Welcome to the Political Complaints Channel

Strategic need to mitigate the risk of regulatory non-compliance.

Whistleblowing Channel Policies

A. Legal obligation.

B. Who can make an internal complaint.

C. Basic principles of the Whistleblowing Channel.

D. Legality of the processing of personal data.

E. Information on protection of personal data.

F. Preservation of the identity of the informant

G. Processing of personal data.

H. Prohibition of retaliation.

I. Protection measures against retaliation.

J. Protection measures for affected people.

K. Cases of exemption and mitigation of the sanction.

A Legal obligation

The entry into force of LO2/2023 Regulating the Protection of people who report Regulatory Violations and the Fight against Corruption requires the implementation of an Internal Information System (SIII). That is, to have an Internal Complaints Channel. Who obliges:

- Companies with more than 50 workers.
- Public organisms.
- Public Law Corporations.
- Public universities.
- Public Sector Foundations.
- Political parties.
- Unions.
- Business organizations.

Our company considers it essential to promote compliance with the law and carry out its activity under the principles of good corporate practices and, for this reason, a Whistleblowing Channel is created as a means to "impose the obligation" to communicate possible irregularities or illegal acts that occur within it.

The Whistleblowing Channel is established as the instrument through which any person who is a member of the company or linked to it can and must report events related to breaches of current legislation, both those that have already occurred and those that are suspected of having occurred.

B Who can file an internal complaint?

Any person who has information about possible regulatory infractions in a work or professional context can be a whistleblower.

Therefore, all members of the company, regardless of their position or functions, as well as its clients, business partners, suppliers and collaborators have the right and duty to communicate and inform the company through their Whistleblowing Channel those irregularities or well-founded suspicions of regulatory non-compliance of which they have knowledge, especially if they constitute illegal acts or professional criminals.

Faq. Are anonymous complaints allowed?

The Law allows the complaint to be made anonymously.

However, when it comes to a complaint about workplace harassment or sexual harassment, the complainant must identify themselves.

Faq. Is the content of the complaint a numerus clausus?

It is not a closed number. The law establishes that any violation of Union Law will be reported.

Faq. How to file an internal complaint?

You have our company's Complaints Channel open.

The electronic platform will guide you on how to complete your complaint.

You can make the report anonymously. In this case, you must refrain from completing personal data.

There is an exception. If the complaint is for workplace harassment or sexual harassment, it must be identified by legal imperative.

Otherwise, you must complete them so that the person responsible for the Whistleblowing Channel can contact you.

If you decide not to complete this identification data, we will understand that you do not want the Complaint Channel Manager to contact you.

Faq. Is the Complaints Channel a complaints mailbox?

Absolutely not. This Whistleblowing Channel should only be used to report regulatory breaches. Under no circumstances to make complaints about the operation of the company in any of its areas.

If you consider that our behavior deserves a complaint, please let us know through another channel. We welcome your feedback as an opportunity to improve.

Basic Principles of the Whistleblowing Channel

The company's Complaints Channel must be an open mechanism for listening to internal complaints through which avenues of investigation and areas of opportunity are generated for the company to mitigate the risk of regulatory non-compliance.

The principles that govern the operation and management of our company's Whistleblowing Channel are the following:

1. **Transparency and accessibility**. The Whistleblower Channel will be publicly known through the company's website and will be easily accessible through an online form there and a specific email for this purpose, arranged for these purposes.
2. **Confidentiality**. Commitment to guarantee confidentiality regarding the identity of the people who use it, as well as the content of their communications.
3. **Good faith.** Communications made through the Complaints Channel will be made in good faith and honesty.
4. **Objectivity and Impartiality**. The communications must be based on truthfulness and will be complete and accurate, even if it is subsequently verified that their content was misleading.
5. **Objectivity and Impartiality.** All communications made and received

through your Complaints Channel will be treated and managed under the same criteria, regardless of who makes them and who they relate to, without establishing any difference or privilege based on the circumstances that occur in the case. their people and their situation in the hierarchical and functional organization chart of the company.

C Lawfulness of personal data processing

1. The necessary processing of personal data will be considered lawful.
2. The processing of personal data, in the cases of internal communication, will be understood to be lawful by virtue of the provisions of articles 6.1.c) of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, 8 of Organic Law 3/2018, of December 5, and 11 of Organic Law 7/2021, of May 26, when, in accordance with the provisions of articles 10 and 13 of this law, it is mandatory to have an internal information system. If it is not mandatory, the treatment will be presumed to be covered by article 6.1.e) of the aforementioned regulations.
3. The processing of personal data in the cases of external communication channels will be understood to be lawful by virtue of the provisions of articles 6.1.c) of Regulation (EU) 2016/679, 8 of Organic Law 3/2018, of 5 of December, and 11 of Organic Law 7/2021, of May 26.
4. 4. The processing of personal data derived from a public disclosure will be presumed covered by the provisions of articles 6.1.e) of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, and 11 of Organic Law 7/2021, of May 26.
5. The processing of special categories of personal data by reasons of essential public interest may be carried out in accordance with the provisions of article 9.2.g) of Regulation (EU) 2016/679.

