GENERAL POLICY OF THE INTERNAL SYSTEM OF INFORMATION AND DEFENSE OF THE INFORMANT

INDEX

1 - INTRODUCTION

The transposition of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 into Spanish law with Law 2/2023 of 20 February regulating the protection of persons who report violations
regulations and the fight against corruption, involves the incorporation of specific instruments so that those who are aware of illegal or irregular actions can provide useful data and information, ensuring full and effective protection of said informants.

In this regard, the aforementioned regulations govern the minimum requirements that must be met by the various internal and external information channels, along with the special protection regime for informants who act in good faith and with an honest conscience, and who are disinterested.

In accordance with the above, THE GROUP has implemented an Internal System of Information (SIIF), which is configured as a fundamental axis for supervision, Control and prevention in the area of regulatory compliance.
This system constitutes a preferred channel and a mandatory tool for channeling information diligently, in order to strengthen the information culture within the organization itself.

The SIIF has been designed as a control and prevention instrument, which contemplates
Information channels managed both internally and by a specialized external company. These channels enjoy the highest levels of professionalism, experience, independence, confidentiality, and compliance with data protection regulations and other applicable regulatory frameworks. Furthermore, the SIIF guarantees the basic principles of anonymity, proper recording, retention and non-alteration, prevention of conflicts of interest, protection of whistleblowers, and prohibition of retaliation.

In accordance with the aforementioned Law, it is an essential requirement that the SIIF has a
Policy that states the general principles of the system and the defense of the informant, duly publicized within the Group. Therefore, together with the Procedure for managing the information received, this Policy is a
essential element of the configuration and operation of the SIIF.

2 - PRINCIPLES OF ACTION AND ESSENTIAL GUARANTEES

The Internal Information System (SIIF) is one of the main axes of the systems Regulatory compliance and crime prevention. In compliance with the highest standards of due diligence in this area, the Group has provided the SIIF with a series of safeguards to ensure its effectiveness, with the collaboration and support of the external expert BONET Consulting. Specifically, the basic principles and fundamental safeguards governing the Group's process and actions in relation to the SIIF are as follows:

- Independence, autonomy, impartiality, and absence of conflicts of interest: In receiving and processing information about violations, response mechanisms have been defined to manage and control potential conflicts of interest and/or lack of independence when those responsible for management, control, and/or supervision present certain characteristics that compromise and restrict the performance of their duties. Furthermore, all communications received are analyzed in accordance with the necessary independence requirements, which guarantee fairness and equity in their handling.

- Professionalism and experience: Experts in regulatory compliance, crime prevention, and good governance are responsible for the proper handling and management of communications, safeguarding the rights of both informants and those accused.

- Completeness, integrity, and confidentiality of information: Participants in the various phases of the investigation are bound by a duty of confidentiality regarding any information they may have access to or become aware of in the course of their duties. Furthermore, unauthorized access to information is prevented, and long-term and secure storage is permitted through the creation of backup copies of information and independent files.

- Data protection and confidentiality of communications: Data processing is in accordance with and complies with the highest standards and policies for the protection of personal data, in accordance with applicable regulations on personal data protection. Likewise, there is a duty to maintain confidentiality regarding any aspect related to the information communicated.

- Anonymity and Anonymization: The possibility of submitting and subsequently processing anonymous communications is provided for, as well as the general obligation to preserve the identity of the informant who has identified himself when making the communication, keeping him anonymous and not revealing his identity to third parties.

- **Affordable use, simplicity and free of charge:**Simplicity in communication is guaranteed, allowing universal access to the system at no associated cost, and the effective application of the legality and ethical principles that govern the Group's activities.

- Adequate and independent record keeping: A private record book is kept of the information received and the internal investigations it has given rise to,

as a guarantee of its processing, management, and non-alteration, independently and without conflicts of interest, for a necessary and proportionate period of time in accordance with current legislation. Under no circumstances will the data be retained for longer than ten years.

- **Good practices for monitoring and investigation** In order to verify the veracity of communications, ensure that evidence is properly collected, and guarantee the rights of those affected, the communication lifecycle will be regulated through an effective and transparent internal procedure. These practices will be documented in the Procedure for Managing Information Received.

