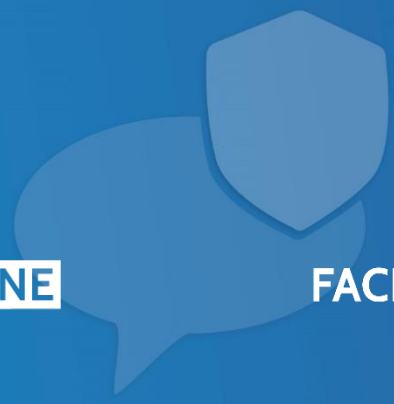
GENERAL POLICY OF THE INTERNAL INFORMATION SYSTEM



CORPORATE LINE
Canal de comunicaciones

FACE to FACE LINE
Canal presencial

CASTELL D'OR

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 regulatory infringements and the fight against corruption**, implies the incorporation of specific instruments so that those who know of illegal or irregular actions can provide useful data and information, ensuring full effective protection of such informants.

In this sense, the aforementioned legislation regulates the minimum aspects that the different internal and external information channels must satisfy, together with the special protection regime informants who act in good faith and with an honest conscience, in a disinterested manner.

In accordance with the foregoing, **THE COMPANY** has implemented an **Internal Information System (SIIF)**, which is configured as a fundamental axis for supervision, control, and prevention in the area of regulatory compliance. Such system constitutes a preferential channel and a mandatory tool to diligently channel information 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 are characterized by the highest levels of professionalism, experience, independence, confidentiality, compliance with data protection regulations and other applicable regulatory frameworks. Likewise, SIIF guarantees the basic principles of anonymity, proper recording, preservation and non-alteration, prevention of conflicts of interest, protection of the informant and prohibition of retaliation.

In accordance with the mentioned Law, it is an indispensable requirement that the SIIF has a **Policy that sets forth the general principles of the system and the defense of the informant**, duly publicized within the Entity. Therefore, along with the Procedure for the management of information received, this Policy is an 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 regulatory compliance and crime prevention systems. In accordance with the highest diligence requirements in this field, the Entity has provided the SIIF with a series of guarantees to ensure its effectiveness, with the collaboration and support of the external expert **BONET consulting.** Specifically, the basic principles and fundamental guarantees that govern the process and the Entity's actions in relation to the SIIF are as follows:

- **Independence, autonomy, impartiality, and absence of conflicts of interest**: In the reception and treatment of information on violations, reaction mechanisms have been defined to manage and control possible conflicts of interest and/or lack of independence, when those responsible for management, control and/or supervision present a series of characteristics that compromise and condition the performance of their duties. Likewise, all communications received are subject to analysis with the necessary requirements of independence, which guarantee fairness and justice in their treatment.

- **Professionalism and experience**: Professional experts in regulatory compliance, crime prevention and good governance are in charge of the processing and proper management of communications, preserving the rights of whistleblowers and defendants.

- **Completeness, integrity, and confidentiality of information**: Participants in the different stages of investigation have a duty of confidentiality regarding any information they may access or become aware of due to the exercise of their functions. In addition, access to it by unauthorized personnel is prevented and a durable and secure storage of the same is allowed, through the generation of backup copies of the information and independent files.

- **Data protection and secrecy of communications:** The processing of data conforms to and complies with the highest measures and policies for the protection of personal data, according to the applicable regulations on the Protection of Personal Data. Likewise, there is a duty of secrecy regarding any aspect related to the information communicated.

- **Anonymity and Anonymization**: The possibility of submitting and subsequently processing anonymous communications is contemplated, as well as the general duty to preserve the identity of the informant who has identified themselves when making the communication, keeping them anonymous and not disclosing their identity to third parties.

- **Accessible use, simplicity, and free of charge:** The simplicity of making the communication is ensured, allowing universal access to the system without any associated cost, and the effective application of the legality and ethical principles that govern the Entity's activity.

- **Adequate and independent record**: A private book-record of the information received and the internal investigations to which they have given rise is drawn up, as a guarantee of their treatment, management, and non-alteration, independently and without conflicts of interest, for a period of time that is necessary and proportionate in accordance with current legislation. In no case will the data be kept for a period of more than ten years.