D Information on personal data protection

1. When personal data is obtained directly from the interested parties, they will be provided with the information referred to in articles 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, and 11 of the Organic Law 3/2018, of December 5.
2. Informants will also be expressly informed that their identity will in all cases be reserved, and that it will not be communicated to the people to whom the reported events refer or to third parties.
3. The person to whom the reported events refer will under no circumstances be informed of the identity of the informant or of the person who carried out the public disclosure.
4. Interested parties may exercise the rights referred to in articles 15 to 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016.
5. In the event that the person to whom the facts related in the communication refer exercise the right of opposition, it will be presumed that, unless proven otherwise, there are compelling legitimate reasons that legitimize the processing of their personal data.

E Preservation of the identity of the informant

1. Whoever submits a communication or makes a public disclosure has the right not to have his or her identity revealed to third parties.
2. Internal information systems, external channels and those who receive public disclosures will not obtain data that allows the identification of the informant and must have appropriate technical and organizational measures to preserve the identity and guarantee the confidentiality of the data corresponding to the disclosures. affected persons and any third party mentioned in the information provided, especially the identity of the informant if he or she has been identified.
3. 3. The identity of the informant may only be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority within the framework of a criminal, disciplinary or sanctioning investigation.

   Disclosures made under this section will be subject to safeguards established in the applicable regulations. In particular, it will be transferred to the informant before revealing his or her identity, unless such information could compromise the investigation or the judicial procedure. When the competent authority communicates it to the
   formant, will send you a letter explaining the reasons for the disclosure of the confidential data in question.

Faq. Who are protected as whistleblowers?

The protection of the identity of the complainant is one of the main objectives of LO 2/2023.

Our company is committed to the principle of confidentiality regarding the identity of informants.

The protection reaches any natural person. Not only to workers, but also to any third party who files the complaint.

Failure to comply with this obligation will be considered a serious infraction that will be sanctioned in accordance with Organic Law 2/2023.

F Processing of personal data in the Complaints Channel

1. 1. Access to personal data contained in the Internal Information System will be limited, within the scope of its powers and functions, exclusively to:

   a) The person responsible for the system and whoever manages it directly.

   b) The person responsible for human resources or the duly designated competent body, only when the adoption of disciplinary measures against a worker could be appropriate. In the case of public employees, the body competent to process the same.

   c) The person responsible for the legal services of the entity or organization, if the adoption of legal measures is appropriate in relation to the facts reported in the communication.

   d) Those in charge of the treatment that may eventually be designated. e) The data protection delegate.
2. The processing of data by other people, or even its communication to third parties, will be lawful when it is necessary for the adoption of corrective measures in the entity or the processing of sanctioning or criminal procedures that, where appropriate, may apply.
3. In no case will personal data that are not necessary for the knowledge and investigation of the actions or omissions referred to in article 2 be subject to processing, and, where appropriate, they will be immediately deleted. Likewise, all personal data that may have been communicated and that refer to conduct that is not included in the scope of application of the law will be deleted. If the information received contains personal data included within the special categories of data, it will be immediately deleted, without proceeding to its registration and processing.
4. The data that are subject to processing may be kept in the information system only for the time necessary to decide on the appropriateness of initiating an investigation into the reported facts. If it is proven that the information provided or part of it is not truthful, it must be immediately deleted from the moment there is evidence of said circumstance, unless said lack of truthfulness may constitute a criminal offense, in which case it will be kept. the information for the necessary time during which the judicial procedure is processed.
5. 5. In any case, after three months from receipt of the communication without investigation actions having been initiated, it must be deleted, unless the purpose of conservation is to leave evidence of the operation of the system. Communications that have not been processed may only be recorded in anonymized form, without the blocking obligation provided for in article 32 of Organic Law 3/2018, of December 5, being applicable. 5. Employees and third parties must be informed about the processing of personal data within the framework of the information systems referred to in this article.

G Prohibition of Retaliation.

