support and adequate protection against reprisals that may be suffered by those who report any of the compliance actions or omissions and to develop an awareness of the need to use the Internal Information System or Ethics Hotline Channel, as well as to regulate how to use the application it houses (hereinafter referred to as the "Ethics Hotline"): "Platform"), with the purpose of providing advice and certainty in the decision making process of the person aware of possible infringements, to alert and assist in the prevention and detection of threats against the public and private interest.

In this regard, in order to have the necessary tools to facilitate any detection of a possible illegal act and to protect all the people who form part of the Group and its reputation in the eyes of our stakeholders, the Company has reinforced the existing Ethics Hotline Channel with the implementation of a Platform to receive, analyse and process Alerts (hereinafter referred to as the "Platform"): "Alerts"), which fully guarantees confidentiality and complies with the highest standards of Information Security and Data Protection. And if the user so wishes, this communication can be made completely anonymously, guaranteeing the non-existence of any possible retaliation.

To this end, the following key issues need to be identified:

1) Subjective scope of application: **To whom does this Policy apply? Who is responsible?**
2) Target scope of the Alert: **What can be Alerted; When should I do it?**
3) Implementation of the channel: **How to use the CIRSA Group's Ethics Hotline Channel; Can an Alert be made anonymously?**
4) Consequences of the Alert: **What happens when an Alert is made through the Ethics Hotline Channel?**
5) The CIRSA Group's Ethics Hotline Channel Operating Policy is a universal Policy applicable to all companies belonging to the Group, unless there is a regulatory justification that provides for an exception to such application.

2.1. Subjective scope of application: To whom does this Policy apply; who is responsible?

2.1.1 To whom does this Policy apply?

The persons subject to this Policy (hereinafter "Recipients" and/or "Whistleblowers") are: all CIRSA Group employees, volunteers, interns, trainees, employees undergoing training regardless of whether or not they receive remuneration, as well as those whose employment relationship has not yet begun, in cases where the information on infringements has been obtained during the selection process or pre-contractual negotiation; those reporting within the framework of an employment or statutory relationship that has already ended; partners; shareholders or participants; members of the administrative, management and supervisory bodies, including non-executives; customers; collaborators, suppliers, self-employed persons, contractors and subcontractors, including any person working for or under their supervision and direction; legal representatives of employees in the exercise of their functions of advising and supporting the reporting person; natural persons who, within the organisation in which the reporting person provides services, assist the reporting person in the process; natural persons related to the reporting person who may suffer retaliation, such as co-workers; legal persons for whom the reporting person works or with whom he/she has any other relationship in an employment context or in which he/she has a significant shareholding and; in general, any person who provides services for the Group on a contractual basis, in addition to the Group's own stakeholders (hereinafter the "Third Parties").

2.1.2 Who is responsible?

The person responsible for the CIRSA Group's Internal Information System or Ethics Hotline Channel is the Board of Directors of Cirsa Enterprises, s.l. itself, as the Group's parent company, which in turn has appointed the Corporate Compliance Body as the body responsible for its management and the processing of investigation files, which it will carry out independently and autonomously from the rest of the company's bodies and may not receive instructions of any kind in its exercise.

2.2. Target scope of the Alert: What can be Alerted; When should I do it?

2.2.1 What can I Alert under this Policy?

This Policy encourages the reporting of any concerns that the Whistleblower may have in relation to possible violations by action or omission of the CIRSA Group's Global Compliance Management System, which in accordance with the scope defined in Directive (EU) 1937/2019 and Law 2/2023 may constitute breaches of European Union law or constitute a serious or very serious criminal or administrative offence. This includes information on breaches in a broad sense: reasonable suspicions, actual or potential breaches that have occurred or are likely to occur, among others.

To this end, by way of example, but not limitation, the following possible communications are highlighted:

A. **CORRUPTION**: breaches of legislation, policies, standards, guidelines and/or procedures relating to:

- **Bribery/Trading in influence**: offering or accepting improper advantages of any kind, whether in a private business context or in a public context, to officials, authorities, etc.

  Examples: offering or accepting commissions or monetary gifts; invitation from or through business partners, with the appearance of wanting to influence a business relationship.

