INTERNAL INFORMATION SYSTEM PROCEDURE OR UNAVETS WHISTLEBLOWER CHANNEL

1.- INTERNAL INFORMATION SYSTEM OR WHISTLEBLOWER CHANNEL.

1.1.- Concept and nature.

The penal code warns in article 31 bis of the obligation of the legal entity to establish within itself systems or means for communication about possible risks or legal breaches.

Likewise, Law 2/2023, of February 20, regulating the protection of persons reporting regulatory breaches and the fight against corruption, has also introduced a series of requirements that legal entities must comply with for the establishment and management of these "internal information systems" or "whistleblower channels".

Therefore, this Entity as part of its culture of ethical compliance, has implemented this INTERNAL INFORMATION SYSTEM OR WHISTLEBLOWER CHANNEL, through which events related to materialised risks, events which involve suspicions of a crime, and also any other conduct that constitutes a breach of legal regulations, as well as the Internal Policies of the Company or its Code of Ethics, can be reported.

It can be used by all employees, members of the administration body, or any other third party included in article 3 of the aforementioned Law 2/2023 of February 20, confidentially or anonymously without fear of retaliation in accordance with the provisions of said norm.
This channel is applicable to the Entity and, where appropriate, to any other company of its same Group in Spain.

By reporting and expressing their concerns, the whistleblower is contributing to our entity being recognised as a responsible organisation in all aspects of its activity.

1.2.- Basic guiding principles of the System

Accessibility: there are different options for reporting incidents, although the use of the telematic system enabled on the company's website in the "Internal Information System or Whistleblower Channel" section is recommended.
Confidentiality: the identity and contact details of the person making the communication, as well as the facts and documents communicated about the possible irregular action through this channel, will always be considered confidential information and, therefore, will not be disclosed without their consent to the accused party and/or third parties or unless required by administrative or judicial authority, in accordance with article 31.1 of Law

2/2023.

Anonymity: anonymous reports are accepted.
Responsible for the system: the entity has delegated the management of reports to a responsible person for the system, duly identified and in accordance with Law 2/2023.
Objectivity and impartiality: all reports will be managed objectively and impartially, guaranteeing the right to privacy, defence, and the presumption of innocence of the persons involved. It is not a channel for suggestions.
Data protection: In accordance with article 24 of LO 3/2018 of December 5 on the protection of personal data and guarantee of digital rights (amended by the Seventh Additional Provision of the aforementioned Law 2/2023), "The processing of personal data necessary to guarantee the protection of persons reporting regulatory breaches will be lawful.
Said processing will be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, by Organic Law 3/2018 of 5 December on the Protection of Personal Data and Digital Rights Guarantees and by the Law regulating the protection of persons reporting regulatory breaches and fighting against corruption."
The data must be kept in the reporting system only for the time necessary to decide whether or not to initiate an investigation into the reported facts. In any case, three months after the data is entered (or six if the deadline has been extended due to the complexity of the report), it must be deleted from the system, unless the purpose of the retention is to provide evidence of the operation of the legal entity's crime prevention model.
If the facts are proven or there are sufficient indications, the data will be kept for as long as necessary for the entity to exercise its rights before the courts of justice.

Anonymous reports will be identified by an internal reference to be incorporated into the reporting system.

Only the following may access the reports in the first instance:
• The data controller of the system and whoever manages it directly.
• The competent internal body duly designated in the Entity, when disciplinary measures may be taken against an employee.
• The legal services manager of the Entity, if legal measures are taken regarding the reported facts.
• The processors or sub-processors who may be appointed.
• The Data Protection Officer and the Compliance Officer.

1.3.- Rights and Obligations
Rights and Guarantees of informants
Persons providing information will be guaranteed the exercise of the

following rights, without prejudice to any others recognised by the Constitution and laws:
• submit information anonymously and maintain anonymity during the procedure.
• make the communication verbally or in writing. In the case of verbal communication, the informant will be offered the opportunity to verify, rectify, and accept, by signing, the transcription of the message.
• indicate an address, email, or secure location to receive communications from the data controller of the System.
• appear before the data controller of the System or the delegated manager on their own initiative.
• renounce communication with the data controller of the system or the delegated manager who initiates the procedure, and, if applicable, withdraw such renunciation at any time.
• preservation of their identity. The identity of the informant may not be revealed without their express consent to anyone not competent to receive and manage reports, with the exceptions provided for by EU law or Spanish regulations in the context of investigations carried out by authorities or in the course of judicial proceedings.
• protection of their personal data.
• know the identity of the delegated manager instructing the procedure.
• confidentiality of communications.
• protection and support measures as provided for in Law 2/2023.
• file a complaint with the Independent Authority for the Protection of Whistleblowers.
• not be subject to retaliation, even if the result of the investigations verifies that there has been no breach of applicable regulations or the Entity's Code of Ethics, provided there has been no bad faith.