- Protection of whistleblowers and affected individuals: Individuals who report or disclose violations are entitled to protective measures and will not be subject to any retaliation or adverse consequences for their cooperation, including threats of retaliation and attempted retaliation. Similarly, those affected by the report are entitled to the same protections provided for whistleblowers, with their identities protected and the confidentiality of the facts and information surrounding the proceedings guaranteed.

- Diligent action, responsibility, and good faith of the informant: Use of the system is based on the principles of responsibility, diligence, and good faith, so every informant must have reasonable grounds to believe that the information is true at the time of reporting. Reporting unfounded, false, or distorted facts, as well as submitting information obtained illegally, maliciously, or morally dishonestly, constitutes a violation of the principle of good faith and may result in disciplinary measures.

3 - RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM

For the effectiveness of the Internal Information System (SIIF), it is essential to designate a person responsible for its proper functioning, organization, and diligent processing of information. This person will also be responsible for ensuring proper communication and dissemination of the SIIF, as well as for developing and updating the relevant training plan.

The administrative body or governing body of the Group is competent for the designation and communication to the competent authority of the natural person or body member responsible for the management of said system and for his dismissal or termination (hereinafter, the System Manager).

The System Manager carries out his/her functions independently and autonomous from the rest of the Group's organizational bodies, avoiding possible situations of conflict of interest with the ordinary performance of its duties.

However, the System Manager may rely on other third parties for specialized support and/or to meet independence requirements to ensure the proper performance of his or her duties.

In particular, for the exercise of his functions the System Manager will coordinate with the following subjects:

A- The human resources manager, when disciplinary measures may be appropriate against the individuals involved and/or coordinate the implementation of protective measures.

B- Those responsible for regulatory compliance and/or the Group's legal services, if appropriate, should adopt legal or regulatory compliance measures that must be taken into consideration by them in relation to communications received in the SIIF.

C- The data controllers who may be appointed.

D- The Data Protection Officer/Delegate.

E- Other persons and/or entities involved in the management of the SIIF.

4 - INDEPENDENT INFORMANT PROTECTION AUTHORITY

The Group's Internal Information System (SIIF) is the priority and mandatory means for reporting known illicit conduct or violations, as it ensures the proper adoption of protective measures and fosters an information culture within the organization.

However, other "external" information channels have been determined, in order to Offer citizens an alternative means of submitting communications and/or complaints in cases where internal channels do not comply with the guarantees required by applicable regulations, the relevant protection measures are not applied, or individuals are exposed to retaliation for their status as informants.

Therefore, any natural person may directly inform the Authority. Independent Whistleblower Protection Commission, AAI of any commission actions or omissions constituting a violation of the legal system, through the external information channel of said specialized public authority. Access to this external information channel and the Authority's contact information are published on its website.

5 CONFIDENTIALITY AND PROTECTION OF PERSONAL DATA

The processing of personal data derived from the Internal Information System (SIIF) are governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018 of 5 December, and Organic Law 7/2021 of 26 May. Therefore, at the time of recruitment, interested parties are informed of the processing of their data and their rights, in accordance with current regulations.

In compliance with the principle of data minimization, personal data collected are those necessary and relevant for the processing of the communication. In the event that data is collected accidentally and is not necessary for understanding and investigating the actions or omissions, it will be deleted without undue delay. Furthermore, the data will be retained for the time necessary to decide whether to initiate an investigation.

Furthermore, the design of the SIIF guarantees the confidentiality of the identity of the informant and any third party mentioned in the communication, as well as the actions carried out in the management and processing of the communication. In this sense, the access to personal data and other information contained in the system is Limited to those responsible for management, within the scope of their powers and duties. Therefore, appropriate technical and organizational measures are in place to protect the identity of those affected and prevent access by unauthorized persons.

In the event of any doubt or query regarding the processing of personal data carried out within the Group's entities in relation to the SIIF, any interested party may contact the Data Protection Officer/Delegate. designated, through the contact details that have been previously communicated to you and that are at your disposal.

6 PROTECTION MEASURES

Persons who report or disclose violations using the Internal System
Information (SIIF) of the Group are entitled to protection, under the same conditions
that those who report through external channels, provided they have reasonable grounds to believe that the information referred to is true at the time of communication or disclosure, even if they do not provide conclusive evidence.

In this regard, acts constituting retaliation, including threats and attempts, against persons who submit a communication are expressly prohibited. Retaliation is defined as:

a- Acts or omissions prohibited by law.

b- Acts or omissions that directly or indirectly result in unfavorable treatment, placing a person at a disadvantage compared to another.

