INTERNAL INFORMATION SYSTEM MANAGEMENT POLICY

GHI GLOBAL ADVISORY PARTNERS, AV, S.L.

DOCUMENTARY RECORD

PROCESS MANAGER	Internal System Manager

	DATE	ORGANIZATIONAL UNIT
ELABORATED	04/06/2024	Regulatory Compliance
REVISED	06/06/2024	Internal System Manager
APPROVED	06/06/2024	Board of Directors

EDIT CONTROL

DATE	EDITION	CONCEPT
06/06/2024	01	Elaboration of the procedure
15/04/2026	02	Transformation into a Securities Agency

TABLE OF CONTENTS

1. INTRODUCTION

In an ethical and responsible commitment, GHI GLOBAL ADVISORY PARTNERS, AV, S.L. hereinafter ("the Company") fosters a culture of regulatory compliance in its organization, since irregular conduct harms the organization in particular, and society as a whole. For this reason, the Company, seeking to prevent and avoid such conduct and protect those who report it effectively, has equipped itself with an Internal Information System as an instrument aimed at strengthening the organization's culture of information and integrity and communication that allows detecting regulatory breaches and acts of corruption in accordance with the provisions of Law 2/2023. of 20 February, regulating the protection of persons who report regulatory and anti-corruption infringements (hereinafter "Law 2/2023" or "the Law") which transposes Directive 2019/1937, of the European Parliament and Council, of 23 October 2019, on the protection of persons who report breaches of Union law (hereinafter "the Directive") into Spanish law.

The purpose of the Law is to protect, against possible reprisals, persons who, in a work or professional context, detect serious or very serious criminal or administrative infractions or omissions and report or report them through the mechanisms regulated therein. To this end, the Law requires any entity obliged by this law to have a preferential channel to report on the actions and infractions referred to in the law itself, referred to therein as the "Internal Information System" (hereinafter also "SII"), as well as to implement an internal information channel (hereinafter also "CII") and to have a procedure for managing the information received.

As an essential part of its Information System, the Company has set up internal information channels in order to enable the reporting of breaches in terms of regulatory compliance, fraud and corruption provided for by Law 2/2023 of 20 February by all the persons established in said regulations. In compliance with the provisions of the aforementioned Law and in order to ensure the correct application and management of the Internal Information System and Channel, the Board of Directors of the Company has approved the creation of this information management procedure.

2. DEFINITIONS

For the purposes of this Procedure, the following definitions shall apply:

- **Informant:** natural or legal person who has obtained information on actions or omissions that may constitute infringements in a work or professional context, including in any case those provided for in point 3.1., and who brings them to the attention of the Company.
- **Affected or affected person:** natural person to whom the reporting person is attributed with the commission of the offences referred to in point 3. 1. Affected persons shall also be considered to be those who, without having been informed by the informant, through the acts of investigation of the procedure have become aware of the alleged commission by them of the infringements referred to above.
- **Third parties:** natural persons who may have knowledge of aspects related to the reported infringement, either as a direct or indirect witness and who can contribute information to the proceedings.
- **Internal Information System (SII):** is the information channel established in the Company to report on the actions or omissions constituting an infringement provided for in point 3.1, with the functions and contents set out in point 4. It includes the Internal Information Channel (point 6.1) and the Information Management and Information Registration System (management procedure in point 7).
- **Internal Information Channel (CII):** The channel specifically enabled by the Company to receive information related to the subject matter of this procedure (point 3.1). More detail in point 6.1.
- **Independent Authority for the Protection of Whistleblowers (AAI):** It constitutes the basic pillar of the institutional system in terms of whistleblower protection. Administrative authority at the state level, with its own legal personality, full capacity to act publicly and privately, which will act in the development of its activity and for the fulfilment of its purposes with full autonomy and organic and functional independence with respect to the Government, the entities that make up the public sector and the public authorities in the exercise of their functions, although he is

accountable for his management to Congress and Senate. It relates to the Government through the Ministry of Justice, to which it is linked.

Its main functions, indicated in the Law, are the management of the external information channel to which any whistleblower can go (point 6.2), whistleblower protection, sanctioning, advisory and information on general provisions within the scope of its competences and the promotion of the culture of information.

