WHISTLEBLOWING CHANNEL POLICY

October 2023

INDEX

1. Introduction and purpose

The Whistleblowing Channel is constituted as the mechanism provided by the company that allows employees to confidentially report any irregularity of potential importance that is noticed in the internal operation of the company, as well as any third party with whom the company has a relationship regarding any action within the framework of such relationship.

In this regard, current legislation (and especially the current Criminal Code, after its reform of 2010 and 2015, and the Circular 1/2016, of January 22 of the State Attorney General's Office) reinforces the need for companies to have "criminal risk prevention models"; that is, with systems and control mechanisms that allow them to prevent, detect and react to the risk of committing a crime in a company -and for its benefit- by any of its members. And for the effectiveness of these prevention models, the so-called "Whistleblowing Channel" plays a fundamental role, a channel that, in line with the ethical and compliance culture existing in **EXTE** (or the "**Company**"), allows its employees to report possible risks and non-compliance.

In the same vein, Law 2/2023 of February 21, 2023, regulating the protection of persons who report regulatory infringements and the fight against corruption, has transposed Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, known as the Whistleblowing Directive, and aims to protect those persons who report allegations of corruption, fraud and rights violations.

EXTE's Whistleblowing Channel is governed by the **principles of confidentiality** of the data provided and the statements made, of **respect** and **substantiation**; so that any decision that the Company adopts from the receipt of a complaint through the Channel, will be taken in a reasoned, proportionate and considering the circumstances of the reported facts, with full respect for the rights and with due guarantees for the informant and for the affected persons, if any.

In particular, the Whistleblowing Channel **guarantees the confidentiality of the identity of whistleblowers and affected persons**, as well as the confidentiality of communications. Likewise, the **presumption of innocence** is guaranteed to all affected persons. Any person who reports through the Channel will enjoy due protection and any action against him/her that may be understood as a threat, discrimination or reprisal may be sanctioned.

All Company employees should be familiar with this tool, which is extremely valuable and useful for preserving and protecting their rights, the applicable law and the Company's image and reputation.

2. Scope of application

This Whistleblowing Channel Policy (the "**Policy**") applies to all individuals and legal entities involved in EXTE's business, including, without limitation, employees and third parties.

For the purposes of this Policy, "**third party**" shall mean any entity with which the Company conducts business. They can be suppliers, vendors, customers, distributors, business partners, advisors, consultants, contractors, subcontractors, marketing and sales agents.

Likewise, the definition of "**employee**" shall apply to directors, managers and, in general, to all Company personnel, regardless of the position they hold within the Company or the territorial area in which they carry out their activities.

In this regard, it should be noted that by EXTE we refer to the different companies that make up the Group, whose parent company is "Belmont Corporate Services S.L.", which has approved this Policy. Likewise, all the companies that make up the Group have adhered to it and implement it in their daily activities.

The Board of Directors has appointed Laura Abis as Head of the Whistleblowing Channel, who - in addition to having the status of manager - is the person in charge of the diligent processing of information and whistleblower complaints. The Head of the Whistleblowing Channel will perform these functions independently and autonomously from the rest of the Company's bodies, with all the personal and material resources necessary to carry them out.

Each Group company is responsible for the subsequent management of the acceptance of reports of irregularities, acts contrary to the law or the Group's internal rules affecting that company, under the terms set forth in this Policy and its implementing rules, in order to implement the necessary and applicable measures according to the jurisdiction in which the Group company operates.

2.1 Subjective scope

They will be able to report irregularities through the Whistleblowing Channel:

- Employees, former employees, apprentices -paid or unpaid-, volunteers, interns and candidates in a selection process.
- Executives, understood as those who provide management services for the Company and have powers of representation, organization or control, regardless of whether their contractual relationship with the Company is commercial or employment related.
- The Directors and/or members of its Board of Directors and the shareholders.
- Third parties.

