INTERNAL REPORTING CHANNET PROCEDURE

PROCEDURE FOR THE INTERNAL REPORTING SYSTEM OR WHISTLEBLOWER CHANNEL

1.- THE INTERNAL REPORTING SYSTEM OR WHISTLEBLOWER CHANNEL

1.1.- CONCEPT AND NATURE

The Criminal Code, in its Article 31 bis, establishes the obligation for legal entities to implement systems or means for reporting potential risks or legal violations.
Likewise, Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption, introduces a series of requirements that legal entities must meet for the establishment and management of such "internal reporting systems" or "whistleblower channels."
Accordingly, as part of its culture of ethical compliance, this Entity has implemented this INTERNAL REPORTING SYSTEM OR WHISTLEBLOWER CHANNEL, through which incidents relating to materialized risks, suspected criminal offenses, and any other conduct that violates legal regulations or the Company's Internal Policies may be reported.
It may be used by all employees, members of the management body, or any other interested third party included in Article 3 of the aforementioned Law 2/2023 of February 20, confidentially or anonymously and without fear of retaliation, as established by the aforementioned regulation.
By submitting a report and expressing concern, the whistleblower contributes to the recognition of our organization as a responsible entity in all aspects of its activity.

1.2.- BASIC GUIDING PRINCIPLES OF THE SYSTEM

Accessibility: There are two options for submitting reports:
· Through the link provided in the "whistleblower channel" section on the INTERMAS website
· By postal mail to Ronda de Collsabadell, 11, Industrial Park: 08450 Llinars del Vallès (Barcelona), or by hand delivery to the company offices

Confidentiality: The identity and contact details of the person submitting the report, as well as the facts and documents provided regarding the possible irregular conduct through this channel, will always be treated as confidential information and, therefore, will not be disclosed without the person's consent to the reported party and/or third parties, except when required by an administrative or judicial authority, in accordance with Article 31.1 of Law 2/2023.

Anonymity: Since anonymous reports are accepted, it is preferred that such reports be submitted via the telematic channel indicated above. Reports submitted by postal mail or hand delivery must be placed in a sealed envelope addressed to the INFORMATION SYSTEM MANAGER without any identifying details on the outside of the envelope. If the report is anonymous, no identifying data of the whistleblower should be included.
System Manager: The entity has delegated the management of reports to a designated system manager, duly identified and in accordance with Law 2/2023.

Objectivity and Impartiality: All reports will be handled objectively and impartially, guaranteeing the rights to privacy, defense, and the presumption of innocence of the individuals involved.

Data Protection: In accordance with Article 24 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (as amended by the Seventh Additional Provision of Law 2/2023), "The processing of personal data necessary to ensure the protection of individuals reporting regulatory infringements shall be lawful." Such processing shall comply with Regulation (EU) 2016/679 of the European Parliament and Council of April 27, 2016, with Organic Law 3/2018 of December 5, and with the aforementioned Law regulating the protection of whistleblowers. The legal basis for data processing is found in Article 30.3 of the LOPDGDD.

The data must be retained in the reporting system only for as long as necessary to decide whether to initiate an investigation into the reported facts. In any case, after three months from the entry of the data (or six months if the deadline is extended due to the complexity of the case), the data must be deleted from the system, unless the purpose of retention is to demonstrate the operation of the crime prevention model of the legal entity.
Under no circumstances will personal data be processed if not necessary for these purposes or if they refer to conduct outside the scope of the law. Such data must be deleted immediately. If the received information includes special categories of personal data, it will be immediately deleted and not recorded or processed.

If the facts are proven or sufficiently substantiated, the data will be retained for as long as necessary for the entity to exercise its rights before the courts.

Anonymous reports will be assigned an internal reference code so they can be incorporated into the reporting system.

Only the following parties may access the reports:
· The system manager
· The competent internal body duly designated within the Entity, if disciplinary measures against an employee may be considered
· The legal services manager of the Entity, if legal actions are to be taken regarding the reported facts
· External advisors or third parties required due to the nature of the case, who will be considered data processors or sub-processors
· The internal data protection officer or delegate and the Compliance Body

1.3.- RIGHTS AND OBLIGATIONS

Rights and Guarantees of Whistleblowers

Whistleblowers are guaranteed the effective exercise of the following rights, without prejudice to any other rights granted by the Constitution and applicable laws:

· To submit information anonymously and to have anonymity preserved throughout the procedure, provided they follow the established process described above.
· To make the communication verbally or in writing. For verbal reports, a system will be provided to enable this mode of communication.
· To indicate a mailing address, email, or secure location to receive communications from the System Manager, except in the case of anonymous reports.
· To appear before the System Manager or the appointed delegate on their own initiative.
· To refuse communication with the System Manager or the delegate handling the procedure and, if applicable, to revoke such refusal at any time.
· To have their identity protected. The identity of the whistleblower may not be disclosed without their express consent to anyone who is not authorized to receive and manage reports, except as required by European Union or Spanish law in the context of investigations conducted by authorities or during judicial proceedings.
· To have their personal data protected.
· To know the identity of the person handling the procedure.
· To confidentiality in all communications.
· To receive protective and support measures as provided for in Law 2/2023.
· To file a complaint with the Independent Whistleblower Protection Authority.
· To not suffer retaliation, even if the investigation concludes that there has been no violation of applicable regulations or the Entity's Code of Ethics, provided the report was not made in bad faith.