3. OBJECTIVE

Through this procedure, the necessary provisions are documented and established so that the Information System and the internal information channels associated with it are adapted to the requirements established by Law 2/2023 and by the applicable regulations on the reporting of regulatory breaches and corruption.

The objective of the Information System of the Society is to strengthen the culture of information and its integrity, as well as the promotion of the culture of communication as a mechanism to prevent and detect threats to the public interest.

The Information System shall have the necessary measures in place to provide adequate protection against retaliation to natural persons who report any of the infringements defined in paragraph 4 and follow the procedures defined in this document

4. SCOPE OF APPLICATION OF THE INFORMATION SYSTEM

This section establishes the scope of the scope of protection of the Information System, as well as the protection measures established therein.

4.1. MATERIAL SCOPE OF APPLICATION: Communications protected by the Information System.

The Information Management Procedure integrated into the Information System will provide protection against the communication of the following infringements for which information has been obtained in a work or professional context:

- Infringements of European Union law under EU Directive 1937/2019:
  - Matters of financial services, transport safety, environmental or consumer protection, public health, food safety and animal welfare, public procurement and awards, listed in Annex I;
  - Fraud affecting the EU's financial interests, as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU)
  - They have an impact on the internal market, as referred to in Article 26(2) TFEU, including infringements of EU competition rules and aid granted by States, as well as infringements relating to the internal market in relation to acts infringing corporation tax rules or practices aimed at obtaining a tax advantage that undermines the object or purpose of the applicable legislation to corporation tax.
- Serious or very serious criminal or administrative offences. All offences that involve economic damage to the Public Treasury and Social Security, as well as those related to harassment defined in Organic Law 3/2007, of 22 March, for effective equality between women and men, will be understood to be included.

This protection shall not exclude the application of the rules relating to criminal proceedings, including investigative measures.

The protection provided for workers who report breaches of labour law in the field of occupational safety and health is without prejudice to that established in their specific regulations.

The following will not have the protection measures and guarantees described in this procedure:

- Information that affects classified information.

- Information relating to infringements in the processing of procurement procedures containing classified information or which has been declared secret or reserved, or those whose execution must be accompanied by special security measures in accordance with current legislation, or in which the protection of interests essential to the security of the State so requires.

  In the event of information or public disclosure of any of the infringements referred to in Part II of the Annex to the Directive, the specific regulations on the notification of infringements in these areas shall apply.

- Communications that are no longer accepted by an internal channel of information of the Society, those that lack any credibility or that are already available to the public or that constitute mere rumors.

4.2. SUBJECTIVE SCOPE OF PROTECTION

The internal information system will provide protection to natural persons who report infringements that occur in a work and/or professional context:

- Personnel linked by an employment relationship to the Company.
- Self-employed workers who maintain, or have maintained, a professional activity with the Company.
- Shareholders and persons belonging to the administration, management or supervisory body of the Company, including non-executive members.
- Any person who works for or under the supervision and direction of contractors, subcontractors and suppliers of the Company.
- Informants who report information on infringements obtained in an employment or statutory relationship that has already ended, volunteers, trainees, trainees or not, whether or not they receive remuneration, and those whose employment relationship has not yet begun, if the information on infringements has been obtained during the selection process or pre-contractual negotiation.

The whistleblower protection measures provided for in the law shall also apply to:

- Natural persons who, within the framework of the organisation in which the informant provides services, assist the informant in the process,
- Natural persons who are related to the whistleblower and who may be subject to retaliation, such as co-workers or family members of the whistleblower, and
- Legal entities, for which you work or with whom you have any other type of relationship in a work context or in which you hold a significant participation. For these purposes, it is understood that the participation in the capital or in the voting rights corresponding to shares or participations is significant when, due to its proportion, it allows the person who holds it to have the capacity to influence the investee legal person.

At a general level, and except for the exceptions established in the regulations and in this procedure, legal persons will not have access to the guarantees of protection of the Information System.

5. RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM.

The Company's Board of Directors has appointed one of its directors as Head of the Information System as the figure in charge of ensuring the diligent management of the system. The System Manager will exercise his position independently of the Board of Directors, having adopted the necessary measures to ensure that he exercises his functions autonomously and independently.

