# OPERATION POLICY OF THE ETHICAL CHANNEL OF TECNO-SPUMA, SL

November 2023

## IMPORTANT INFORMATION ABOUT THE DOCUMENT

| | |
|---|---|
| **Document name:** | Ethical Channel Operation Policy |
| **Standard that develops:** | Tecno-Spuma Code of Ethics |
| **Author:** | System Manager (Compliance Committee) |
| **Responsible for compliance:** | System Manager (Compliance Committee) |
| **Approval body:** | Administrative Body (Board of Directors) |
| **Approval date of the current version:** | November 2023 |

## HISTORY OF VERSIONS AND MODIFICATIONS

| Version: | Date: | Author: | Approval Body: | Summary of changes: |
|---|---|---|---|---|
| V.1 | November 2023 | System Manager (Compliance Committee) | Administration organ | New Policy |

# INDEX

# 1. PURPOSE AND OBJECT

The purpose of this Policy for the Operation of the Ethical Channel (hereinafter, the " **Policy** ") is to define and establish an ideal and effective model for the operation of the Internal Information System (hereinafter, the " **Ethical Channel** ") of TECNO- SPUMA, SL (hereinafter, "TECNO-SPUMA", or the "Company", interchangeably), adapted to the regulations on this matter (DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of October 23, 2019 regarding to the protection of people who report violations of Union Law (hereinafter, " **Whistleblower Directive** ") and Law 2/2023, of February 20, regulating the protection of people who report regulatory and combat violations against corruption (hereinafter, " **Law for the Protection of Whistleblowers** "), as well as the highest national and international standards in force (UNE-ISO 37002:2021 on Whistleblowing Management Systems. Guidelines), which allows you to receive and process:

- On the one hand, communications related to non-compliance and/or practices contrary to the principles established in the Code of Ethics and the Policies, and Protocols of TECNO-SPUMA, as well as in the internal rules and procedures that develop them and in the other regulations that come. imposed by the regulatory framework of the organization and/or,

- On the other hand, actions or omissions that may constitute violations of European Union law or serious or very serious criminal or administrative violations of Spanish national law.

This Policy establishes the procedure that regulates the operation of the TECNO-SPUMA Ethical Channel, in such a way that it includes issues related to the making of communications by the reporting persons, as well as the management and resolution of the same by the System Manager.

The purpose of this Policy is to guarantee professional, confidential, impartial management and maximum protection of the rights of the interested parties (including the rights recognized in the personal data protection regulations) throughout the entire process of realization, management , processing, investigation and resolution of communications made through the TECNO-SPUMA Ethical Channel.

In this regard, this Policy establishes three basic guarantees:

i) guarantee of protection of informants;
ii) guarantee of absence of reprisals to the reporting persons and
iii) guarantee of the rights of the accused during the management and processing of communications.

## 2. SCOPE

This Policy is applicable to all members of TECNO-SPUMA (including both workers and managers, as well as shareholders and members of the Administrative Body, regardless of the position or position they occupy within the organization, the nature legal nature of their relationship and whatever their area of activity or hierarchical level), who are aware, in a work or professional context, of any infraction established in section 1 of this Policy.

Likewise, what is established in this Policy will also be extended to third parties such as: business partners, collaborating companies, subcontractors, suppliers and other people or entities that have a professional relationship with TECNO-SPUMA.

## 3. PRINCIPLES OF THE ETHICAL CHANNEL

### 3.1. CONFIDENTIALITY

TECNO-SPUMA guarantees the maximum confidentiality of the communications received through its Ethical Channel and the data contained therein.

The identity of the person who reports an irregularity through the Ethical Channel will be considered confidential information and, therefore, will not be communicated to the person reported. In the same sense, the confidentiality of the identity of the person reported will be guaranteed.

Likewise, there is an express prohibition on the personal data contained in the communication and resulting from the investigation carried out being known to any person other than those expressly authorized. In this sense, specific confidentiality commitments will be signed with the people in charge of managing them.