- **Proper monitoring and investigative practices**: In order to verify the veracity of communications, the correct collection of evidence and to guarantee the rights of the affected parties, the life cycle of the communication shall be regulated in an effective and transparent internal procedure. These practices will be documented in the procedure for the management of information received.

- **Protection of the whistleblower and affected persons:** Persons who report or disclose infractions are entitled to protection measures and shall not be subject to any retaliation or adverse consequence for their collaboration, including threats of retaliation and attempts of retaliation. Similarly, the persons affected by the communication shall be entitled to the same protection established for whistleblowers, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

- **Diligence, responsibility, and good faith of the whistleblower:** The use of the system is based on the principles of responsibility, diligence, and good faith, so that every informant must have reasonable grounds to believe that the information is truthful at the time of its communication. The communication of unfounded, false, or misrepresented facts, as well as the remission of information obtained in an unlawful manner, with a malicious and morally dishonest attitude, is a breach of the principle of good faith and may result in the application of disciplinary measures.

3 RESPONSIBLE OF THE INTERNAL INFORMATION SYSTEM

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

The governing body of the Entity is competent for the designation and communication to the competent authority, natural person or collegiate body responsible for the management of that system and its dismissal or dismissal (hereinafter referred to as the **Responsible**).

The Responsible performs his/her **functions independently and autonomously** from the rest of the Entity's organizational bodies, avoiding possible situations of conflict of interest with the ordinary performance of his/her duties. However, the Responsible may resort to other third parties for specialized support and/or to comply with independence requirements, ensuring the proper performance of his/her duties.

In particular, for the exercise of its functions, the Responsible shall coordinate with the following subjects:

- **A** The human resources manager, when disciplinary measures may be taken against the persons involved and/or to coordinate the application of protective measures.
- **B** The compliance officers and/or legal services personnel of the Entity, if legal or regulatory compliance measures that need to be taken into consideration in relation to the communications received in the SIIF are warranted.
- **C** The data processors that eventually will be designated.
- **D** Data Protection Officer (DPO) / Responsible for Data Protection.
- **E** Persons and/or entities involved in the management of the SIIF.

4 INDEPENDENT WHISTLEBLOWER PROTECTION AUTHORITY

The Internal Information System (SIIF) of the Entity is the primary and mandatory means for reporting illicit conduct or infractions of which one is aware, as it ensures the proper adoption of protective measures and promotes a culture of information within the organization.

However, other "external" information channels have been determined, in order to offer citizens an alternative where they can submit a communication and/or complaint, in the event that the internal channels do not comply with the guarantees required by the applicable regulations, the pertinent protection measures are not applied, or the persons are exposed to reprisals due to their status as informants.

Therefore, any individual can directly report to the **Independent Authority for Informant Protection (A.A.I.)** the commission of any actions or omissions constituting a violation of the legal system through the external information channel of this specialized public authority. Access to this external information channel and the contact details of the Authority are published on its website.

5 CONFIDENTIALITY AND PROTECTION OF PERSONAL DATA

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

In compliance with the principle of data minimization, the personal data collected are those necessary and relevant for the processing of the communication. In the event that data are collected by accident, which are not necessary for the knowledge and investigation of the actions or omissions, they will be deleted without undue delay. Likewise, the data will be retained for the time necessary to decide on the precedence of initiating an investigation.

On the other hand, the design of the SIIF ensures the **confidentiality** of the informant's identity and any third party mentioned in the communication, as well as the actions taken in the management and processing of the same. In this regard, access to personal data and other information contained in the system is limited to those responsible for management within the scope of their competencies and functions. Therefore, appropriate technical and organizational measures are in place to preserve the identity of those affected and prevent unauthorized access.

In case of any doubt or inquiry regarding the processing of personal data carried out within the Entity in relation to the SIIF, any concerned party can contact the appointed **Delegate/ Data Protection Officer**, using the contact details that have been previously communicated and made available to them.

6 PROTECTION MEASURES

Persons who report or disclose infractions using the Entity's **Internal Information System (SIIF)** have the **right to protection** under the same conditions as those who report through external channels, provided they have reasonable grounds to believe that the information is true at the time of communication or disclosure, even if they do not provide conclusive evidence.