The person in charge of the Information System shall monitor the information provided by the communities through the Internal Information Channel and shall be responsible for the diligent management of the system.

6. CHANNEL IDENTIFICATION

6.1. INTERNAL INFORMATION CHANNEL

In order to ensure that the system is managed securely, the Company has the services of a computer software application for the submission of communications. This tool allows the submission of information protected by this procedure in a secure manner, in application of both national legislation and Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

The Head of the Information System will be the figure in charge of supervising that the technical solutions used to support the internal information channel are in accordance with the minimum security and confidentiality requirements established by the applicable regulations and by this procedure.

The technological system adopted has appropriate technical and organisational measures to preserve the identity and guarantee the confidentiality of the data of the affected persons and any third party mentioned in the communication. The system also has guarantees of compliance with the GDPR regulations. Communications over the channel are end-to-end encrypted and have guarantees that IP addresses cannot be traced.

The Internal Channel, detailed below, integrates the different internal information channels that already exist within the Company, regulated in the Company's internal procedures and policies, mainly relating to the prevention of whistleblowing channels for conflicts of interest, for suspicious transactions due to market abuse and insider trading and on possible breaches in the prevention of money laundering and terrorist financing (Manual of prevention of money laundering and terrorist financing) and possible breaches of the Internal Code of Conduct that serves as the Company's code of ethics.

6.1.1. PROCEDURE: MANAGEMENT OF THE INTERNAL INFORMATION CHANNEL

How to make a communication.

To make any communication, you must access the web address provided on the Company's homepage https://ghiglobalpartners.com/es/canal-de-denuncias/ in a separate section and submit the information considered necessary by the informant to report any of the infringements provided for in this procedure and the applicable regulations.

It is recommended, as far as possible and in order to streamline the internal processes of communication management and investigation, that the information submitted be as descriptive as possible and that such means of proof as are considered appropriate for the investigation and proof of the facts alleged be provided. In addition, it is recommended that communications be supported by documentary evidence, and witness evidence – including the testimony of the informant himself – or other means of evidence admissible in law are also admissible, although failure to provide them will not mean that they are inadmissible by default.

It may also be presented, at the request of the informant, by means of a face-to-face meeting within a maximum period of seven days, requesting it in the initial communication. These meetings, with the prior consent of the informant, will be documented through a complete and accurate transcript of the conversation carried out. The informant will be offered the opportunity to check, rectify and accept by signing said transcription.

Once the communication has been made, the system will provide the informant with an Identification Code in order to ensure contact between the Company and the informant even if anonymity has been chosen in the communication

When the information is not sent through the Internal Channel and reaches members of the Company other than the System Manager, they have the obligation to send it immediately to the System, as well as the duty to preserve confidentiality and refrain from carrying out any action that may directly or indirectly reveal the identity of the informant and the person affected. The disclosure by the third party receiving of the mere existence and, where appropriate, of the content of the information, may entail a breach of the guarantees of confidentiality and anonymity, conduct classified as a very serious infringement in article 63.1.c) of Law 2/2023 of 20 February.

Channel recipients

The Company has the management services of the Internal Information System by an external third party, which will be responsible for the initial reception, classification and review of the admission to processing of the communications received. Likewise, the Information System Manager will also have access to the internal information channel.

In the event that the information refers to any of the recipients of the internal information channel, systems must be established to prevent the affected persons from accessing the information.

Formal requirements of the communication

The communication must contain at least the following requirements:

- Identification of the informant. (unless the information is submitted anonymously).
- Description of the facts.
- Identification of the person or persons affected.
- Identification, where appropriate, of third parties who may provide relevant information.
- If the right to refuse to communicate with the RSII is exercised.

When submitting the information, if he does not exercise this waiver, the informant may indicate an address, email or safe place for the purpose of receiving communications such as acknowledgement of receipt, etc. The email will in no case be used to request confidential information.

If the IHR finds that any of the requirements just indicated are lacking, it will proceed to request the correction as far as possible.

Acknowledgment of receipt

Upon receipt of the communication, the Information System Manager must send an acknowledgement of receipt to the informant within a period of no more than 7 calendar days, counted from the date of the communication. Receipt of the communication will not be acknowledged in those cases where, with reasons, it is considered that such acknowledgement of receipt may jeopardize the confidentiality of the communication.