Without prejudice to the foregoing, the data of the person making the communication may be provided to the administrative, judicial authorities or the Public Prosecutor's Office, to the extent that they are required by such authorities as a consequence of any criminal, disciplinary or sanctioning procedure derived of the object of the communication.

Said transfer of data will always be carried out in full compliance with the legislation on the protection of personal data, requiring that in all cases access by third parties to it be prevented.

When the communication is sent through reporting channels other than those established in this Policy or to members not responsible for its treatment or to

non-competent personnel, there will be an obligation on the part of the recipient of the communication to immediately send it to the System Controller, guaranteeing its confidentiality at all times. Failure to comply with this obligation will be classified as a very serious infraction, for which TECNO-SPUMA may adopt appropriate disciplinary measures.

### 3.2. INDEPENDENCE

The processing, investigation and resolution procedures and, in general, the management of communications received through the TECNO-SPUMA Ethical Channel will be governed by maximum objectivity and independence, establishing in this Policy the corresponding mechanisms in order to avoid concurrence of possible conflicts of interest.

### 3.3. GOOD FAITH

All communications submitted through the Ethical Channel must be made in good faith. Which means that, at the time of submitting the communication, the reporting person must have reasonable and sufficient grounds to believe that the information indicated is true, truthful and that it contains possible violations.

In this sense, false or malicious communications or complaints may give rise to the corresponding sanctions by TECNO-SPUMA, without prejudice to the civil and even criminal liabilities that may arise.

### 3.4. PROHIBITION OF RETALIALS

TECNO-SPUMA undertakes not to adopt any form of retaliation, threats of retaliation or attempted retaliation, direct or indirect, against people who, in good faith, have reported any irregularity through the Ethical Channel.

Retaliation should be understood as any act or omission that is prohibited by law, or that, directly or indirectly, involves unfavorable treatment that places the people who suffer it at a particular disadvantage with respect to others in the work or professional context. , only because of their status as informants.

Protection against retaliation also extends to people who report possible violations through the external information channels mentioned in section 6 of this Policy.

In addition to reporting persons, the prohibition of retaliation established in this Policy also extends to the following persons:

1. natural persons who, within the framework of the organization in which the reporting person provides services, assist them in the process;

2. natural persons who are related to the reporting person and who may suffer retaliation, such as co-workers or family members, and

3. legal entities, for which the reporting person works or with which they maintain any other type of relationship in a work context or in which they have a significant participation. For these purposes, it is understood that the participation in the capital or in the voting rights corresponding to shares or participations is significant when, due to its proportion, it allows the person who owns it to have the capacity to influence the invested legal entity.

In the event that any member of TECNO-SPUMA, in contravention of the provisions of this Policy, takes direct or indirect retaliation, it will be the organization itself that will take the necessary measures to stop the retaliation as soon as possible and, when appropriate, take disciplinary measures. that are appropriate against those responsible for them .

Likewise, through this Policy, the rights to privacy, to be heard, to be informed of the actions or omissions attributed to them, to defense, to honor and to the presumption of innocence of the targeted persons will also be guaranteed. of the investigation, as well as the right to access the file.

# 4. OPERATION OF THE ETHICAL CHANNEL

## 4.1. PRESENTATION OF COMMUNICATIONS

### 4.1.1. AVAILABLE CHANNELS

Informants may make communications through the channels provided for this purpose.

In this sense, TECNO-SPUMA makes available the following channels to carry out the communications included in this Policy:

- Accessing the channel enabled for these purposes on the corporate website ( www.tecno-spuma.com )
- By ordinary mail to the postal address: Carrer Santa Coloma (Pol. Industrial Puigció ), 16, 17412 Maçanet de la Selva, (Girona) (To the exclusive attention of the System Manager - Compliance Committee)

At the request of the reporting person, the communication may also be presented through a face-to-face meeting with the System Manager, which, if applicable, must be carried out within a maximum period of seven (7) days from the request.

#### 4.1.2. COMMUNICATION INFORMATION

The communication must contain the following information:

- Identity of the reporting person (names, surnames and ID). Except in cases of anonymous communications. In this sense, the TECNO-SPUMA Ethics channel allows communications to be carried out anonymously, without providing the identity of the reporting person.