Expressly prohibited in this regard are acts constituting **retaliation**, including threats and attempts, against persons who submit a communication. Retaliation is understood as:

a Acts or omissions prohibited by law.

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

For illustrative purposes and not limited to, the following are considered retaliatory acts:

> Suspension of the employment contract, dismissal, termination of the relationship, early termination, annulment of the employment and/or commercial contract, disciplinary measures, reprimand or other penalty, demotion or denial of promotions, substantial modification of conditions, non-conversion of temporary contracts into permanent ones, or equivalent measures.

> Damages (including reputational), economic losses, coercion, intimidation, harassment, or ostracism.

> Evaluation or negative references regarding work or professional performance.

> Blacklisting or dissemination of information that hinders or prevents access to employment or contracts for works or services.

> Denial or cancellation of a license or permit.

> Denial of training.

> Discrimination, unfavorable or unjust treatment.

> Denial of incentives, benefits, bonuses, commissions, and any other form of compensation.

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

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

In order to ensure the right to protection of the informant and of the persons affected by the communication, the Entity has established the following technical and organizational measures, which apply from the initial moment when 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 informant's identity, as well as of the data and information derived from the submitted communications. In this regard, the Entity has established a series of internal information channels that allow for the anonymous submission of communications. These channels include:

    - **Digital Channel:** Digital platform for the submission of written communications.
    - **Face to Face Channel:** System for receiving communications through in-person meetings or videoconferencing.

    Regardless of the channel used, the SIIF ensures the 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 implementation of the SIIF, the Entity has appointed a Manager whose role is to oversee, monitor, and control its operation. In this regard, the Manager, along with the external expert, will take necessary protective measures and ensure their proper monitoring and implementation. The involvement of the external expert provides the Manager's functions with the autonomy and independence elements required by current regulations.

    Likewise, the Manager will be responsible for conducting a preliminary analysis of the received communications to determine the suitability of adopting specific protective measures for the informant and/or affected third parties. In addition, depending on the nature and scope of the information, the Manager will have the support and advice of those responsible for the different operational areas of the Entity for the successful conclusion of the investigation. The Manager may also seek the expertise of other third parties in areas that require expert opinion.

3. **Custody, management, and security of SIIF information:** The Entity has a document management system configured with appropriate security and control measures to demonstrate the effectiveness of the SIIF. It is noteworthy that this

system includes anonymization processes to prevent the identification of informants. Additionally, the Entity has adopted reasonable technical measures for the secure storage, retrieval, and safe elimination of information, as well as the implementation of access controls to prevent unauthorized use.

However, information that is false, distorted, manifestly lacks all credibility and foundation, or shows rational indications of being obtained through the commission of a crime is excluded from the mentioned protection. This is because all communications must be made under the principle of **good faith**, and therefore, the informant must have reasonable grounds to believe that the information is true at the time of communication. In summary, the principle of good faith requires that under no circumstances can it be inferred that there is falsehood, lack of truth, or an intention to seek revenge or harm to a third party.

It is important to remember that the protection measures are not only directed in favor of the informants. Also those persons to whom the facts related in the communication refer **(affected persons)** have a unique protection against the risk that the information, even with apparent signs of truthfulness, has been manipulated, is false or responds to other motivations. During the processing of the file, these persons have the right to the presumption of innocence, to judicial protection and defense, to access to the file, as well as to the confidentiality of the facts and data of the procedure and to the confidentiality of their identity. In conclusion, they have the same protection and rights enjoyed by the informant.

7 DISCIPLINARY REGIME

The non-compliance with applicable regulations and behaviors contrary to the instructions, policies, codes, procedures, and protocols of the Entity is grounds for the application of the **disciplinary regime at the labor and commercial levels**, in coordination with the provisions of the applicable Collective Agreement, the Workers' Statute, and other applicable rules.