In addition, all employees, managers, members of the Board of Directors or external collaborators of EXTE who have committed any irregularity or conduct that may constitute an infringement of European

Union law or that may constitute a serious or very serious criminal or administrative offence may be the **subject of a complaint.**

2.2 Objective Scope

The conducts that can be reported through the Whistleblowing Channel are all those conducts constituting a serious or very serious criminal or administrative offense, which are included in the global criminal framework.

With respect to the obligation to report actions or omissions that may constitute breaches of European Union law, and without prejudice to compliance with applicable EU regulations within the European Union, the Company must pay special attention to those areas in which it operates. The following areas are given as examples: (i) public procurement, (ii) financial services, products and markets, and prevention of money laundering and terrorist financing, (iii) consumer protection, and (iv) protection of privacy and personal data, and security of networks and information systems.

Likewise, any conduct that is contrary to the principles and standards of conduct established in EXTE's Code of Ethics and Conduct may also be reported through this Whistleblowing Channel.

3. Operation of the Whistleblowing Channel

3.1 Access and operation of the Whistleblowing Channel

The Whistleblowing Channel will be accessible through, may be accessible through any of these 3 channels, at EXTE's discretion:

- their website
- a **telephone number.** In such a case, the complaint will be recorded and retained as an audio recording, in accordance with applicable law.
- **specific Whistleblowing Channel e-mail addresses** that is available to employees. The Company expressly states that any complaint that is not made through the aforementioned means may be deemed not to have been received or admitted for processing, in which case it will be deleted and destroyed.

The Whistleblowing Channel is unique for all the companies of the Group, although it will have a system that allows assigning each report to the company to which the facts that are the object of the report refer, and the report will be sent to the person in charge of the Whistleblowing Channel or to whom the latter may designate in each subsidiary.

A whistleblower who wishes to remain anonymous may do so subject to the sufficient safeguards set forth in this Policy.

Any action aimed to prevent an employee from making a communication through the Whistleblowing Channel will be sanctioned in accordance with the applicable labour and disciplinary regime.

The internal process of the different companies for the registration, admission for processing, verification and resolution of the communications received in the Whistleblowing Channel shall be carried out in the shortest possible time, considering the characteristics of the facts reported and the other concurrent circumstances.

Complaints should only include those cases in which the facts have a real implication between the Company and the reported party; otherwise, they will not be taken into account and should not be attended to. The information obtained in this way may not be used for any purpose other than that provided for in this Policy.

3.2 Registration and classification of complaints

Communications are permitted in writing (by mail or e-mail), verbally (by telephone or voice messaging), or both. In any case, verbal communications must be documented, subject to the informant's consent (i) through a recording of the conversation, or (ii) by means of a complete and accurate transcript.

On the other hand, the submission and processing of anonymous communications is allowed, which means that the Whistleblowing Channel enables mechanisms that allow the submission of complaints without the informant having to reveal his or her identity.

Once the communication has been received, an acknowledgement of receipt must be sent within a maximum period of 7 days, unless the informant prefers not to receive it or it could entail a risk of confidentiality.

The information received should be ranked in order of importance from 1 to 5, with 1 being those considered most relevant and 5 being those considered least relevant. The following are considered to be among the most relevant:

- Situations that may give rise to possible criminal liabilities of the Company or its officers, including, but not limited to, those that may involve acts that, if confirmed, could be classified as corruption in the public sphere in any of its forms.
- Situations in which there is a risk of violating any legislation in force.
- Situations that, if known outside the Company, could cause damage to the Group's reputation.
- Situations involving a "business continuity" risk.

- High amount associated with the well-founded complaint.
- Number of people or areas affected by the reported facts.
- Facts that could constitute acts of corruption.

The evaluation indicated in this section will determine the priority at the time of starting the review and allocation of resources. Once the preliminary analysis of the communication has been carried out, its rating will be provisionally indicated.

In the event that, subsequently, new data or indications are obtained that make it advisable to change the initially assigned rating, the change of priority shall be justified and duly documented.

Complaints received through the Whistleblowing Channel and which are related to situations of discrimination, mobbing, sexual or gender-based harassment, shall be processed, where appropriate, in accordance with the specific procedures that may exist for these specific matters in the Company.