With the acknowledgement of receipt, the following information will be sent to the informant to the informant:

- Clear and accessible information on the external channels of information to the competent authorities, as well as to the institutions, bodies, offices or agencies of the European Union as provided for in Annex II.
- Privacy Policy on the Company's Data Protection
- Information that their identity will be reserved in any case and will not be communicated to the persons to whom the facts reported refer or to third parties.
- Information regarding the processing of personal data in accordance with the provisions of the GDPR.
  With respect to third parties who appear in person, they will be provided, at the time of such appearance, with information regarding the processing of their personal data in accordance with the provisions of the GDPR.
- Information on the possibility of submitting the information to the AAI.

Admission for processing

Once the communication has been received, the System Manager will proceed to assess the admissibility of the communication, in order to assess whether the information complies with the material scope indicated in section 4.1. of this document and is submitted by a person with access in accordance with the provisions of section 4.2. As a result of this initial analysis, it will decide not to admit the communication, if it does not conform to the scope mentioned above, or to admit it for processing.

The person in charge of the Information System must inform the informant of the admission of the investigation procedure, or, where appropriate, its inadmissibility.

In the event that due to lack of evidence it is not possible to continue with the investigation process, this circumstance must be communicated to the informant in order to request the submission of additional information. In the event that this is not provided within 10 days, the informant will be informed of the impossibility of continuing with the investigation and proceeding to finalize and archive the communication.

Even in the event that it is decided not to admit the investigation, a record of the communication must be kept.

In the event of admission, the analysis or instruction procedures will be initiated, including interaction with interested parties and communications and compliance with the requirements regarding the protection of personal data. In the event of inadmissibility, the file will be managed and the informant will be notified of this.

The information will be sent immediately to the Public Prosecutor's Office when the facts could constitute an offence, or to the European Public Prosecutor's Office in the event that the facts affect the financial interests of the European Union. In this case, the procedure will be terminated by recording this circumstance in the register of the same.

6.2. INSTRUCTION AND STUDY PHASE

From the receipt of the communication, and in the event of admission for processing, the investigation process will begin, and the provisions of the internal investigation procedure established by the Company must be followed

In accordance with the provisions of the applicable regulations, the maximum period for the resolution and response to the investigation actions will be 3 months from the sending of the acknowledgement of receipt. This period may be extended for another 3 additional months for those cases that are considered to be of special complexity.

The investigation, carried out by the System Manager, will include all those actions aimed at verifying the plausibility of the facts reported. The acts of investigation shall be carried out in such a way as to guarantee the fundamental rights of the informant and the affected person.

The communications that are made with the affected person, as well as all the acts in this phase of investigation, are documented in the information management system and their result is recorded, whether they have been collected by issuing the corresponding acknowledgement of receipt, or if they have been refused in the Information Register. The affected party is not obliged to declare or comply with the requirements of the RSII, without prejudice to the record of this circumstance in the file.

6.2.1. INFORMATION TO THE AFFECTED PERSON

Within a maximum period of 15 working days from the admission decision, the affected party will be informed of the existence of the proceedings, of the facts reported succinctly, unless such communication may facilitate the concealment, destruction and alteration of evidence, in which case, the person in charge of the System may modify said period until such circumstances disappear.

In addition, you will be informed of your right to submit written allegations and provide the evidence you consider, to request an interview with the System Manager and the processing of your personal data.

In no case will the affected subject be informed of the identity of the informant nor will he be given access to the communication. The affected party will be warned of the consequences of disclosing information to third parties under the terms provided for in Law 2/2023.

6.2.2. HEARING PROCEDURE.

Once the communication indicated in the previous point has been received, the affected party may submit allegations and the documentation they deem appropriate within 15 working days.

If the System Manager considers it appropriate to carry out an interview, or if it is requested by the affected party, the System Manager sets it with an indication of the place, date and time and will communicate it to the affected party. Without prejudice to the above, the affected party has the right to be heard at any time.

Communications and interviews will be carried out with the greatest possible discretion, in order to preserve the secrecy of the proceedings, preserving the identity of the informant, third parties and affected parties, and, in any case, guaranteeing the confidentiality of the information.