- **Fraud**: presenting false facts, data or information, or omitting true facts, data or information, in order to obtain, or not necessarily to obtain, an unlawful financial benefit for oneself or for others.

  Examples: issuing excessive invoices in order to keep the surplus; credit fraud; subsidy fraud; insurance fraud; falsification of identity documents, keys or other means of identification; tampering with machines or testing methods.

- **Theft**: unauthorised removal of money or objects from another's property for one's own use or for transfer to a third party.

  Examples: theft of goods from the warehouse; withholding of company funds or work materials.

- **Non-compliance with accounting and financial reporting rules/Offences against the tax and social security authorities**: deliberate misrepresentation of transactions, inadequate controls over an organisation's operations.

  Examples: false information about income, expenses, assets or property; fraudulent representation of transactions; destruction of supporting documents; concealment of assets.

B. MONEY LAUNDERING

Breaches of legislation, policies, manuals and/or procedures in the area of

Prevention of Money Laundering and Financing of Terrorism through the introduction of illegally obtained money or illegally acquired assets into the legal economic and financial circuit.

Examples: transfer of funds through a "tax haven"; a business partner's claim to settle all or part of a transaction in cash; indications of the business partner's proximity to criminal or terrorist organisations; doubts about the identity of the customer or suspicions that the customer is acting as a front for a third party.

C. DATA PROTECTION

Violation of Data Protection and Telecommunications Secrecy legislation, policies, manuals and/or procedures.

Examples: unauthorised collection, processing or disclosure of personal data; unauthorised technical surveillance of employees; use of data for private purposes; use of customer data for commercial purposes without their consent.

D. INFORMATION SECURITY

Breaches of Information Security regulations, policies, guidelines and/or procedures designed to protect data against falsification, destruction and unauthorised disclosure, computer damage or disclosure of secrets.

Examples: breach of security of computer systems and networks that seriously compromises the confidentiality, integrity or availability of information or equipment; disclosure of user accounts and passwords to unauthorised persons; cyber attacks.

E. UNETHICAL PRACTICES

Violation of behavioural standards and guidelines, professional obligations and legal requirements through deliberate or unintentional improper practices or actions contrary to the Code of Conduct. Examples: violations of the Responsible Gambling Policy or Environmental Protection Policy, use of misleading advertising; drug trafficking; incidents in the normal course of gambling operations.

F. HUMAN RIGHTS

Breaches of labour legislation, human resources policies, guidelines and/or procedures, legal obligations and requirements to ensure gender equality, implementation of core International Labour Organisation conventions, working conditions, social dialogue, respect for workers' right to be informed and consulted, respect for trade union rights, health and safety in the workplace.

Examples: violations of Human Rights and Human Resources Policies; failure to promote the principle of equal treatment between women and men; discrimination and non-inclusion of people with disabilities; sexual and moral harassment or against moral integrity; illegal or misleading hiring and imposition of harmful working conditions; omission of health and safety measures.

G. SEEKING ADVICE

Here you can raise doubts or queries on general issues related to your compliance in the company and ask for advice on such issues.

2.2.2 When should reporting take place?

The CIRSA Group is convinced that the best way to promote the Alerts is to create an environment where people feel comfortable to share any possible incident that may violate the Group's Global Compliance Management System. And, therefore, it promotes the fostering of an environment in which facts related to possible breaches of the System can be reflected.

This is in line with a principle that governs all the CIRSA Group's relations with its stakeholders: Alerts must always be made in good faith, which amounts to the implementation of a "culture of fairness", in accordance with the provisions of Directive (EU) 1937/2019 and Law 2/2023. This means that, at the time of the Alert, the Whistleblower must have reasonable grounds to believe that the information it indicates is true and contains possible infringements.

2.2.3 What happens in emergency cases?

Undoubtedly, the processing of the Alerts raised through the different channels available to the CIRSA Group requires that the body in charge of receiving them -the Compliance Body-, classifies, for internal use, the content of the Alert, which will allow the processing to be adapted to its content. For this purpose, the established classification is:

- False Alert.
- High.
- Medium.
- Low.
- Others.

In any event, it is imperative to ensure that any member of the Group's Compliance Body is informed as soon as possible so that, once the facts have been addressed, the matter can be dealt with as efficiently as possible by processing the Alert in accordance with the Protocol for Investigating Acts of Fraud and Non-Compliance.