1.4.- Obligations of the Informants

Informants, regarding the submission of their communications through the internal information channel, shall be subject to the following obligations:
• Have reasonable or sufficient indications about the certainty of the information they communicate, and may not make generic or bad faith communications, or abuse their rights, in which case they may incur civil, criminal, or administrative liability.
• Describe as detailed as possible the facts or behaviours they communicate, providing all available documentation on the described situation or objective evidence to obtain the proofs.
• Abstain from making communications for a purpose other than that intended by the System or that violate the fundamental rights to honour, 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 granted the rights recognised by the Constitution and laws, without prejudice to the possibility of extending to them as far as possible, the support and protection measures for whistleblowers provided for in Law 2/2023; specifically the following:

• be informed, as soon as possible, of the information that concerns them.
• access to the actions taken against them, without prejudice to the temporary limitations which may be adopted to ensure the outcome of the actions.
• know the identity of the manager instructing the procedure.
• to honour and privacy, as well as the preservation of their personal data.
• confidentiality of communications.

2.- PROCEDURE FOR RECEIVING AND PROCESSING REPORTS

2.1.- Reception

Communication may be made in writing or verbally, anonymously, or confidentially, in accordance with the provisions of this Procedure, through the following channels:

• Online: through the established system enabled on the company's website in the "Internal Information System or Whistleblower Channel" section.
• By post to the registered office of the company.
• Verbally: if the informant prefers to do so in person, in which case they will be offered the opportunity to verify, rectify, and accept, by signing, the transcription of the message.
• Through the Data Protection Officer and the Compliance Officer.

2.2.- Processing

Reception will be conducted by the data controller or persons of the System. They will carry out the following actions:

• Register the communication, indicating the date of receipt and the channel through which it has been received.
• Send the informant an acknowledgment of receipt of the communication.
• Classify the communication according to its subject matter.
• Carry out a first assessment to verify whether the communication meets the requirements of this procedure and the applicable law. In case of doubt, the compliance officer or the data controller of the system will make the necessary enquiries to clarify it.

2.3.- Verification of the facts

If the data controller of the system considers it appropriate, they will carry out a first verification of the facts reported, informing the Compliance Officer of their decision.

The verification of the reported facts may be carried out, inter alia, through

the following actions:
• Consultation of documentation and files of the Entity or the Group company involved.
• Via additional information from the informant or from third parties involved, without prejudice to their rights.
• Designation of an internal or external expert.
• Collaboration with the legal department or external legal advisors.
• Interposition of complaints or claims with public authorities.
• Any other action necessary to verify the facts.

2.4.- Analysis and Decision

Once the verification has been completed, the data controller of the system, assisted by the Compliance Officer, if necessary, will make a decision on whether or not to initiate an investigation procedure.
If it is decided to initiate an investigation, the entity will take the necessary measures to guarantee the effectiveness and objectivity of the procedure, respecting at all times the rights of the persons involved, as well as the principles of confidentiality, objectivity, and impartiality.
If the decision is not to initiate an investigation, the reasons for the decision will be communicated to the informant, unless prohibited by law.

2.5.- Resolution

Once the investigation is concluded, a reasoned resolution will be issued, containing the following elements:
• Description of the facts investigated.
• Legal and regulatory provisions applicable to the reported facts.
• Evaluation of the evidence obtained.
• Conclusion reached.
• Proposed measures, where appropriate, to remedy or mitigate the consequences of the reported facts, as well as to prevent their recurrence.
• Identification of the persons involved, if the resolution is not anonymous.

2.6.- Follow-up and Closure

The Compliance Officer will ensure compliance with the resolutions issued, monitoring their implementation, and ensuring that the necessary corrective measures are taken.
Once the actions envisaged in the resolution have been completed, the file will be closed, communicating it to the informant if applicable.

3.- FILING AND DOCUMENTATION

3.1.- File

A file will be opened for each communication received, which will include all the actions carried out in relation to it, the resolutions issued, and the supporting documentation.

The file will be archived for a period of five years from the date of closure of the file, unless it contains data or documentation that may be relevant in the event of judicial, administrative, or disciplinary proceedings, in which case it will be kept until the end of the procedure.

3.2.- Documentation

The communications received through the internal information system or whistleblower channel, as well as the actions carried out and the resolutions issued, will be documented in accordance with the requirements established by the applicable law on the protection of personal data and, where appropriate, with the provisions of the Entity's own Data Protection Policy.

4.- SUPERVISION AND CONTROL

The Compliance Officer and the Data Protection Officer will ensure compliance with this Procedure and the applicable legal and regulatory provisions.

They will periodically monitor the operation of the system, ensuring that the necessary corrective measures are taken to correct any deviations detected.

The reports of the internal control and audit functions, as well as the resolutions issued in the scope of this system, will be communicated to the Audit and Control Committee or to the body of the administration body responsible for overseeing the functioning of the internal control and risk management system.

5.- TRAINING AND DISSEMINATION

Training activities will be carried out to inform employees and other persons involved in the procedure about the existence and operation of the internal information system or whistleblower channel.

The content of the training will include the rights and obligations of whistleblowers, the procedures for receiving and processing reports, and the measures for protection and support provided for in Law 2/2023.

6.- ENTRY INTO FORCE AND MODIFICATION

This Procedure will enter into force on the day following its approval by the competent body and will be mandatory for all employees, members of the administration body, and other persons involved in the activities of the Entity.

Any modification or updating of this Procedure will be communicated to all employees and persons involved, who will receive training on its content.

The internal information system or whistleblower channel may also be adapted to technological or regulatory developments in order to improve its operation and effectiveness in the detection and prevention of risks.

This procedure was approved by the Board of Directors on April 15, 2024.