By way of example and not limitation, the following are considered reprisals:

- Suspension of the employment contract, dismissal or termination of the relationship, early termination, annulment of the employment and/or commercial contract, disciplinary measures, reprimand or other sanction, demotion or denial of promotion, substantial modification of conditions, and failure to convert a temporary contract into a permanent one, or equivalent measures.

- Damages (including reputational), economic losses, coercion,
bullying, harassment or ostracism.

- Negative evaluations or references regarding job or professional performance.

- Blacklists or dissemination of information that hinders or prevents access to employment/contracts for works or services.

- Denial or cancellation of license or permit.

- Denial of training.

- Discrimination, unfavorable or unfair treatment.

- Denial of incentives, benefits, bonuses, commissions, and any other type of compensation.

- Early termination, suspension, alteration or cancellation of contracts for goods or services.

These acts shall be null and void and, where appropriate, shall give rise to disciplinary or liability measures, which may include compensation for damages to the injured party.

In order to guarantee the right to protection of the informant and the persons affected by the communication, the Group has established the following technical and organizational measures, which are applied from the initial moment the communication is received:

1- Configuration of the SIIF: The SIIF has been designed with appropriate technical and organizational measures to ensure the protection of the reporting entity's identity, as well as any data and information derived from the communications submitted. In this regard, the Group has enabled several internal reporting channels, which allow communications to be submitted anonymously. These channels are:

- Online/digital channel: Digital platform for the submission of written communications.

- Face-to-face channel: The system for receiving communications through face-to-face meetings or videoconferences.

Regardless of the channel used, the SIIF guarantees effective application of the basic principles and guarantees specified in this Policy, in order to comply with the requirements of the regulatory framework and protect the rights of informants and affected persons.

2- SIIF Manager: To ensure the proper application of the SIIF, the Group has designated a Manager whose role is to supervise, monitor, and control its operation. In this regard, the Manager, together with the external expert, will adopt the necessary protective measures and ensure their proper monitoring and implementation. The participation of the external expert provides the Manager's functions with the elements of autonomy and independence required by current regulations.

   Likewise, the Controller will be responsible for conducting a preliminary analysis of the communications received to determine the suitability of adopting specific protective measures for the informant and/or affected third parties. Furthermore, depending on the nature and scope of the information, the Controller will have the support and advice of the heads of the Group's various operational areas to successfully complete the investigation. It may also call on other third parties specialized in matters requiring expert opinion.

3- Custody, management, and security of SIIF information: The Group has a document management system configured with appropriate security and control measures to demonstrate the effectiveness of the SIIF. It should be noted that this system includes anonymization processes to prevent the identification of informants. Additionally, the Group has adopted reasonable technical measures for the secure storage, retrieval, and disposal of information, as well as the implementation of access controls to prevent unauthorized use.

However, information submitted that is false, distorted, manifestly lacks credibility or foundation, or that has reasonable grounds for having been obtained through the commission of a crime, is excluded from this protection. This is because all communications must be made in good faith, and therefore, the informant must have reasonable grounds to believe the information is true at the time of communication. In

short, the principle of good faith requires that in no case can it be inferred that there is falsehood, misrepresentation, or an intent to revenge or harm a third party.

It is important to remember that protective measures are not only directed towards the Informants. Those to whom the facts described in the communication refer (affected persons) also enjoy unique protection against the risk that the information, even with apparent veracity, may have been manipulated, be false, or respond to other motivations. During the processing of the case, these persons have the right to the presumption of innocence, judicial protection and defense, access to the case file, as well as the confidentiality of the facts and data of the procedure and the confidentiality of their identity. In short, they have the same protection and rights as the informant.

7 - DISCIPLINARY REGIME

Failure to comply with applicable regulations and conduct contrary to the Group's instructions, policies, codes, procedures, and protocols will result in the application of disciplinary measures at the labor and commercial levels, in coordination with the provisions of the applicable Collective Agreement, the Workers' Statute, and other applicable regulations.

The Group will notify and sanction any actions or omissions contrary to this Policy incurred by employees, collaborators or any member related to the Group and, in particular:

- Failure to report any suspicion or knowledge of violations or breaches of the Group's regulatory framework and internal protocols and standards through the SIIF.

- Any attempt or effective action to hinder the submission of communications or prevent, frustrate or slow down their follow-up.