2.3. Implementation of the channel: How do I use the CIRSA Group's Ethics Hotline Channel; Can there be an anonymous Alert?

2.3.1 Steps to follow in submitting an Alert

Any Alerts under this Policy, or if you have any additional questions or comments, can be made through one of the channels listed below:

Main channels:

1) On the public corporate website in the section CSR - Compliance - Ethics Hotline Channel via the following link: https://www.cirsa.com/
2) On the Intranet in the Shortcuts section - Ethics Hotline Channel through the following link: https://cirsa.sharepoint.com/sites/es_intranet
3) Directly through the following link: https://www.bkms- system.com/COMPLIANCE-CIRSA

Other channels:

4) Member of the Compliance Body (Corporate Director Human Resources, Corporate Director Internal Audit and Corporate Director Legal and Compliance):
   - Joan Ramón Balagué Ribalta.
   - Xavier Cots Vega.
   - Miquel Vizcaíno Prat.
   - Carlos Jiménez Cordero.
5) E-mail: compliance@cirsa.com
6) Telephone: 608 655 567
7) In person or by post:
   CIRSA Corporate Services, S.L. - Compliance Area
   Carretera de Castellar, 338
   08226 – Terrassa (Barcelona) Spain

Or via:

8) Anti-Fraud Office of Catalonia (OAC): https://antifrau.cat/es/es
9) Valencian Anti-Fraud Agency (AVA): https://www.antifraucv.es/
10) Andalusian Anti-Fraud Office (OAAF): https://antifraudeandalucia.es/
11) Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC): https://sepblac.es/es
12) Spanish Data Protection Agency (AEPD): https://aepd.es/es
13) National Competition Market Commission (CNMC): https://cnmc.es

2.3.2 What information do I need to provide when sending an Alert?

The CIRSA Group recommends that the information provided be as complete and truthful as possible. And therefore requests that, in case of an Alert, all information known to the Whistleblower in relation to possible infringements be shared. And to do so in detail. In addition, it is preferable that any supporting evidence or documents are provided or clearly referred to in the Alert. This allows the case to be handled as quickly and efficiently as possible.

2.3.3 Identification when submitting the Alert: anonymity and confidentiality

The Ethics Hotline Channel allows Alerts to be carried out anonymously.

However, the CIRSA Group encourages that, in the case of an Alert, the Whistleblower should identify himself/herself by providing his/her name and contact details. In this way, the staff in charge of processing the alert will be able to contact the Whistleblower to request additional information and clarifications, provide support and assistance, follow up if necessary, etc. At the same time, CIRSA believes that this is the best way of accrediting the high standards on which this Policy is based by certifying the principle of non-retaliation in the event of an Alert.

In the above sense, it should be noted that when a (non-anonymous) Alert is submitted, the CIRSA Group ensures through appropriate technical and organisational measures that the internal Alert procedure will be carried out in a secure manner that preserves the Whistleblower's right not to have his/her identity disclosed to Third Parties and guarantees the confidentiality of the data of the Whistleblower, the affected person and any other Third Party mentioned in the information provided or other related information.

The identity of the Whistleblower may only be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or disciplinary investigation. In this respect, such disclosures shall be subject to safeguards laid down in the applicable regulations, in particular, the informant shall be contacted before his or her identity is revealed, unless such information could jeopardise the investigation or judicial proceedings.

2.3.4 Consequences of the Alert: What happens when an Alert is made through the CIRSA Group's alternative channels?

CIRSA Group uses a digital platform to support the administration of Alternative Channels, in line with the requirements of Directive 1937/2019 and Law 2/2023.

Alerts through alternative channels are stored directly on the platform, which has robust information security measures in place to preserve the integrity, availability and confidentiality of the information. The platform allows the Whistleblower to specify the location, date, company, division, etc. affected, as well as the persons related to the Alert. In addition, it allows for the option of anonymous communication. It shall give the Whistleblower the option to accompany the communication with supporting documentation justifying the content of the communication.

Receipt shall be acknowledged through the Compliance Body within seven working days of receipt.