If, during the investigation of the procedure, it is found that the facts could be of the nature of a crime, the person in charge of the system will refer the proceedings to the Public Prosecutor's Office and will issue a report expressly stating this circumstance and the completion of the procedure.

6.2.3. ACCESS TO THE FILE.

At any time during the processing of the procedure, the informant and the affected party will have the right to access the content of the file, provided that such access does not facilitate the concealment, destruction and alteration of evidence, in which case the System Manager may defer access in a reasoned manner, until such circumstances disappear. The System Manager will adopt the necessary measures to ensure that access takes place while preserving the identity of the informant.

In the event that the file is accessed, this will be recorded in the information management system, with an indication of the content, date and time in the Register.

The affected party has the duty to maintain the confidentiality of the information to which he or she becomes aware as a result of access to the file. Any action aimed at identifying the informant or third parties is prohibited.

6.3. COMPLETION OF THE INTERNAL PROCESS

Once the communication has been admitted for processing and after its study, the System Manager will issue a report, and the informant will be notified, to the extent that he or she is identified and has not made use of the right to refuse to communicate with the System Manager, and the affected person.

Once the report has been issued, the System Manager will adopt one of the following decisions with the file:

- The archive of the same.
- Referral to the Public Prosecutor's Office or the European Public Prosecutor's Office if there are indications of a crime.
- The communication of the information to the competent authority or to the AAI if it considers that the facts reported could constitute serious or very serious misconduct.

  In the latter case, the System Manager transfers the information obtained and the result of its analysis to the competent authority through a procedure that guarantees the confidentiality of the identity of the informant and the information transferred.

In any case, the System Manager must respond to the investigation actions within a period that may not exceed three months from the receipt of the communication or, if no acknowledgement of receipt was sent to the informant, three months from the expiration of the period of seven days after the communication was made. except in cases of special complexity that require an extension of the term, in which case, it may be extended up to a maximum of three additional months.

6.4. RECORDING OF INFORMATION

The information management system will be contained in an Information Register, which is a secure database with restricted access to the System Manager, in which all communications received will be recorded with at least the following data:

a) Date of receipt
b) Identification Code
c) Actions developed
d) Measures taken
e) Closing date

Without prejudice to the Register of Information referred to above, the submission of information shall be documented, where appropriate:

1. By means of a copy of the document presenting the information.
2. Through the complete and exact transcription of the conversation held in the face-to-face meeting, if it has taken place.

From the beginning of the process, the System Manager guarantees the confidentiality of the interlocutor and the protection of their personal data. The system will not store personal data that are not essential for the knowledge and processing of the information received. The IHR will delete unnecessary personal data.

This register will not be public and may only be accessed by reasoned request of the competent judicial authority, by order, and within the framework of a judicial procedure and under the protection of the latter.

Personal data relating to the information received and the actions of the System Controller will only be kept for the period that is necessary and proportionate for the purposes of complying with Law 2/2023.

The System Manager will delete these personal data after a set period (in any case less than one year), after which only the non-personal information will remain in the Information Register Book for the purposes of monitoring actions and statistics.

7. RIGHTS OF THE WHISTLEBLOWER

The main rights of the informant, apart from what is indicated in Law 2/2023 are:

1. You can freely choose the channel, internal or external, to which to direct your communication.
2. In the case of the Company's CII, it may submit the information by post or, if requested, in person.
3. To appear before the IHR on their own initiative.
4. You may submit the communication anonymously, therefore you have the right to preserve your identity.
5. To the protection of your personal data.
6. To indicate an address, email or safe place where to receive communications from the RSII.
7. The confidentiality of your data and communications is guaranteed throughout the process of managing the information submitted.
8. You also have the right to opt out of being sent communications after the submission of the information.
9. Unless you expressly waive the right to receive communications or submit your communication anonymously, you have the right to know the status of the processing of your communication and the final result of the RSII's action within the established deadlines.
10. Persons who report or disclose infringements provided for in the scope of application of Law 2/2023 will be entitled to protection provided that:
    a. have reasonable grounds to believe that the information is true at the time of the communication, even if they do not provide conclusive evidence, and that this information falls within the scope of this Act.
    b. the communication has been made in accordance with the requirements provided for in the law.