- Relationship with TECNO-SPUMA (employee, supplier, shareholder, subcontractor, intern, etc.) and, where applicable, position at TECNO-SPUMA.

- Description as detailed and complete as possible of the conduct, event or alleged irregularity that is reported.

- Identity of the person reported (name, surname and position), if the person responsible for the event is known and the area in which the event being reported occurred.

- Indications, explanatory explanations or evidence on which the information is based. All available evidence must be provided or indicated where and how to obtain it ( e.g. witnesses, documents, records, etc.).

- Approximate dates of the occurrence of the events.

- If applicable, means of communication (address, email, telephone or other) of the reporting person so that the System Responsible can make notifications or communications.

If the content of the communication has been evaluated, it lacks the minimum requirements that are mandatory for its correct evaluation, by the System Manager, the corresponding information and/or documentation will be requested from the reporting person through the means of communication. indicated by this, proceeding to archive the communication, in case of not having the necessary information to open the investigation phase.

### 4.2. COMMUNICATIONS MANAGEMENT AND RESOLUTION

#### 4.2.1. SYSTEM RESPONSIBLE

The Administrative Body of TECNO-SPUMA, SL is the competent body for the appointment, as well as dismissal or dismissal, of the System Manager, who, in

turn, is responsible for the management and processing of communications that enter through of the TECNO-SPUMA Ethical Channel.

The person responsible for the System may be a natural person or a collegiate body that must delegate to one of its members (natural person) the powers of management and processing of research files.

Both the appointment and the dismissal of the System Manager will be notified to the Independent Authority for the Protection of Informants (AAI) or, where appropriate, to the competent authorities or bodies of the autonomous communities.

In this sense, the Administrative Body of TECNO-SPUMA, SL has designated a collegiate body, the Compliance Committee of the organization, as System Manager, who, in turn, has designated one of its members (natural person) to carry out the powers of management and processing of the Ethical Channel communications.

The System Manager will act independently from the rest of the functions and hierarchical or functional subordination that, if applicable, may exist, developing the necessary tasks under the premises of confidentiality, respect, independence, neutrality, impartiality, honesty and objectivity towards people. affected by the communication in question, also ensuring that the procedure is carried out in accordance with the procedures and principles established in this Policy.

In the event that the System Controller has incompatibility or conflict of interest with the fact or persons that are the subject of the communication, he or she will refrain from participating in the management and processing of the communication and will therefore not have access to the information derived from the actions carried out in its management. In this regard, the System Manager will be replaced by another person designated and appointed by the General Director or, where appropriate, the Administrative Body or other competent body.

- **Competencies of the System Manager**

The main competencies of the System Manager in the field of management of the TECNO-SPUMA Ethical Channel are the following:

- Manage the Ethical Channel tool.
- Receive communications made through the Ethical Channel.
- Analyze the content of the communications received and decide on their admission for processing.
- Determine the convenience or need to adopt immediate measures to avoid (stop or mitigate) further damage.

- In the case of nominative complaints (or, being initially anonymous, from the moment in which, where appropriate, the reporting person communicates his or her identity), the reporting person will be notified of receipt of the complaint (sending acknowledgment of receipt), except that this may jeopardize the confidentiality of the communication.
- Ensure that appropriate measures are taken to prevent and avoid possible retaliation against the complainant.
- Carry out the investigation/instruction of the facts internally in accordance with the rules and principles established in this Policy (or decide on the origin of its investigation through an external expert manager).
- Prepare a report on the result of the investigation carried out, highlighting whether the reported facts are considered proven and propose the appropriate measures to resolve the fact, as well as, where appropriate, the disciplinary measures to be taken, always being able to delegate this authority to another competent body.
- Inform interested parties (including the reporting person) of the completion of the procedure.
- Extend the resolution period for reasons of complexity.
- Resolve doubts and queries that arise in relation to the Channel.
- Keep the Complaints Registry Book updated.
- Ensure that the necessary security of the communications Information Management System is established, including the restriction of access to it.
- Manage the storage of communication information in the Communications Information Management System.