The Whistleblowing Channel is complemented by an external channel, managed by a public authority, called the Independent Whistleblower Protection Authority. Once the information has been submitted, it will be registered in the Whistleblowing Channel of Information Management.

3.3 Preliminary analysis of the reported facts

Once a communication has been received, the person in charge of the Complaints Channel shall determine whether or not to process it, considering whether it meets the minimum requirements. In the event that the communication is manifestly unfounded or, being anonymous, does not provide sufficient information to verify the facts denounced, it will not be admitted for processing, and such decision will be documented.

3.4 Verification of the reported facts

When, according to the preliminary analysis of the complaint, the person in charge of the Complaints Channel will proceed to verify and analyze the facts reported, for which the collaboration of other areas of the Company or third parties, if necessary, may be required.

Throughout the investigation process, the presumption of innocence is guaranteed to all persons concerned.

Access to the complaint and other documentation generated during the investigation process should be limited to those who perform internal control and compliance functions. Access by third parties shall only be lawful when it is necessary for the adoption of disciplinary measures or the processing of legal proceedings.

The data must be retained within the Whistleblowing Channel system for as long as necessary for the investigation of the facts. In any case, the data must be deleted three months after its entry into the Whistleblowing Channel unless its subsequent retention serves to provide evidence of the operation of the Whistleblowing Channel. This three-month period may be extended for a further three months if necessary.

In the event that the investigation reveals the need to adopt measures against the accused, this data may be shared with the corresponding areas exclusively to the extent necessary for the adoption of such measures.

3.5 Resolution of the complaint

Once the investigation of the reported facts has been concluded, the person in charge of the Whistleblowing Channel will reach conclusions that will be transferred to the competent areas and, in accordance with the provisions that develop this Policy, said conclusions will be formalized in a report.

In addition, adequate compliance with applicable data protection legislation and, in particular, with respect to the rights of the owners of such data must be ensured.

The response to the investigation proceedings may not take more than 3 months from its receipt, although it may be extended for another period of up to 3 more months in cases of greater complexity.

EXTE has a register in which all communications received are recorded, as well as the internal investigations that take place.

a) If the existence of an infraction is not considered to have been accredited: Case file closed.

If it is determined that no irregularity, act contrary to the law or internal rules has been accredited, it shall be agreed to close the file without the need to adopt any measure, archiving it and documenting said decision.

b) If the existence of an infringement is deemed to be established

If it is determined that an irregularity has been committed, an act contrary to the law or the Group's internal rules, it will be reported to the person responsible for the affected area and to the Human Resources area for the appropriate disciplinary effects. In those cases which, due to their relevance, are deemed necessary, at the request of any of the aforementioned areas, they may be transferred to:

- Judicial authority
- Public Prosecutor's Office
- Administrative authority

- Global Workers' Representative, if applicable.

After following the above milestones and deadlines, the decision adopted at this stage of the procedure will be communicated to the **whistleblower** within a maximum period of five (5) working days, unless a longer period is necessary for justified reasons.

Likewise, any person who has been the subject of a complaint admitted for processing will be informed about (i) the receipt of the complaint, (ii) the fact of which he/she is accused, (iii) the departments and third parties who, if applicable, may be recipients of the complaint and (iv) how to exercise his/her rights of access, rectification, cancellation and opposition, in accordance with data protection regulations.

However, the right of access of the **accused** will be limited to his/her own personal data subject to processing, for which reason, and given the confidential nature of the reports, the reported person will not be able to exercise this right to know the identity and personal data of the whistleblower.

In exceptional cases, if it is considered that there is a risk that the notification to the denounced person may compromise the investigation, such communication may be postponed until the aforementioned risk disappears. In any case, the period for informing the denounced person shall not exceed one (1) month from the receipt of the denunciation, with the possibility of extending said period to a maximum of three (3) months if there are justified reasons to do so. All of the above without prejudice that the law may expressly and bindingly establish different terms, in which case these shall be the ones to be observed.

4. Rights and guarantees of the whistleblower

The Whistleblowing Channel is governed by the principles of confidentiality, respect and substance.