The Act expressly prohibits acts constituting retaliation against the whistleblower, including threats of retaliation and attempted retaliation against persons who submit a communication in accordance with the provisions of the Act, which are classified as a very serious offence under section 63 of the Act. Retaliation includes, but is not limited to, suspension of the employment contract, dismissal or termination of the employment relationship, degradation or denial of promotion, intimidation, harassment, discrimination, or unfavorable or unfair treatment. More detail on prohibited retaliation and whistleblower protection measures in Title VII of the Act.

The rights provided for in points 2, 4, 5, 6 and 7 above are recognised for third parties in the proceedings. Without prejudice to the possibility of extending to them, and as far as possible, the support and protection measures for the whistleblower provided for in Law 2/2023.

8. RIGHTS OF AFFECTED PERSONS

The persons affected have the rights recognized by the Constitution and the laws, which must be guaranteed by the person in charge of the system, and in particular the following:

1. To be informed as soon as possible of the information affecting them, and to be heard at any time.
2. To the presumption of innocence.
3. To honor and privacy.
4. Right of defense, using the means valid in law for the same and to be assisted by a lawyer.
5. The right of access to the file in the terms regulated by law, with access to the proceedings against them, without prejudice to the time limitations that may be adopted to guarantee the outcome of the proceedings.
6. To the preservation of their identity, in front of any person outside the System Manager.
7. To the protection of your personal data.
8. To the confidentiality of communications, facts and data of the procedure.

The persons affected by the communications made in the internal information channels will be informed of the actions or omissions attributed to them, of their right to be heard, as well as of their rights, within a period and in the manner considered most appropriate to guarantee the successful completion of the investigation.

The person affected by the information will have the right of access to the file. Upon request, all personal information or data of third parties, such as the informant, witnesses or other persons mentioned, must be removed from the documents. In cases where, due to the nature of the information or the facts described therein, the identity of the informant or of third parties is obvious or easily identifiable, the right of access to the informant's file may be postponed, until the necessary guarantees are taken to ensure the confidentiality of the identity of the informant or third parties.

9. GUARANTEE OF CONFIDENTIALITY IN THE CASE OF COMMUNICATIONS BY MEANS OUTSIDE THE INTERNAL CHANNEL.

In the event that communications are sent outside the internal information channels within the scope established by this procedure, the recipients of the communication must maintain confidentiality about the information received and immediately communicate it to the Internal Information Manager.

Failure to comply with this obligation will be a very serious infringement in accordance with the provisions of Law 2/2023, of 20 February.

The Company has internal organisational measures aimed at ensuring that all its staff have been trained on the obligation established in this article.

10. INFRACTIONS-SANCTIONING REGIME

The AAI is the competent body for hearing the infringements contemplated in Title IX of Law 2/2023.

These offences include, inter alia, the adoption of any retaliation resulting from the communication to informants, the violation of the guarantees of confidentiality and anonymity provided for in the Law, the duty to maintain secrecy on any aspect related to the information, and the communication or public disclosure of information knowing that it is false.

11. INFORMATION SYSTEM GUARANTEES

The Information System has been configured to guarantee the confidentiality of the identity of the informant, as well as of any other person mentioned in the communication. The information system is configured so that it does not obtain data from the people who make communications.

Likewise, measures have been established to guarantee security and confidentiality in the management of communications and internal investigation procedures. The information in the communication will only be disclosed to those who are strictly necessary for the management of the investigation in accordance with the applicable regulations.

The identity of the informant may only be revealed outside the internal investigation procedure in the event of communication to the Judicial Authority, Public Prosecutor's Office or competent administrative authority in the framework of a criminal or sanctioning investigation. In these cases, such transfer will be indicated to the informant before revealing his identity, unless it could compromise the investigation or judicial proceedings.

The record book of the information received and investigations shall not be public, and only at the reasoned request of the competent judicial authority, by means of an order, and within the framework of a judicial proceeding and under the supervision of the latter, may the contents of the aforementioned register be accessed in whole or in part

11.1. GUARANTEE OF NON-RETALIATION AND PROTECTION OF THE WHISTLEBLOWER.

The Company's Board of Directors expressly prohibits acts constituting retaliation, including threats and attempted retaliation, against persons who submit a communication or who publicly communicate or disclose information in accordance with the protection requirements provided for in Law 2/2023 of 20 February.