The System Manager will develop these functions and powers independently and autonomously with respect to the rest of the organization's bodies.

For the performance of the above functions and powers, and in those cases in which it is deemed necessary, the System Manager may be assisted by an external consultant or even delegate some of the above functions to the latter. In this sense, the System Manager must obtain a confidentiality agreement from external collaborators, involved in the management and resolution of the communication. Likewise, it will collect it from internal collaborators when it deems necessary.

### 4.2.2. RECEPTION AND EVALUATION

Once a communication is received through the Ethical Channel, the System Manager will proceed to register it in a Communications Registry Book, assigning the communication an identification code.

The Communications Registry Book is contained in a secure database (Information Management System) with access restricted exclusively to

authorized persons, and all communications and information received through the Ethical Channel and during processing will be recorded. from the same.

In each of the communications records recorded in the Communications Record Book, the following data will be included:

- Reception date.
- Identification code.
- Actions developed.
- Measures taken.
- Deadline.

The Registry Book will not be public and only at the reasoned request of the competent judicial authority, by means of an order, and within the framework of a judicial procedure and under the guardianship of the latter, its contents may be accessed in whole or in part.

Once the communication is received, within a maximum period of seven (7) calendar days following its receipt, the System Manager will send an acknowledgment of receipt of the communication to the reporting person, unless the reporting person is anonymous; that the complainant has renounced receiving communications related to the investigation or; that this may jeopardize the confidentiality of the communication.

If the reporting person accepts it, the possibility is expressly provided for the System Responsible to maintain the communication.

The System Manager will check the content of the communication. If documentation is missing or has some formal defect, a request for information will be made to the reporting person. Likewise, the Responsible Party, if it considers it necessary, may request additional information from the reporting person regarding the communication made.

The System Manager must check whether the communication exposes facts or conduct that are within the scope of application of this Policy and, therefore, whether its admissibility is appropriate.

Once this preliminary analysis has been carried out, the System Manager, within a period that may not exceed ten (10) business days from the date the communication information is entered in the Registry Book, must:

a) Admit the communication to processing.

b) Disallow communication, in any of the following cases:

1. When the facts reported lack all plausibility.

2. When the facts reported do not constitute a violation of the assumptions established in this Policy.

3. When the communication is manifestly unfounded or there are, in the opinion of the System Controller, rational indications of having been obtained through the commission of a crime.
   In the latter case, in addition to the inadmissibility, a detailed list of the facts that are considered to constitute a crime will be sent to the Public Prosecutor's Office.

4. When the communication does not contain new and significant information about infringements compared to a previous communication in respect of which the corresponding procedures have been concluded, unless new factual or legal circumstances arise that justify a different follow-up.
   In these cases, the System Manager will notify the resolution to the reporting person in a reasoned manner.

Likewise, communications in which the facts described are misleading and/or there is corroboration that the communication was made in bad faith, that is, with the intention of harming the organization or third parties related to it, will not be admitted.

c) Send, immediately, the information to the Public Prosecutor's Office when the facts could indirectly constitute a crime or to the European Public Prosecutor's Office in the event that the facts affect the financial interests of the European Union.

d) Send the communication to the authority, entity or body that is considered competent for its processing .

The decision to admit, reject or forward the communication will be communicated by the System Manager to the reporting person within five (5) business days following the decision, unless the communication is anonymous or the reporting person would have renounced receiving communications.

The System Manager will also assess the convenience or need to adopt immediate measures to avoid further damage and, where appropriate, execute them.

#### 4.2.3. PROCESSING AND INVESTIGATION

Once the communication is admitted for processing, the System Manager, acting as instructor, will carry out all necessary actions, procedures and

investigations aimed at verifying the plausibility of the facts of the communication, and may entrust this task to an external expert. if circumstances require it.

Thus, the veracity and accuracy of the information contained in the communication and, in particular, of the communicated conduct will be verified, following at all times the principles established in this Policy and under a strict regime of confidentiality to respect the rights of the reporting person and the person investigated.

During the investigation, the person investigated will be notified of the communication with a brief summary of the facts established therein. This information may be provided during the hearing process of the investigated person, if it is considered that its prior contribution could facilitate the concealment, destruction or alteration of the evidence.