Upon acknowledgement of receipt, whether the Whistleblower has identified himself or herself or has done so anonymously by enabling access to the communication mailbox, the CIRSA Group, through the person designated internally, may contact the Whistleblower directly to identify himself or herself as the manager or instructor, and provide comments and updates. The processing of the Alert shall be resolved within a reasonable period of time, not exceeding three months from the acknowledgement of receipt, which may be extended to six months in cases of particular relevance or complexity. In no case will any personal data that may have been communicated and that refer to conduct that is not included in the objective scope of application set out in this Policy and those that are not necessary for the knowledge and investigation of the actions or omissions be processed, proceeding, where appropriate, to their immediate deletion. If the information received contains personal data included in the special categories of data, it shall be deleted immediately, without being recorded and processed. However, after the first three months following receipt of the Alert, any information of a personal nature concerning the Whistleblower, the aforementioned persons or Third Parties shall be removed from the Alert channel, unless it is essential to preserve it in order to leave evidence of the functioning of the Crime Prevention Model.

It is important to note that the platform transfers these Alerts only to specific people within the CIRSA Group, called Managers, who are expressly authorised and trained to manage them. In addition, the internal team that handles the documents provided is trained on how to manage them effectively, as well as to ensure their confidentiality.

The principle of action is that, when the Alert indicates a possible violation of the CIRSA Group's Global Compliance Management System, an investigation will be initiated in accordance with the Protocol for Investigating Acts of Fraud and Non-Compliance. And where the facts may be indicative of a crime, the immediate referral of the information to the Public Prosecutor's Office. If the facts affect the financial interests of the European Union, a referral shall be made to the European Public Prosecutor's Office.

CIRSA will provide information to the Whistleblower about the Alert and, to the extent possible, the outcome of the assessment of the issue. It should be noted that, in some cases, there may be limitations on the updates that can be provided on the Alert, as developed in the Group's Fraud and Non-Compliance Investigation Protocol mentioned above.

2.3.5 Fair and responsible handling of Alerts

The principle of good faith also applies from the company side. CIRSA therefore respects the rights of employees, and ensures that the rights of employees mentioned in Alerts made in accordance with this Policy are also protected.

2.3.6 What is to be understood by good faith from the company and from the Whistleblower?

From the Whistleblower's point of view, good faith means alerting with, at a minimum, reasonable grounds to believe that the information about possible infringements reported was true at the time of reporting.

From the company's point of view, in this context of Alert channels, good faith means that the company will not take any retaliation for submitting an Alert, and will protect the confidentiality and identity of the Whistleblower's person in any case and only with the following exceptions:

a. When the law, in its different modalities, requires it to be communicated to a judicial or administrative authority.
b. When permitted and essential with respect to external advisors and consultants and other suppliers of the CIRSA Group for the operation of the Ethics Hotline Channel or the investigation of the Alerted facts, as set out in sections 3.6 and 3.7 of this Policy. In these cases, CIRSA contractually demands the utmost confidentiality from these suppliers.

2.3.7 What is meant by retaliation? Protective measures

Retaliation means any act or omission that is prohibited by law, or that, directly or indirectly, results in unfavourable treatment that places the persons subjected to it at a particular disadvantage compared to another in the employment or professional context, solely because of their status as whistleblowers, or because they have made a public disclosure.

What are the measures to protect against retaliation?

a. Persons who communicate information about actions or omissions under the 2/2023 Act or who make a public disclosure shall not be deemed to have violated any restriction on disclosure of information, and shall not incur any liability of any kind in connection with such communication or public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure of such information was necessary to disclose an action or omission under the 2/2023 Act. This measure shall not affect criminal liabilities.
b. Whistleblowers shall not incur liability in respect of the acquisition of or access to information that is publicly communicated or disclosed, provided that such acquisition or access does not constitute a criminal offence.
c. Any other potential liability of reporters arising from acts or omissions that are unrelated to the communication or public disclosure or that are not necessary to disclose a breach under the 2/2023 Act will be enforceable under applicable law.
d. In proceedings before a court or other authority concerning harm suffered by whistleblowers, once the whistleblower has reasonably demonstrated that he or she has reported or made a public disclosure in accordance with this Act and has suffered harm, it shall be presumed that the harm occurred in retaliation for reporting or making a public disclosure. In such cases, it shall be for the person who has taken the harmful measure to prove that such measure was based on duly justified reasons not linked to the public communication or disclosure.
e. In legal proceedings, including those relating to defamation, copyright infringement, breach of secrecy, breach of data protection rules, disclosure of trade secrets, or claims for compensation based on employment or statutory law, the Whistleblowers will not incur liability of any kind as a result of communications or public disclosures protected by Law 2/2023. Such persons shall be entitled to plead in their defence in such legal proceedings that they have communicated or made a public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure was necessary to bring to light a violation under Law 2/2023.