Any person who reports in good faith shall enjoy due protection in accordance with the provisions of the applicable regulations. The following rights are acknowledged for the benefit of whistleblowers in particular:

1. Ability to decide whether or not to communicate anonymously;

2. Formulate the communication verbally or in writing;

3. Choose and indicate a safe place to receive communications and the acknowledgement of receipt in case they wish to receive it;

4. Opt-out of receiving any type of communications;

5. Appear before the Independent Whistleblower Protection Authority and request that the appearance be conducted by videoconference;

6. Exercise personal data protection rights;

7. Know the status and outcome of the complaint;

8. To enjoy due and necessary confidentiality, which may only be breached when it constitutes a necessary and deemed proportionate obligation imposed in the context of an external investigation conducted by the authorities in the framework of a proceeding.

9. Know their right to prohibit retaliation.

This last right of the whistleblower includes the prohibition of any acts constituting retaliation by the Company, including threats and attempts of retaliation. By way of example, the following are considered retaliation: (i) contract suspension or dismissal, (ii) economic damages or losses, (iii) negative performance evaluation or references, (iv) blacklisting, (v) denial or cancellation of leaves and/or permissions, and/or (vi) discrimination and unfavorable or unfair treatment within the framework of the employment relationship.

All persons who report violations shall be entitled to protection provided that they meet the following conditions: (i) the existence of reasonable grounds to presume that the information is truthful, even if they do not provide evidence; (ii) the adequacy of the communication as provided by this Policy. In any case, they are excluded from this protection:

- Information related to complaints about interpersonal conflicts. For the purposes of this policy, an interpersonal conflict shall mean any quarrel or dispute between two or more employees that does not constitute a violation for the purposes of this Policy.

- Information on irregularities that is already fully available to the public, or that does not contain new information with respect to previous ones.

- Information that is no more than hearsay, that lacks all credibility and that has been obtained through the commission of a crime.

The processing of personal data shall be governed by Regulation (EU) 2016/679, on Data Protection and by the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.

5. Data protection

In the management of the Complaints Channel, compliance with the provisions of Regulation (EU) 2016/679, on Data Protection (RGPD) and by the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (LOPDGDD) shall be complied with. Similarly, each of the subsidiaries belonging to EXTE shall be responsible for examining its national regulations on personal data protection and ensuring compliance with them through a further and internal development of this Policy. In particular, the following aspects shall be taken into account:

- All companies must implement the personal data security measures that are applicable according to the risk level established for the Whistle-Blowing Channel or, as the case may be, the measures that are mandatory by virtue of the applicable legal regulations and the internal regulations relating to this aspect of the Group. The level of security must be at least equivalent to that provided for in the data protection compliance system for sensitive or special category data, in accordance with the applicable data protection regulations.

- Adequate compliance with the processing of personal data must be guaranteed, and in particular with respect to the rights of the owners of such data to be informed about the processing of such data.

Personal data collected within the framework of the Complaints Channel:

- They shall be limited to those strictly and objectively necessary to process the complaints and, where appropriate, to verify the reality of the facts reported;
- They will be treated at all times in accordance with the data protection regulations applicable to each of the companies that make up EXTE, for legitimate and specific purposes in connection with the investigation that may arise as a result of the complaint;
- They shall not be used for purposes incompatible with those defined in this Policy;
- They shall be adequate and not excessive in relation to the aforementioned purposes.

EXTE has adopted technical and organizational measures necessary to preserve the security of the data collected in order to protect them from unauthorized disclosure or access. To this end, EXTE has taken appropriate measures to ensure the confidentiality of all data and will ensure that data relating to the identity of the informant are not disclosed to the respondent during the investigation, respecting in any case the fundamental rights of the person, without prejudice to any actions that, where appropriate, may be taken by the competent judicial authorities.

In addition, the privacy impact of the processing necessary to comply with the obligations set forth in this Policy and a risk assessment of such processing will be assessed in order to ensure the respectful operation of the Whistleblowing Channel.