Without prejudice to the right to make allegations in writing, the investigation will include, whenever possible, an interview with the person reported in which, always with absolute respect for the presumption of innocence, he will be invited to present his version of the facts and provide those means of proof that it considers appropriate and relevant.

In order to guarantee the right of defense of the person reported, he or she will have access to the file (without revealing information that could identify the reporting person) and may be heard at any time. Likewise, you will be warned of the possibility of appearing assisted by a lawyer.

In addition, the instructor will give hearings to all affected people and possible witnesses and will carry out whatever procedures he deems necessary (review of documentation, obtaining information from external sources, etc.). In this regard, all members of the organization are obliged to collaborate loyally in the investigation that is carried out. The intervention of witnesses and affected people will be strictly confidential.

The researcher may collect all the information and documentation that he considers appropriate from any area or department of the organization, in order to substantiate the investigation.

Of all the investigation actions and, in particular, of the explanations/statements given by the people who have intervened in the communication investigation procedure, a written record will be drawn up (provided that their prior consent is obtained), record that will be duly signed by the persons involved in order to certify its content and that it conforms to their declaration. The content of said minutes will be incorporated into the TECNO-SPUMA Information Management System with the same guarantees of confidentiality as the rest of the file.

In the event that the presence of the person investigated during the instruction period could compromise the development of the investigation or the strict observance of the guiding principles of the procedure established in this Policy, at the proposal of the instructor, the person may be granted investigated a paid leave to be absent from her job, without loss of remuneration, in order to guarantee the carrying out of the necessary research activities without interference that could harm her. The paid leave will be granted for the time essential to carry out the appropriate research work, and in no case may it be extended beyond the duration of the research process.

The presence of external legal advisors will be allowed in the hearings/statements of the affected parties, interested parties, witnesses, etc., if the instructor deems it appropriate.

In all investigation procedures, compliance with the principles contained in this Policy will be especially monitored and confidentiality, impartiality, as well as the rights to privacy, defense, honor and the presumption of innocence of the persons subject to investigation will be guaranteed. investigation. Likewise, the procedure will be transparent and will guarantee the right to information of the people involved in it.

#### 4.2.4. RESOLUTION AND COMMUNICATION

Once all the investigation actions have been completed, the System Manager will prepare and issue a report that will contain at least the following content:

- A statement of the facts reported (descriptive information of the communication) together with the identification code of the communication and the date of registration.
- Assessment of the content of the communication.
- The actions carried out in order to verify the plausibility of the facts.
- The conclusions reached in the investigation and the assessment of the proceedings and the evidence that supports them.
- Measures adopted (if any).

Once the Report is issued, the System Manager will adopt one of the following decisions:

a) File of the file , which will be notified to the reporting person and, where appropriate, to the affected person.

b) Proposal for resolution of the file and, where appropriate, the corresponding proposals for actions and/or proposals for disciplinary measures , always being able to delegate this last power to another competent body.

c) Referral to the Public Prosecutor's Office if, despite not initially seeing indications that the facts could have the character of a crime, this results from the course of the investigation. If the crime affects the financial interests of the European Union, it will be referred to the European Public Prosecutor's Office.

d) Referral of the communication to the authority, entity or body that is considered competent for its processing .

The maximum period to respond to the investigation actions may not exceed three (3) months from the receipt of the communication, except in cases of special complexity that require an extension of the period, in which case, it may be extended. , by decision of the System Manager, up to a maximum of another three (3) additional months.

The proposed resolution will be sent to the Director General or, where appropriate, to the Administrative Body or competent body, who must adopt and execute the final resolution.

Whatever the decision, it will be communicated to the reporting person within five (5) business days of the decision being made, unless they have waived it or the communication is anonymous, as well as to the rest of the affected parties.

In the event that the resolution issued concludes that a member of TECNO-SPUMA has committed an irregularity, the legally appropriate disciplinary, administrative or judicial actions will begin.