2.3.8 What does the prohibition of retaliation mean?

The CIRSA Group does not tolerate any form of retaliation. This includes threatening, or otherwise intimidating, a person who alerts to facts related to this Policy.

The prohibition of retaliation covers, for two years, any act or omission, direct or indirect, that may prejudice a Whistleblower's rights because of his or her bona fide Alerting.

For example, the CIRSA Group will not take any of the following actions against Whistleblowers for submitting an Alert:

1) Suspension of the employment contract, dismissal or termination of the employment relationship;
2) Negative evaluation or references regarding job or professional performance;
3) Refusal of training;
4) Downgrading or denial of promotion;
5) Imposition of any disciplinary measure and any other substantial modification of working conditions such as an unjustified change of workplace location, reduction of salary, change of working hours;
6) Coercion, intimidation, harassment or ostracism;
7) Discrimination, unfavourable or unfair treatment;
8) Non-renewal or early termination of a temporary employment contract after the probationary period or non-conversion to an open-ended contract;
9) Damage, including reputational damage, or economic and financial losses;
10) Early termination or cancellation of a contract for goods or services;
11) Refusal or revocation of a licence or permit;
12) Blacklisting or dissemination of information in a particular sectoral area, which hinders or prevents access to employment or the contracting of works or services.
13) Other measures that could be considered retaliatory.

A person who reports an offence may invoke this prohibition of retaliation in the following circumstances:

a. have reasonable grounds to believe that the information referred to is true at the time of communication or disclosure, even if they do not provide conclusive evidence, and that the information falls within the scope of Law 2/2023;
b. the communication or disclosure has been made in accordance with the requirements of Law 2/2023.

Whistleblowers who communicate or disclose are expressly excluded:

a. Information contained in communications which have been inadmissible.
b. Information linked to complaints about interpersonal conflicts or involving only the Whistleblower and the persons to whom the communication or disclosure relates.
c. Information which is already fully available to the public or which constitutes mere hearsay.
d. Information concerning actions or omissions not covered by Law 2/2023.

The Ethics Hotline Channel Operating Policy extends the prohibition of retaliation to the following persons:

a. Any third party related to the Whistleblower, such as co-workers or family members;
b. Any person within the organisation providing services to the Whistleblower or assisting the Whistleblower in the Alert process, such as the legal representatives of workers in the exercise of their advisory and support functions;
c. Any legal entity that the Whistleblower owns, works for or is otherwise related to in an employment or professional context.

In the event that any member of the CIRSA Group directly or indirectly retaliates against this Policy, the Group itself will take the necessary measures to ensure that the retaliation ceases as soon as possible and, where appropriate, will take disciplinary action against those responsible for the retaliation.

2.3.9 What is meant by the prohibition of retaliation in case of External Alerts and public disclosures?

Protection against retaliation also extends to persons who report possible breaches to competent authorities via their authorised external channels or through public disclosures, even if they do so anonymously and are identified after the fact. Both direct and indirect retaliatory actions are prohibited.

A person who makes a public disclosure may invoke this prohibition of retaliation if he or she meets the conditions set out in Law 2/2023 and one of the following conditions:

a. That you have first made the communication through the Ethics Hotline and external channel, without appropriate action having been taken within the established timeframe.
b. It has reasonable grounds to believe that either the breach may constitute an imminent or manifest danger to the public interest, in particular where there is an emergency situation, or there is a risk of irreversible damage, including a danger to the physical integrity of a person; or, in case of communication through an external reporting channel, there is a risk of retaliation or there is little likelihood of effective handling of the information due to the particular circumstances of the case, such as concealment or destruction of evidence, collusion of an authority with the perpetrator of the breach, or involvement of the authority in the breach.