1. Acts constituting retaliation, including threats of retaliation and attempted retaliation against persons who submit a communication in accordance with the provisions of this law, are expressly prohibited.
2. Retaliation is understood to mean any acts or omissions that are prohibited by law, or that, directly or indirectly, involve unfavorable treatment that places the people who suffer them at a particular disadvantage with respect to others in the labor or employment context. professional, solely because of their status as informants, or for having made a public disclosure.
3. For the purposes of the provisions of this law, and by way of example, reprisals are considered to be those adopted in the form of:
   a) Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including the non-renewal or early termination of a temporary employment contract once the trial period has passed, or early termination or cancellation of employment contracts. goods or services, imposition of any disciplinary measure, demotion or denial of promotions and any other substantial modification of working conditions and the non-conversion of a temporary employment contract into an indefinite one, in the event that the worker had legitimate expectations that he would be offered a permanent job; unless these measures were carried out within the regular exercise of management power under the protection of labor legislation or legislation regulating the status of the corresponding public employee, due to proven circumstances, facts or infractions, and unrelated to the presentation 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) Inclusion in blacklists or dissemination of information in a certain sectoral area, which hinders or prevents access to employment or the contracting of works or services.
   e) Denial or cancellation of a license or permit.
   f) Denial of training.
   g) Discrimination, or unfavorable or unfair treatment.
4. The person who sees their rights harmed due to their communication or disclosure after the two-year period has elapsed may request protection from the competent authority which, exceptionally and in a justified manner, may extend the protection period. , after hearing the people or bodies that could be affected. The denial of the extension of the protection period must be motivated.
5. Administrative acts that are intended to prevent or hinder the presentation of communications and disclosures, as well as those that constitute retaliation or cause discrimination after the presentation of those under this law, will be null and void and will give rise, in their case, to corrective disciplinary or liability measures, which may include the corresponding compensation for damages to the injured party.
6. The Independent Whistleblower Protection Authority, A.A.I. may, within the framework of the sanctioning procedures that it instructs, adopt provisional measures in the terms established in article 56 of Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations. Article 37. Support measures. 1. People who communicate or reveal infringement.

H Protection measures against retaliation

1. Persons who communicate information about the actions or omissions covered by this law or who make a public disclosure in accordance with this law will not be considered to have violated any restriction on disclosure of information, and they will not incur liability of any kind in in relation to 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 reveal an act or omission under this law, all without prejudice to the provisions of art. - article 2.3. This measure will not affect criminal responsibilities. The provisions of the previous paragraph extend to the communication of information made by the representatives of the workers, even if they are subject to legal obligations of secrecy or not to reveal confidential information. All this without prejudice to the specific protection rules applicable in accordance with labor regulations.
2. Informants will not incur liability with respect to the acquisition or access to information that is communicated or revealed publicly, provided that said acquisition or access does not constitute a crime.
3. Any other possible liability of informants arising from acts or omissions that are not related to the public communication or disclosure or that are not necessary to reveal a violation under this law will be enforceable in accordance with applicable regulations.
4. In proceedings before a court or other authority concerning harm suffered by whistleblowers, once the whistleblower has reasonably demonstrated that he or she has communicated or made a public disclosure in accordance with this law and that he or she has suffered harm. harm, it will be presumed that the harm occurred in retaliation for reporting or making a public disclosure. In such cases, it will be up to the person who took the harmful measure to prove that the measure was based on duly justified reasons not linked to the public communication or disclosure.
5. In judicial proceedings, including those relating to defamation, violation of copyright, violation of secrecy, violation of data protection regulations, disclosure of business secrets, or requests for compensation based on labor law or statutory, the persons referred to in article 3 of this law will not incur liability of any kind as a consequence of communications or public disclosures protected by it. Said persons will have the right to allege in their defense and within the framework of the aforementioned judicial processes, having communicated or made a public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure was necessary to put reveals a violation under this law.

I Measures to protect affected people

1. During the processing of the file, the people affected by the communication will have the right to the presumption of innocence, the right of defense and the right of access to the file in the terms regulated in this law, as well as the same protection. established for informants, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

J Cases of exemption and mitigation of the sanction

1. When a person who has participated in the commission of the administrative infraction that is the subject of the information is the one who informs of its existence by presenting the information and provided that it had been presented prior to it having been Once notified of the initiation of the investigation or sanctioning procedure, the body competent to resolve the procedure, by means of a reasoned resolution, may exempt you from compliance with the administrative sanction that corresponds to you as long as the following points are proven in the file: a) Have ceased to commit the infraction at the time of presentation of the communication or disclosure and identified, where appropriate, the rest of the people who have participated in or favored it. b) Have cooperated fully, continuously and diligently throughout the entire investigation procedure. c) Having provided truthful and relevant information, means of proof or significant data for the accreditation of the facts investigated, without having proceeded to destroy them or hide them, nor having revealed their content to third parties, directly or indirectly. d) Have proceeded to repair the damage caused that is attributable to you.
2. When these requirements are not met in their entirety, including partial repair of the damage, it will be at the discretion of the competent authority, after assessing the degree of contribution to the resolution of the file, the possibility of mitigating the sanction that would have corresponded to the infraction committed. , provided that the informant or author of the disclosure has not previously been sanctioned for facts of the same nature that gave rise to the initiation of the procedure.
3. The mitigation of the sanction may be extended to the rest of the participants in the commission of the infraction, depending on the degree of active collaboration in clarifying the facts, identification of other participants and repair or reduction of the damage caused, assessed. by the body in charge of the resolution. 4. The provisions of this article will not apply to the infractions established in Law 15/2007, of July 3, on the Defense of Competition.

Remember

The Complaints Channel
it is a corporate tool for continuous improvement.