1.4.- OBLIGATIONS OF WHISTLEBLOWERS

Whistleblowers, in submitting their communications through the internal reporting channel, are subject to the following obligations:
· To have reasonable or sufficient grounds to believe in the truth of the information they report. Generic, bad-faith, or abusive reports are prohibited and may result in civil, criminal, or administrative liability.
· To describe in as much detail as possible the facts or conduct being reported, providing all available documentation or objective indications to support the investigation.
· To refrain from submitting reports for purposes other than those intended by the System or that violate the fundamental rights to honor, image, and personal and family privacy of third parties, or that are contrary to human dignity.

1.5.- RIGHTS OF THIRD PARTIES

Persons considered as third parties in the procedure will be recognized the rights granted by the Constitution and applicable laws, without prejudice to the possibility of extending to them, to the extent possible, the support and protection measures provided for whistleblowers in Law 2/2023; in particular, the following:
· To be informed, as soon as possible, of the information that affects them.
· To access proceedings against them, without prejudice to temporary limitations adopted to ensure the effectiveness of the investigation.
· To know the identity of the person handling the procedure.
· To honor and privacy, as well as the preservation of their identity. The identity of third

parties may not be disclosed without their express consent to anyone not authorized to receive and manage reports, except as required by European Union or Spanish law in the context of investigations conducted by authorities or during judicial proceedings.
· To the presumption of innocence and to use all lawful means for their defense.
· To indicate a mailing address, email, or secure location to receive communications from the System Manager.
· To appear before the System Manager or the appointed delegate on their own initiative.
· To have their personal data protected.
· To confidentiality in all communications.
· To not suffer retaliation.

2.- INCIDENT REPORTING PROCEDURE

2.1.- REPORTABLE INCIDENTS OR BREACHES

The following are considered reportable incidents or breaches:
· Any violation of current legislation
· Any breach of the ENTITY'S CODE OF ETHICS or INTERNAL POLICIES, or of the values, general principles of conduct, or behavioral standards of the staff, as set out therein
· Any event that may pose a risk to the reputation of our organization

2.2.- MINIMUM CONTENT OF REPORTS

To be accepted and properly processed, reports must necessarily include the following information:

· Whistleblower identified by full name (except in anonymous reports), along with a brief summary of the facts or arguments supporting the report.
· Person or department against whom the report is directed.

The burden of proof shall always lie with the whistleblower, who must submit the documents supporting the report. The reported party may submit any documents deemed appropriate in response.

If any of the persons affected by the report are involved in the investigation, they must be replaced by someone not directly connected to the matter.

3.- INVESTIGATION PHASE OF THE PROCEDURE

3.1.- RECEIPT AND ACKNOWLEDGMENT OF RECEIPT

Once the report has been received, the system manager shall acknowledge its receipt to the whistleblower within a maximum of 3 days, unless the report is anonymous, and will

begin the necessary verifications and checks; a case file will be generated and identified by a reference number.

If necessary, and if the report is not anonymous, the system manager may request clarifications or additional information.

3.2.- PRELIMINARY ANALYSIS OF THE INFORMATION RECEIVED

With the initial information, the system manager shall conduct a preliminary analysis to verify the substance, sufficiency, and credibility of the report, the credibility of the whistleblower, and the relevance of the reported facts; determining whether they may constitute a legal violation or a breach of the code of conduct.

Based on the outcome of this preliminary analysis, one of the following decisions may be adopted, with a written and justified record:

· Inadmissibility of the report and immediate closure of the case if the reported facts do not fall within the scope of this channel.
· Admissibility of the report and immediate closure of the case if its content is clearly irrelevant, the information is insufficient to proceed, the facts are implausible, or the whistleblower lacks all credibility.
· Admissibility of the report and initiation of the corresponding investigation procedure regarding the reported facts.

3.3.- PROCEDURE AFTER THE ANALYSIS

If the report is deemed inadmissible, the system manager shall inform the whistleblower (except in anonymous reports) of the inadmissibility or closure of the case, as applicable, and of any additional measures that may have been taken.

If the report is admitted, the investigation body shall be formed, whose functions include processing the report and drafting the report for its resolution.

Nevertheless, urgent measures may be adopted—always with justification—for the following purposes:

· Mitigating the effects of an actual or potential risk
· Executing urgent measures to preserve evidence
· Urgent communication, where appropriate, of the information to the governing bodies of the legal entity

If admitted, the procedure will follow these steps:

· Identify the applicable legislation, policies, procedures, or internal regulations affected, as well as reputational, economic, financial, or legal risks arising from the incident.
· Identify all relevant information and documents that may be useful for review (emails, websites, audiovisual surveillance and security footage, attendee lists, passwords or security devices, accounting records, etc.).
· Determine, with the assistance of the Human Resources Department, the necessity and urgency of implementing precautionary measures regarding the individuals under investigation.
· Depending on the severity, immediately suspend the individuals under investigation.