2.3.10 Support measures

Whistleblowers who report or disclose breaches under Law2/2023 through the procedures provided for in the Law will have access to the following support measures free of charge:

a. Full and independent information and advice on the procedures and remedies available, protection against reprisals and the rights of the person concerned.
b. Effective assistance by competent authorities to any relevant authority involved in their protection against retaliation.
c. Legal assistance in criminal proceedings and cross-border civil proceedings in accordance with Community law.
d. Financial and psychological support, on an exceptional basis, if so decided by the Independent Authority for the Protection of the Informant, I.A.P. following an assessment of the circumstances arising from the submission of the communication.

2.3.11 Protection measures for concerned persons

During the processing of the file, the persons affected by the communication shall have the right to: i) presumption of innocence and respect for honour; ii) be informed of the actions or omissions attributed to them; iii) be heard at any time; iv) defence and; v) access to the file under the terms regulated by law; as well as to the same protection established for informants, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

2.3.12 Exemption and mitigation of penalties

When a person who has participated in the commission of the infringement that is the object of the information is the one who reports its existence by submitting the information and provided that the information was submitted before the notification of the initiation of the investigation or sanctioning procedure, the body competent to resolve the procedure, by means of a reasoned decision, may exempt him/her from compliance with the corresponding sanction, provided that the following points are accredited in the file:

a. To have ceased to commit the infringement at the time of submission of the communication or disclosure and to have identified, where applicable, the other persons who participated in the infringement or who have favoured the infringement.
b. Have cooperated fully, continuously and diligently throughout the investigation procedure.
c. Having provided truthful and relevant information, means of proof or significant data for the accreditation of the facts under investigation, without having proceeded to destroy or conceal them, or having directly or indirectly revealed their content to third parties.
d. Have made reparation for the damage caused that can be attributed to it.

Where these requirements are not met in full, including partial reparation of the damage, the competent body shall decide, after assessing the degree of contribution to the resolution of the case, whether to mitigate the sanction that would have corresponded to the offence committed, provided that the informant or author of the disclosure has not previously been sanctioned for acts of the same nature that gave rise to the initiation of the procedure.

The mitigation of the penalty may be extended to the rest of the participants in the commission of the offence, depending on the degree of active collaboration in the clarification of the facts, identification of other participants and repair or mitigation of the damage caused, as assessed by the body responsible for the decision.

3. DATA PROTECTION, PROCESSING AND RETENTION

CIRSA wishes to inform its employees and customers of this additional information on data protection (hereinafter, "Data Protection Policy"), which provides in a transparent and simple manner all the legally required information in relation to the management processing of the Internal Alerts information system, the purposes for which their data are processed and the rights they may exercise. This Data Protection Policy will always be available on the digital platform enabled as an Alternative Channel.

3.1. Who are the data controllers and how can you contact them?

The management of the internal alerts information system necessarily involves the processing of personal data by CIRSA:

- At a global level and in particular for Spain, it is the Board of Directors of CIRSA ENTERPRISES, S.L. (hereinafter "CIRSA"), incorporated under Spanish law, holder of tax identification number B-87.959.649 with registered office at Calle Fermina Sevillano, number 5-7, 28022 Madrid (Madrid) and registered in the Mercantile Register of Madrid in Volume 36.763, Folio 13, Page M-658.665.
- At the international level, the board of directors of the parent company in each country as appropriate by virtue of the origin of the Alert issued when necessary for further investigation of the facts alerted, for disciplinary action and/or for the processing of legal proceedings, if any. You can find out more about the CIRSA Group's international presence athttps://www.cirsa.com/cirsa/presencia- international/.

The aforementioned companies are jointly responsible for the processing of your personal data, as they jointly determine and carry out the processing of personal information for the management of the Internal Alerts information system.

If you have any queries regarding the processing of your personal data, you can contact the Data Protection Delegate by e-mail: protecciondedatos@cirsa.com.

3.2. What is personal data and processing?

Personal data is any information relating to an identified or identifiable natural person. An identifiable natural person will be considered to be any person who can be identified, directly or indirectly, in particular by reference to an identifier such as for example a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The processing of personal data is any operation or set of operations which we undertake with respect to your personal data, such as for example the collection, recording, storage, use and communication of your data.