Likewise, if as a result of the investigation proceedings other facts are discovered that could constitute new irregularities supposedly committed by the same or different persons of those investigated, the instructor will propose the opening of a new file, or if it is related to what was instructed in the file that was being carried out, the expansion of the investigative file, if it is considered more appropriate.

#### 4.2.5. DISCIPLINARY MEASURES

When it is determined that the reported conduct constitutes a violation in labor matters, TECNO-SPUMA may adopt the appropriate measures in accordance with the applicable disciplinary regime and, specifically, with the provisions of the Collective Agreement applicable in TECNO-SPUMA and in the Spanish Workers' Statute.

Without prejudice to the fact that the mandatory labor regulations applicable at all times will be observed in all cases, to the extent that they allow it, to assess

the seriousness of the conduct, for the purposes of grading the sanctions to be imposed, The following criteria may be considered, among others:

- Degree of intentionality;
- Failure to comply with prior warnings;
- Recidivism;
- Concurrence of several violations in the same act or activity;
- Concurrence of concealment in the conduct carried out by the offending person;
- Concurrence of continuity in the conduct carried out by the offending person;
- The rectification of the breach that gave rise to the infringement on the offending person's own initiative;
- Repair of damages or losses caused by the offending person;
- Level of responsibility in the organization of the offending person;
- Magnitude of the economic damage derived from the infringement;
- Magnitude of any other damages not economically assessable, derived from the infringement;
- Impact on other employees or third parties;
- Collaboration with the organization.

Notwithstanding the adoption of disciplinary measures, when the facts could indirectly constitute a crime, the corresponding information will be sent immediately to the Public Prosecutor's Office. In the event that the events affect the financial interests of the European Union, it will be referred to the European Public Prosecutor's Office.

# 5. DATA PROTECTION AND CONSERVATION

## 5.1. RESPONSIBLE FOR THE TREATMENT

In compliance with the provisions of the General Data Protection Regulation and the Data Protection Law, you are informed that the personal data that, where appropriate, could be included in the communication, will be integrated into a file owned by TECNO-SPUMA for your treatment.

TECNO-SPUMA is committed to maintaining strict protection of privacy, security and data conservation, as detailed in our policies and procedures and internal regulations on these matters. In this sense, these rules will also apply with respect to all personal data related to communications made in accordance with this Policy.

## 5.2. DATA COLLECTION

In the processing of communications (realization and investigation thereof) carried out in accordance with this Policy, TECNO-SPUMA collects the following personal data:

- Name and contact information of the reporting person (unless reporting anonymously) and their status as an employee of TECNO-SPUMA;

- Name and other personal information of the people mentioned in the complaint (witnesses, possible infringing person, etc.), if such information is provided (description of their functions, contact information and participation or role in the reported events);

### 5.3. PRESERVATION OF THE IDENTITY OF THE REPORTING PERSON AND OTHER AFFECTED PEOPLE

TECNO-SPUMA will preserve the identity and guarantee the confidentiality of the data corresponding to the affected persons and any third party mentioned in the information provided, especially the identity of the reporting person if they have been identified. In this sense, the person to whom the facts reported in the communication refer will under no circumstances be informed of the identity of the reporting person.

In this sense, whoever submits a communication has the right not to have his or her identity revealed to third parties. The identity of the reporting person 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.

These disclosures will be subject to safeguards established in applicable regulations. In particular, the reporting person will be contacted before revealing his or her identity, unless such information could compromise the investigation or judicial procedure.

### 5.4. DATA CONSERVATION

TECNO-SPUMA will maintain a record of all communications received. These records and the personal data they contain will be kept confidential in the Information Management System. The records will not be kept longer than necessary and in any case for as long as necessary to comply with any applicable legal requirement at any given time.

TECNO-SPUMA will keep the personal data of the complainant for the time necessary to decide on the appropriateness of initiating an investigation into the facts or conduct reported and, once decided, they will be deleted from the Ethics Channel, and may be processed outside the system to investigate the facts by the time needed to make a decision. Once the investigation of the communication has been completed and the appropriate actions have been

taken, where appropriate, the data of those complaints that have been processed will remain duly blocked to comply with the legal obligations that, in each case, correspond.