Retaliation is understood to be any acts or omissions prohibited by Law 2/2023, which directly or indirectly involve unfavourable treatment that places the people who suffer them at a particular disadvantage compared to others in the work or professional context, just because of their status as whistleblowers or because they have made a public disclosure.

By way of example, the following are considered retaliation:

- Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including the non-renewal or early termination of a temporary employment contract.
- Damages, including reputational damages, or financial loss, coercion, intimidation, harassment or ostracism.
- Negative evaluation or references regarding work or professional performance.
- Inclusion of blacklists or dissemination of information that hinders or prevents access to employment or the contracting of works or services.
- Refusal of training.
- Discrimination, or unfavorable or unfair treatment.

In accordance with the provisions of the applicable regulations, natural persons who communicate information on actions or omissions set out in Law 2/2023 will not be considered to have infringed any restriction on the disclosure of information, and will not incur liability of any kind in relation to such communication, provided that they have reasonable grounds to believe that the information communicated is true at the time of communication and that the aforementioned information enters the information within the scope of application of the Law. This measure will not affect criminal liabilities.

The Head of the Club's Internal Information System must ensure that none of the people who communicate through the internal information system, external information channels or even through public disclosure in compliance with the requirements of the regulations are subject to any type of retaliation.

11.2. PRESUMPTION OF INNOCENCE.

During the processing of the investigation, the persons affected by the communication will have the right to the presumption of innocence, the right of defence and access to the file under the terms regulated in this procedure and Law 2/2023, of 20 February.

Likewise, the persons affected by communications will have the same protection as that provided for informants, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

12. PROTECTION OF PERSONAL DATA

The processing of personal data obtained through the SII will be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (also "General Data Protection Regulation" or "GDPR"); in Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights; and in Title VI of Law 2/2023 itself. More detail on the protection of personal data held by the Company is its procedure "PRC 007 Protection of Personal Data".

The IHR is the processor of the data received through the CII and the administrative body is the controller of the personal data received.

The SII prevents unauthorized access and preserves the identity and guarantees the confidentiality of the data corresponding to the affected persons and to any third party mentioned in the information provided, especially the identity of the informant in case he or she has been identified.

The identity of the informant may only be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation, and these cases shall be subject to the safeguards established in the applicable regulations.

If the information received contains special categories of data, it will be immediately deleted, unless the processing is necessary for reasons of an essential public interest as provided for in the GDPR, as provided for in article 30.5 of the Law.

Personal data whose relevance is not manifestly relevant to the processing of specific information will not be collected or, if collected by accident, will be deleted without undue delay.

In any case, after 3 months have elapsed since receipt of the communication without any investigation actions having been initiated, it must be deleted, unless the purpose of the conservation is to leave evidence of the operation of the system.

13. ADVERTISEMENT

The Company will provide all interested parties with appropriate and easily accessible information on the use of the internal information system implemented in its organization, and the essential principles of the procedure for managing the communications made.

The person responsible for the system must comply with the publication obligations.

This information is accessible through this document, and available for consultation on the Company's website at the following address: https://ghiglobalpartners.com/es/

14. IMPLEMENTING REGULATIONS

The main rules that apply in this procedure are:

- DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2019 on the protection of persons who report breaches of Union law.
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- Law 35/2003, of 4 November, on Collective Investment Schemes.
- Organic Law 10/1995 of 23 November 1995 on the Penal Code.
- Organic Law 3/2007, of 22 March, for effective equality between women and men.
- Law 10/2010, of 28 April, on the prevention of money laundering and terrorist financing.
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.
- Law 2/2023, of 20 February, regulating the protection of people who report regulatory breaches and the fight against corruption.

- Law 6/2023, of 17 March, on Securities Markets and Investment Services.