The investigation will include all procedures deemed necessary to clarify the facts, identify those responsible, and determine any corrective measures that should be taken.

Outlined below are some of the key procedures that may be part of any investigation:

· In the case of a non-anonymous report, conducting an interview with the whistleblower to gather more information regarding the report.
· Statements from the individuals under investigation.
· Confidential questionnaires and interviews with witnesses.
· Hearings with the individuals under investigation, their supervisors and colleagues, and any other persons deemed necessary.
· Gathering all relevant information from company documentation.
· If essential to clarify the facts, implementing surveillance measures using detectives or IT, telematic or audiovisual means, provided they meet criteria of reasonableness, suitability, and proportionality, and always respecting the employee's right to privacy and the secrecy of communications.
· Requesting external assistance from other professionals.
· Any other procedures that the Investigation Body deems necessary to clarify the facts.

3.4.- COMMUNICATION TO THE SUBJECTS UNDER INVESTIGATION

Except in the case of anonymous reports, the system manager will contact the involved parties, identifying themselves as the person in charge of investigating the report and briefly informing them of the allegations and the key milestones of the investigation.
If the report is deemed inadmissible, the whistleblower will be informed within a maximum of 3 days from its submission (except in anonymous cases).

3.5.- DOCUMENTATION OF THE INVESTIGATION PROCEDURE

The case file must include detailed documentation of the entire investigation procedure, such as all gathered documents and records of interviews held.
During all interviews conducted by the Investigation Body, written notes of relevant facts will be taken and incorporated into a record that must be signed by the interviewees and the members of the Investigation Body.

Furthermore, each interview will include an explanation of the provisions required by current data protection legislation.

3.6.- FINAL REPORT OF THE INVESTIGATION BODY

Once all investigative actions have been completed, the Investigation Body will prepare, within 15 days, a conclusions report that includes a brief description of the following elements:

· Identity of the members of the Investigation Body

· Nature of the contingency: whenever possible, identifying the involved individuals, the nature of the events, the date, location, and circumstances in which the events allegedly occurred, and the legal or internal regulations that were breached or at risk

· Summary of the facts and key findings: highlighting the most relevant facts gathered during the investigation, distinguishing between those obtained from company documentation, the whistleblower's information, or interviews with subjects and witnesses

· Conclusions and assessment of the facts: detailing the conclusions drawn by the Investigation Body, along with their assessment of the facts, and proposing one of two actions:

· Proposal to continue the procedure, if it is determined that the evidence sufficiently supports the commission of a sanctionable offense by the individual under investigation. This section will identify applicable sanctions, any other additional measures, and potential compensation actions for any affected parties

· Closure of the procedure, if it is determined that the facts do not constitute an offense, are not sufficiently substantiated, or if no known perpetrator is identified

Once completed, the final investigation report will be forwarded immediately to the Decision-Making Body and archived with the rest of the investigation case file.

4.- DECISION-MAKING PHASE

Based on the report prepared by the Investigation Body, if the report is deemed valid, a Decision-Making Body will be constituted. Its function is to form the legal entity's position in response to the report submitted.

To define this position, the Decision-Making Body may seek advice from as many external services as needed and request clarification from the Investigation Body.

Its composition is collegiate and includes the members of the Investigation Body plus one representative from the organization's Management Body.

In the event of a conflict of interest of any Decision-Making Body member in handling a specific matter, that member will be excluded from all proceedings related to the case.

The Decision-Making Body will forward the case file to the individuals under investigation, who will be given 5 days to submit a written response and provide any documents they consider relevant. Once this period has passed, the Decision-Making Body may adopt one of the following decisions:
· Request additional investigative actions
· Request that the management body impose sanctions and/or additional measures
· If potentially criminal behavior is identified, notify the competent administrative or judicial authority
· Take compensatory actions for any person or entity harmed by the reported events
· Make internal communication, training, or dissemination decisions regarding the events, to any company department or to the entire workforce, when considered an effective tool to prevent future incidents (always with the necessary data protection precautions)

5.- REGISTRY

For documentation purposes, the system manager must maintain an up-to-date, chronological, and confidential registry of the investigations (both ongoing and closed), reports, and disciplinary measures applied in relation to noncompliance.

This registry must include at minimum:
· Date of the incident
· Type of incident
· Date of report
· Type of whistleblower
· Persons involved in the situation
· Description of the incident
· Actions taken
· Resulting consequences

The registry mentioned above must always be kept up to date and available for review by those responsible for this policy (the system manager and the entity's Compliance Body), and always under strict confidentiality.
Nevertheless, the extent of disclosure or communication to other employees and management will be determined once the matter has been resolved, whether as a deterrent or to improve procedures and future actions to prevent misconduct.
Furthermore, the resolution of the procedure will become part of the file (employment record, if applicable) of the reported individual.