- The use of the SIIF in bad faith, for example, by providing information or documentation that is known to be false.

- Any retaliation against informants or other affected persons arising from the communication.

- The violation of confidentiality and anonymity guarantees, revealing the identity of the affected individuals and breaching the duty of confidentiality of information.

- Failure to comply with the obligation to cooperate with the investigation of information.

8 - COMMUNICATION, REVIEW AND UPDATE

This Policy, as well as all necessary information regarding the use of the Internal Information System (SIIF) implemented, is available in a separate and readily identifiable section, so that all interested parties have it clearly and easily accessible. However, anyone may request additional information from the Group through the Controller's contact information.

The System Manager will periodically review and, where appropriate, propose updates to the Group's administrative or governing body to adapt this Policy to any circumstances and changes that may arise, as well as to any regulations or case law that may be issued. All of this is intended to align the SIIF with the highest regulatory compliance requirements for its proper functioning and effectiveness.

Likewise, the Group is open to any suggestions and/or proposals that may improve its ethical conduct and foster a culture of regulatory compliance, emphasizing the need for all employees and members of the Group or third parties to collaborate in compliance with its values and principles.

9 - INTERNAL INFORMATION CHANNELS

In order to comply with the provisions of Law 2/2023, the Group has implemented a system configured with the technical and procedural requirements established by said Law for the proper handling of communications. The aim is to offer informants a secure, confidential, or even anonymous communication environment with the Group, and to process information efficiently, professionally, and independently.

To this end, the Group has provided itself with material, technical, and human resources to enable various internal channels that allow for the submission of communications in written or verbal format. These channels are configured, designed, and supported by an external expert to provide the highest levels of professionalism, experience, independence, confidentiality, data and whistleblower protection, and other areas applicable to these types of channels.

It should be noted that any information provided through any of our internal channels will be treated confidentially and will only be accessible to authorized personnel for its proper management and processing.

The channels available to any employee or third party associated with the Group for submitting communications are detailed below:

https://www.corporate-line.com/cnormativo-salvat

Canal On-line/Digital CORPORATE LINE Canal de comunicaciones

The Group has a digital tool that allows written communications to be submitted using a form, which allows for file attachments. Once the form is completed, the tool automatically generates a code that allows for proper tracking and management by the person responsible for processing.

A confirmation is also sent to the informant regarding the entry and registration of the communication in the system. This confirmation contains a summary of the information provided, as well as the code so that the informant can also track the information.
This tool has security measures that guarantee the protection of the information, the identity of the informant and those affected, as well as the confidentiality and confidentiality of the entire communication management and processing process. In this regard, the Group guarantees a secure and efficient communication environment for receiving communications.

The tool also allows for anonymous submission of communications.
Thanks to the communication and monitoring system available, the informant and the System Manager can communicate through the tool, regardless of whether the communication was submitted anonymously.

The link to access this tool and its scope of use are available on the Group's website.

Canal Presencial / "Face to face"

- Telephone: 911087727 / 930460116

  The informant service hours are as follows:

  - Monday to Thursday from 8:30 a.m. to 2:00 p.m. and from 3:00 p.m. to 6:00 p.m.
  - Friday from 8:30 a.m. to 2:30 p.m.

- E-mail: salvatlogistica@sistema-interno-informacion.com

Another channel the Group makes available to its employees and third parties with whom it interacts is the face-to-face channel, which allows for the submission of verbal communications through an in-person meeting or videoconference. In this case, and considering the complexity involved for the Group in ensuring the anonymity of the informant in those cases where it is requested, the Group has entrusted this function to the external expert BONET Consulting, which is responsible for receiving and managing communications of this nature, as well as any others in which the informants are identified and face-to-face management is required.
In this regard, the external expert guarantees the protection of the informant's identity both during the appointment request process, when submitting a communication in person, and at the location where the appointment is held.

In order to guarantee the security and preserve the integrity of the information provided by the informant, the meeting will be recorded in accordance with the law and with the informant's prior consent. This meeting will be documented in a secure format, with the security and anonymization measures required by the regulatory framework. To this end, BONET Consulting has and will enable the necessary technological mechanisms to send supplementary documentation to the information provided at the meeting.

To enable this channel to be used, the Group has set up a telephone number and email address for requests to submit communications in this format. BONET Consulting will be responsible for handling and coordinating the meeting exclusively. Contact information for this request is duly published on the Group's website.