The Entity will notify and sanction actions or omissions contrary to this Policy committed by employees, collaborators, or any member associated with the Entity, in particular:

- Failure to report any suspicion or knowledge of infractions and non-compliance with the regulatory framework and internal protocols and rules of the Entity through the SIIF.
- Any attempt or effective action to obstruct the submission of communications or prevent, frustrate, or slow down their processing.
- The use of the SIIF in bad faith, for example, by providing information or documentation knowing it to be false.
- The adoption of any retaliatory action as a result of the communication against the informants or other affected persons.
- The violation of the guarantees of confidentiality and anonymity, revealing the identity of the persons concerned and breaching the duty of secrecy of the information.
- Failure to comply with the obligation to collaborate with the investigation of information.

8 PUBLICITY, REVIEW AND UPDATING

This Policy, as well as all the necessary information about the use of the **Internal Information System (SIIF**) implemented, is available in a separate and easily identifiable section, so that all interested parties have access to it in a clear and easily accessible manner. However, anyone can request additional information from the Entity through the contact details of the Manager.

The Responsible will periodically review and, if necessary, propose to the Entity's management or governing body the update of this Policy in order to adapt it to all circumstances and changes that may arise, as well as to any regulations or jurisprudence that may be issued. All of this is aimed at aligning the SIIF with the highest requirements of regulatory compliance for its proper functioning and effectiveness.

In the same way, the Entity is open to any **suggestions and/or proposals** that may improve its ethical performance and promote a culture of regulatory compliance, emphasizing the need for all employees and members associated with the Entity or third parties to collaborate in upholding its values and principles.

9 INTERNAL INFORMATION CHANNELS

In order to comply with the provisions set forth in Law 2/2023, the Entity has implemented a system configured with the technical and procedural requirements required by said Law for the proper handling of communications. All of this with the aim of providing informants with a secure, confidential, or even anonymous communication environment with the Entity and processing information in an efficient, professional, and independent manner.

For this purpose, the Entity has equipped itself with material, technical, and human resources to enable different internal channels 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 protection, informant protection, and other applicable areas for this type of channels.

It should be noted that the information provided through any of the internal channels will be treated confidentially, and only authorized personnel will have access to it for its proper management and processing.

The following are the channels available to any employee or third party related to the Entity for the presentation of communications:

Digital Channel

CORPORATE LINE
Canal de comunicaciones

The Entity has a digital tool that allows the submission of written communications through a form, which allows for the attachment of files. Once the form is completed, the tool automatically generates a code that enables proper tracking and management by the person in charge of processing. Also, a confirmation is sent to the informant regarding the entry and registration of the communication in the system, which includes a summary of the provided information, as well as the code for the informant to track the submission.

This tool has security measures in place to ensure the protection of information, the identity of the informant, and those individuals affected by it, as well as the confidentiality and confidentiality of the entire process of managing and processing the communication. In this regard, the Entity ensures a secure and diligent communication environment for the receipt of communications.The tool also allows for the submission of anonymous communications.

Thanks to the communication and tracking system it provides, the informant and the System Responsible can communicate through the tool, regardless of whether the communication has been submitted anonymously.

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

Face to Face Channel

Another channel that the Entity makes available to its employees and those third parties associated with it is the "face to face" or presential channel. Its purpose is to allow the submission of verbal communications through an in-person meeting or videoconference. In this case, considering the complexity involved for the Entity in ensuring the informant's anonymity when requested, the Entity has entrusted this function to the external expert BONET consulting. They are responsible for receiving and managing communications with these characteristics, as well as those in which informants are identified and in-person management is required. In this regard, the external expert ensures the protection of the informant's identity in the process of scheduling an appointment, in the submission of a communication in-person format, and at the location of the meeting.

In order to ensure security and preserve the integrity of the information provided by the informant, the meeting will be recorded in accordance with the provisions of the law and with the prior consent of the informant. This meeting will be documented in a secure format, with the security measures and anonymization required by the regulatory framework. In this regard, BONET consulting has and will enable the necessary technological mechanisms for the submission of additional documentation to the information provided in the meeting.

To use this channel, the Entity has provided a phone and an email contact to request the submission of communications in this format, and the coordination of the meeting will be exclusively handled by BONET consulting. The contact details for making this request are properly published on the Entity's website.