ANNEX I – FACTS THAT CAN BE COMMUNICATED THROUGH THE INTERNAL INFORMATION CHANNEL

LEGAL SYSTEM	SECTOR	SCOPE OF THE INFRINGEMENTS
Spanish legal system	Criminal	Serious or very serious infringements
	Administrative	Serious or very serious infringements
EU law	EU financial interests (Art. 325 TFEU)	Fraud and illegal activities
	Internal market (art. 26.2. TFEU)	Infringements of the internal market relating to the free movement of goods, persons, services and capital
		Infringements of EU competition rules and aid granted by States.
		Infringements of corporate tax rules. Practices aimed at obtaining tax advantages that distort the purpose of corporation tax
European Union law. Specific areas of the Annex to Directive 2019/1937	Public procurement	Public procurement
	Awards	Concession awards
		Security Contract Awards
		Award of contracts by entities in the sectors of: water, energy, transport, postal services
	Financial services, products and markets, and prevention of money laundering and terrorist financing.	Rules establishing a regulatory, supervisory and protective framework for investors and consumers in financial services and capital markets in the Union, banking, credit, investment, insurance and reinsurance, personal and retirement pensions, securities, investment funds and payment services
	Product Safety and Compliance	In manufacturing and distribution companies, possible abusive and unlawful manufacturing, importing or distribution practices relating to unsafe products
	Transport security	Safety requirements in rail transport, civil aviation sector, road transport, maritime sector, land transport of dangerous goods
	Protecting the environment Environment	Infringements committed against the protection of the environment, as they cause damage to the public interest and possible collateral effects beyond national borders. The rules established for the Environmental protection encompasses the following areas: environment and climate, sustainable development and waste management, marine, atmospheric and noise pollution, water and soil management, nature and biodiversity, chemical substances and mixtures, and organic products
	Radiation protection and nuclear safety.	Nuclear safety, radiation protection and the responsible and safe management of fuel that is consumed, as well as radioactive waste
	Food and feed safety, animal health and animal welfare	The aim is to report infringements in these areas to ensure the protection of human health, the interests of the consumer in relation to the food they consume and the effective functioning of the internal market.
	Public Health	To preserve the quality and safety of organs and substances of human origin, medicines and products for medical use and patients' rights
	Consumer protection	Linked to cases where unsafe products can cause significant harm to consumers
	Protection of privacy and personal data, and security of networks and information systems	Infringements against privacy and personal data, and security of networks and information systems, which may cause damage in the public interest

ANNEX II - EXTERNAL INFORMATION CHANNELS

Any natural person who is part of any of the groups with access to the Internal System may contact the external channel managed by the AAI (regulated in Law 2/2023 in its title III) or before the analogous channels of the corresponding authorities or regional bodies, either directly, or after the prior communication of information to the Internal Channel. to report on the commission of any actions or omissions included in the material scope of application of Law 2/2023. This external channel is:

- Channel established by the AAI (state body linked to the Ministry of Justice).

  [Pending completion once this channel has been created].

- Channel established by the Community of Madrid (regional body).

  https://www.comunidad.madrid/transparencia/canal-del-informante

There are other external channels of bodies to communicate information on the infringements included in the material scope of application of Law 2/2023. The main ones are:

- Bank of Spain:

  https://www.bde.es/bde/es/secciones/sobreelbanco/Transparencia/Informacion_inst/registro-de-acti/Canal_de_denuncias.html

- National Securities Markets Commission (CNMV):

  https://www.cnmv.es/portal/whistleblowing/presentacion.aspx

- SEPBLAC:

  https://www.sepblac.es/es/sujetos-obligados/tramites/comunicacion-por-indicio/

- Spanish Data Protection Agency

  https://whistleblowersoftware.com/secure/aepd-canal-proteccion-informante/9950b8af-daf7-493b-92ae-6eb1c7962d99

- Tax Agency

  https://sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/denuncias.html

- National Commission on Markets and Competition (CNMC):

  https://sede.cnmc.gob.es/tramites/competencia/denuncia-de-conducta-prohibida

- Independent Authority for Fiscal Responsibility

  https://www.airef.es/es/canal-de-denuncias/

- European Anti-Fraud Office:

  https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_es

  https://fns.olaf.europa.eu/main_es.htm

- External Channel of the European Union:

  https://european-union.europa.eu/contact-eu/make-complaint_es

- Infofraud (Treasury-Government of Spain):

  https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/paginas/denan.aspx

Through our website, we will inform you of any updates that may occur with regard to external information channels and the creation of external communication channels of the Independent Authority for the Protection of Whistleblowers A.A.I.