Personal data will be deleted from the Ethics Channel within a maximum period of three (3) months from receipt of the communication, unless the purpose of conservation is to leave evidence of the operation of the system, and may continue to be processed outside the Ethics Channel in case that the investigation of the complaint had not been completed, during the necessary time. In no case may the data be kept for a period of more than ten years.

In the event that it is decided not to pursue the complaint filed, the information may be kept anonymously.

### 5.5. ACCESS TO DATA

Access to personal data contained in the Ethical Channel 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 external advisor involved in the investigation, with whom the corresponding confidentiality agreements will be signed.

c) The human resources manager of TECNO-SPUMA or the duly designated competent body, only when disciplinary measures could be adopted against a worker.

d) The person responsible for the legal services of TECNO-SPUMA, if the adoption of legal measures is appropriate in relation to the facts reported in the communication.

e) Those in charge of the treatment that are eventually designated.

### 5.6. PURPOSE OF TREATMENT

Only personal data that is strictly necessary for the purposes of managing, processing and investigating communications relating to the commission of irregularities is processed, as well as carrying out the necessary actions for the investigation of the reported facts, including, where appropriate, , the adoption of disciplinary or legal measures, as appropriate.

Personal data will not be used for a purpose other than that indicated.

### 5.7. RIGHTS OF INTERESTED PERSONS

Interested persons, at any time and in the terms provided by the applicable regulations, may exercise the following rights with respect to their personal data: access, rectification, deletion (right to be forgotten), limitation of processing, opposition; portability, decision on automated treatments, information and claims.

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.

If they deem it appropriate, interested parties may also file a claim with the competent data protection authority.

### 5.8. INFORMATION ON DATA PROTECTION AND EXERCISE OF RIGHTS

Those who wish can obtain more information about the processing of their personal data by contacting TECNO-SPUMA through the following email info@tecno-spuma.com

## 6. EXTERNAL INFORMATION CHANNELS

The reporting persons may, alternatively, send their communication directly, or after sending the communication through the TECNO-SPUMA Ethical Channel, to the public authorities through the external information systems enabled by the Independent Authority for the Protection of the Informant (AAI) or the corresponding authorities or autonomous bodies (in the case of Catalonia, before the Anti-Fraud Office of Catalonia), in accordance with the terms established in Title III of the Law on the Protection of Informants.

## 7. BREACH

This Policy is a mandatory rule for all members of the organization. Its violation will entail an infringement of the same and TECNO-SPUMA will adopt the disciplinary measures that are appropriate, in accordance with labor legislation and the Sanctioning Regime contained in the applicable Collective Agreement, without prejudice to other responsibilities in which the non-compliant person would have. could incur.

## 8. APPLICABLE REGULATIONS

- DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2019 on the protection of persons who report infringements of Union law (“ Whistleblower Directive ”).

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016 relating to the protection of natural persons with regard to the processing of personal data and the free circulation of these data and repealing the Directive 95/46/EC (“General Data Protection Regulation” - GDPR).

- Article 31 bis section 5 of the Spanish Penal Code.

- Law 2/2023, of February 20, regulating the protection of people who report regulatory infractions and the fight against corruption . (“Law for the Protection of Whistleblowers”).

- Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights. (“Data Protection Law” – LOPD-GDD).

- Circular 1/2016 of the State Attorney General's Office, of January 22, on the criminal liability of legal entities in accordance with the reform of the Penal Code carried out by Organic Law 1/2015.

- UNE-ISO 37002:2021 on Irregularity reporting management systems. Guidelines.

- Compliance management systems . Requirements with guidance for use.

## 9. ENTRY INTO FORCE, VALIDITY AND REVISION

The entry into force of this Policy will take place at the same time as the date of approval, modification or update of this document and will be in force as long as it is not repealed.

This Policy must be reviewed periodically in order to detect possible weaknesses or points for improvement, proceeding to update and/or improve what is established therein.

In an extraordinary manner, this Policy will be reviewed, and where appropriate, modified, when significant circumstances of a legal, organizational or any other nature arise that justify its immediate adaptation and/or update.