Likewise, in order to comply with the transparency and information obligations established in the aforementioned personal data protection regulations, the whistleblower and the person or persons reported (the data subject), if applicable, will be informed that their data will be incorporated into a processing system under the responsibility of the corresponding subsidiary, identifying its VAT number and address, for the following purposes:

- Handle the reporting of any reportable facts, take appropriate corrective action and, if necessary, inform the whistleblower of the outcome of the procedure (such investigations may include an analysis of relevant e-mails, computer systems or documents and hard disks, verification of payments, submitted statements and receipts; interviews may also be conducted

with EXTE employees or third parties - natural or legal persons - and information may be obtained from third parties external to EXTE, as well as analysis of EXTE's video surveillance systems or on-site inspections of EXTE's premises);

- Protect EXTE employees, in particular, those who may have suffered any kind of damage or harm due to the conduct under investigation, but also those who may have received unfounded allegations.

- Prevent the commission of misconduct (put in place means to avoid breaches of legal, contractual or EXTE's internal regulations in the future).

- To exercise actions (judicial and extrajudicial) aimed at compensating and/or avoiding economic or other damages or losses for EXTE in order to defend, exercise and enforce its rights and interests and those of its employees and customers thereby effectively.

- Improve EXTE's compliance structures by identifying and removing potential weaknesses in its internal compliance organization.

European data protection regulations, as well as the Whistleblower Protection Act, presume lawful processing operations carried out in the context of the creation and maintenance of internal reporting information systems. The Whistleblower Protection Act states that such processing is deemed necessary for the performance of a legal obligation applicable to the data controller.

The legitimate basis for the rest of the above processing is the protection of EXTE's legitimate interests, namely, to prevent or minimize the extent to EXTE (including its employees, partners and customers) of potential economic and reputational damage resulting from reportable conduct or poor handling of reports made through the system.

Access to the data contained in the Whistleblowing Channel is limited exclusively to those who perform internal control and compliance functions in accordance with the provisions of this Policy, including those persons in charge of data processing who may be designated for this purpose. Only when disciplinary measures may be taken against an employee will such access be allowed to those persons within the Company who are in charge of imposing the necessary corrective measures.

Additionally, only when necessary for the adoption of corrective measures or for the processing of legal proceedings, the data will be transferred to:

- Other group companies. The legitimate basis for the processing shall be EXTE's legitimate interest in properly and efficiently carrying out the whistleblowing process. Such intra-group data transfer may be necessary in particular if the reported facts concern several group companies.

- Courts, authorities and other public bodies. When it is advisable to protect EXTE group companies, their employees, collaborators and customers and/or it is required by the applicable regulations. This may involve a transfer to Spanish or foreign authorities, courts or other public bodies. The legitimate basis for these transfers will be EXTE's legitimate interest in protecting the rights and freedoms of its employees, collaborators and customers and its own economic interests and, when disclosure is mandatory, compliance with the corresponding legal obligations.

- External service providers, in case EXTE resorts to the support of advisors, consultants, auditors, researchers, etc. The legitimate basis for this assignment is EXTE's legitimate interest in ensuring a proper defence and proper handling of legal claims, as well as obtaining appropriate advice on how to handle a given situation in order to avoid damage and harm to EXTE.

The interested party may exercise their rights of access, rectification, limitation of processing, deletion, portability and opposition to the processing of their personal data by sending their request to the postal address Paseo de las Castellana, 130 - 4th floor, Madrid 28046 (Spain) or to the e-mail address gdpr@sunmedia.tv.

They may also contact the supervisory authority, in this case the Spanish Data Protection Agency, to file a complaint, if they deem it appropriate.

6. Publicity

Without prejudice to the obligation of employees to know and act in accordance with the provisions of the Internal Regulations in the performance of their duties, the proper dissemination of this Policy and the existence of the Whistleblowing Channel shall be promoted and ensured.

Exte informs that this is a free translation into English of the original Spanish document approved by the Board of Directors. In case of contradiction or inconsistency between these two versions, the Spanish text will prevail.

7. Entry into force

This Policy shall be effective as of the date of its publication and its duration is presumed to be indefinite.