3.3. What personal data is collected and by what means?

Personal data may only be collected and identify you in cases where you disclose your identity. In such cases, CIRSA may collect the following information through the Internal Alerts information system:

- Name and surname.
- E-mail address.
- Telephone number.
- DNI, NIE or Passport number.
- Content of the Alert made: Country, Workplace - Point of Sale, Business Division - Corporate Address, Relationship, Attachments, etc.

In those cases in which the interested parties make the Alerts anonymously, CIRSA will not be able to identify them and, therefore, will not process any personal data of the interested parties.

3.4. What rights can you exercise?

A. **Rights of access**

You have the right to know whether we are processing your personal data and, where this is the case, to know which data it concerns.

B. **Right to rectification**

You have the right to change any data which is inaccurate or incomplete. For this, you should indicate which data you wish to change and provide sufficient evidence of this.

C. **Right to object**

Under the circumstances provided for by law, you may at any time object, on grounds relating to your particular situation, to our processing of your data. Remember that your opposition to the processing of your data will make it impossible for CIRSA to process such requests.

D. **Right to erasure**

You have the right to cancel your personal data. This does not mean that your data is fully deleted, rather that your data will be stored as blocked data in such a way as to prevent it from being processed, notwithstanding the fact that it may be made available to public administrations, courts and tribunals to deal with any liabilities that may have arisen as a consequence of the processing during the limitation period for the same.

E. **Right to data portability**

You have the right to receive and/or transfer your personal data that you have provided to us to a data controller other than CIRSA.

F. **Right to restriction of processing**

You have the right to request that the processing of your data be suspended when (i) you have challenged the accuracy of your data, while CIRSA verifies its accuracy; or (ii) you have exercised your right to object to the processing of your data, while CIRSA's legitimate grounds override those of you as a data subject.

Likewise, this right allows you to ask CIRSA to retain your personal data when (i) the data processing is unlawful and as a data subject you object to the deletion of your data, requesting instead a restriction on their use; or (ii) CIRSA no longer needs your personal data for the purposes of the processing, but needs them for the formulation, exercise, or defence of claims.

You can exercise your rights by sending your request through your user profile created in the Internal Alerts information mailbox. You are also informed that, in the event that you consider that CIRSA has not properly satisfied the exercise of your rights, you may file a complaint with the Spanish Data Protection Agency (AEPD), by contacting its website http://www.aepd.es.

3.5. How is your data processed?

In order to inform you transparently and in detail about the purposes for which your data are processed, we have separated the information relating to each processing operation into separate tables. In this way, you can find all the specific information on the processing of your data in the corresponding table on a case-by-case basis. The descriptive table contains the following information:

- For what purposes are your data processed?

This column explains the purposes for which your personal data are processed.

- What is the legal basis that legitimises the CIRSA Group to process your data?

This column explains the legal basis or justification that allows the Group to process your personal data lawfully. Data protection regulations require that your data be processed on a lawful basis or justification that legitimises such processing. Thus, in order to process your personal information, we rely on different legal bases or justifications depending on the processing of your data. The legal bases for the processing of your personal data may be:

- Legitimate interest.
- The execution of the contract.
- The fulfilment of a mission carried out in the public interest.
- CIRSA's compliance with a legal obligation.
- Vital interest.
- Your consent.

- How long will your data be kept?

This column gives an indication of how long your data will be kept for. The retention period will depend in any case on the processing of your personal information. It should be borne in mind that certain regulations may require the retention of certain data subjects' data for a certain period of time.

Below is a more detailed description of how CIRSA treats your personal data:

For what purposes is your data processed?	On what legal basis is your data processed?	How long will your personal data be kept?
Correctly process communications, confirm their receipt and respond within the legally stipulated period. Ensure adequate protection for Stakeholders who report actions or omissions contrary to law or the applicable collective bargaining agreement. Keep a record book of the information received and of the internal investigations to which it has given rise, guaranteeing, in all cases, the requirements of confidentiality. To be aware of and investigate the commission, both within the corporation and in the actions of third parties contracted by the corporation, of acts or conduct contrary to the law or the applicable collective bargaining agreement. To forward the information to the Public Prosecutor's Office immediately when the facts could be indicative of a criminal offence. If the facts affect the financial interests of the European Union, refer the matter to the European Public Prosecutor's Office. Comply with CIRSA's legally enforceable obligations.	The fulfilment of a legal obligation arising from the: i) Law 2/2023, of 20 February; ii) Organic Law 3/2018, of 5 December; iii) Organic Law 10/2010, of 28 April and; iv) Organic Law 3/2007, of 22 March.	The data subject's personal data will be processed only for the period of time necessary to decide whether or not to initiate an investigation into the facts reported. With the exception of those that: i) are not necessary for knowledge and investigation; ii) are not truthful; iii) refer to conduct that is not included in the scope of application of the Law and/or; iv) are included within the special categories of data; which shall be deleted immediately. As a general rule, it may not exceed three (3) months from receipt of the communication or, if no acknowledgement of receipt was sent, three (3) months from the expiry of the seven (7) day period following the communication, except in cases of particular complexity requiring an extension of the period, in which case the period may be extended up to a maximum of a further three (3) months. If the time limit has elapsed without any investigative action having been taken, they shall be deleted, unless the purpose of the retention is to leave evidence of the operation of the system. In this case, communications that have not been acted upon may only be recorded in anonymised form. Otherwise, they shall be kept in the register-book for such period as is necessary and proportionate for the purposes of complying with the applicable regulations and, in no case, for a period exceeding ten (10) years.

3.6. To whom is your data communicated?

Whoever submits a communication has the right not to have his or her identity disclosed to third parties.

CIRSA may communicate your data in the framework of a criminal, disciplinary or sanctioning investigation, subject to a legal requirement or basis that legitimises the communication, when it is necessary for the adoption of corrective measures in the entity or the processing of the sanctioning or criminal proceedings that, where appropriate, may be applicable, to:

- The person responsible for the system and whomever manages it directly.
- Human resources manager or duly designated competent body, only where disciplinary action may be appropriate.
- Responsible for the legal services of the entity if legal action should be taken in relation to the facts described in the communication.
- Data protection officer.
- Legal advisors, experts, cybersecurity companies and/or other third parties necessary to carry out the necessary investigations to discern the facts alerted by the interested parties.
- Public Prosecutor's Office.
- European Public Prosecutor's Office.
- Courts and Tribunals.
- Government Agencies and the Public Administration.
- State Security Forces and Bodies.

3.7. Who can access your data?

CIRSA informs you that it works with third parties, specifically, service providers necessary for the correct development of the Internal Information System. These service providers may, in the course of their business, have access to your data. This access does not constitute a transfer of data, but rather access as a data processor, which is regulated and provided for in the GDPR. In any case, we inform you that CIRSA cares for your data and, therefore, has verified that these providers offer an adequate level of security and ensure the protection of the rights and freedoms of data subjects.

3.8. Is your data safe?

Appropriate technical, organisational and legal measures are in place to preserve the identity and guarantee the confidentiality of the data of the persons concerned and of any third parties mentioned in the information provided, especially the identity of the informant if identified.

3.9. Changes to this data protection policy

This Data Protection Policy may change over time due to possible changes in the criteria followed by the competent data protection supervisory authority at any given time. We therefore reserve the right to change this Privacy Policy to permit us to adapt it to said criteria and to jurisprudential or legislative changes.

4. RELATED PROCEDURES

As the Policy described in this document is directly related to other policies and/or procedures, the following is a list of those that the CIRSA Group considers to be the most decisive when it comes to understanding its purpose and scope.

Specifically, these are the procedures linked to and/or affected by this Policy, which are published on the company's website in the "Corporate Commitment Policies and Procedures" section:

- Code of Conduct.
- Crime Prevention Model.
- Corporate Governance Policy.
- Anti-corruption policy.
- Personal Data Protection Policy.
- Information Security Policy.
- Prevention of Money Laundering Policy.
- Human Rights Policy.
- Human Resources Policy.
- Environmental Policy.
- Protocol for Investigating Acts of Fraud and Non-compliance.
- Protocol for the Prevention and Resolution of Harassment Conflicts in the Workplace.