

**POLICY ON THE OPERATION OF THE
WHISTLEBLOWING CHANNEL OF GUIDE BRIDGE
SGEIC, S.A.**

1. PURPOSE

This policy has been developed by GUIDEBRIDGE SGEIC, S.A. (hereinafter, “the Company”) in order to set out the procedure followed in the internal whistleblowing channel established in compliance with, among other legal provisions, Article 8 of 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.

The purpose of the Whistleblowing Channel is to enable employees, clients, suppliers and third parties related to the Company or its activities to report any act that may have occurred within the Company and that may constitute an infringement, a criminal offence or a breach of our internal procedures, including, among others:

- Breaches of anti-money laundering and counter-terrorist financing (AML/CFT) regulations
- Breaches of data protection regulations (LOPD)
- Breaches of market abuse regulations
- Internal Code of Conduct

The Whistleblowing Channel represents an enhancement for the Company, which is committed to ethical conduct at all levels of the organisation.

Internal whistleblowing channels are an effective tool for detecting irregularities that would otherwise go unnoticed by other controls, although they must comply with technical and legal measures that safeguard the rights of the persons concerned.

The Company shall establish an effective management system comprising the strategies, processes and reporting procedures necessary to continuously identify, measure, monitor, manage and report the risks to which the Company itself and the persons involved in its activities are or may be exposed.

2. GENERAL RESPONSIBILITIES

The general responsibilities in relation to the Whistleblowing Channel are set out below:

- **Board of Directors**
 - Approval of this Policy and any subsequent updates thereto
 - Providing the Company with the resources necessary for the proper functioning of the Channel.
 - Updating this Policy
- **Internal Information System Officer**
 - Operation of the Whistleblowing Channel.
 - Ensuring the confidentiality of whistleblowers, where applicable.
 - Recording of reports
 - Retention of documentation
- **Internal Control Body for AML/CFT**
 - Supporting the Internal Information System Officer in relation to reports concerning breaches of the AML/CFT Law
- **Internal Code of Conduct (RIC) Monitoring Body**
 - Supporting the Internal Information System Officer in relation to reports concerning breaches of the Company’s Internal Code of Conduct
 - Supporting the Internal Information System Officer in relation to reports concerning breaches of market abuse regulations.

3. RECIPIENTS OF THIS MANUAL

This policy is addressed to employees, clients, suppliers and third parties involved in the Company’s activities who may make use of the Whistleblowing Channel in accordance with the provisions set out herein.

All directors, officers and employees, irrespective of the legal form governing their employment or service relationship, as well as suppliers, sponsors, collaborators, agents and members of the Company's various collegiate bodies, must report through the Whistleblowing Channel any irregularity or non-compliance of which they become aware and which falls within its objective scope, without fear of dismissal or any other form of retaliation, and in the assurance that the information provided will be treated with the utmost confidentiality.

4. WHISTLEBLOWING CHANNEL

4.1. OPERATION

The whistleblowing channel shall operate on a centralised basis through the following web address:

The channel is structured, in aggregate terms, as follows:

1. IDENTIFICATION

- a. REPORT INCLUDING THE WHISTLEBLOWER'S IDENTIFYING DETAILS
- b. ANONYMOUS REPORT

2. REPORT DETAILS

- a. REASON FOR THE REPORT
- b. DESCRIPTION OF THE REPORT

3. SUPPORTING EVIDENCE (OPTIONAL)

Reports submitted shall be received by the person designated by the Internal Information System Officer, a position held by Mr Manuel Garrido Valdivielso.

Upon submission of a report, an acknowledgement of receipt is automatically generated and sent to the whistleblower, provided that an email address has been supplied for that purpose.

Once received and recorded, the report shall be communicated to the Internal Information System Officer, preserving the confidentiality or anonymity of the whistleblower. Should the report concern the Internal Information System Officer, the person concerned shall not participate in the investigation of, or deliberations on, the reported facts.

In the case of reports concerning breaches of the RIC, of any of the Company's internal control policies or procedures or of this manual, or arising from any other type of regulatory non-compliance of a criminal nature, the Internal Information System Officer shall assess their validity and, should there be indications that unlawful conduct has been committed, shall proceed to analyse and investigate them in detail.

Within the framework of the internal investigation conducted by the Internal Information System Officer, the Officer may gather all such information and documentation as he or she deems appropriate from any of the Company's areas, departments or persons as may be necessary to clarify the facts, determine any consequences that may arise and decide on the course of action to be taken.

Following the analysis and investigation, which must be carried out as swiftly as possible having regard to the complexity and/or seriousness of the reported facts, the Internal Information System Officer shall take one of the following actions:

1. If it is concluded that the report is unfounded or lacks minimum seriousness, it shall be closed and the whistleblower shall be notified accordingly.
2. If it is concluded that there has been conduct contrary to the Internal Code of Conduct or to any other internal control policy or procedure of the Company, the matter shall be referred to the Head of Administration so that the relevant employment disciplinary proceedings may be initiated, which may result in the imposition of a sanction where the investigating body deems it necessary, in accordance with the regulations breached and the applicable employment regime.

3. If it is concluded that the breach has given rise to a criminal risk, determining whether it affects the Company or the reported person, once such risk has been assessed with the support of such departments as deemed necessary, the Board of Directors shall be presented with the measures considered appropriate to minimise the risk or prevent it in the future, where possible, as well as the possibility of training staff so that they are forewarned through the various means available within the organisation (training, circulars, notices), in coordination with the responsible departments.
4. If the investigation procedure initiated by the Internal Information System Officer
5. reveals reasonable indications that a criminal offence has been committed, the crime detection protocol shall be activated. This entails the Internal Information System Officer bringing the matter to the attention of the Board of Directors.
The Board, on the basis of the information received and the legal report, shall take the appropriate measures to report the infringement to the competent authorities, providing all the information available to it at that time.

Should the report concern any member of the Board of Directors and, following the investigation, there be indications of irregular activity, the Internal Information System Officer shall report to the Board of Directors, specifying that the person or persons concerned must be absent when a decision is taken on the resolution to be adopted.

The system ensures that whistleblowers acting in good faith are protected against retaliation and guarantees confidentiality at all stages.

4.2. RESPONSE PERIOD

The period for providing a response shall not exceed three months from the acknowledgement of receipt or, where no acknowledgement of receipt was sent to the whistleblower, three months from the expiry of the seven-day period following the submission of the report.

4.3. CONFIDENTIALITY AND PROHIBITION OF RETALIATION

Access to the report shall be restricted exclusively to the Internal Information System Officer, who shall guarantee the confidentiality of the identity of the whistleblower and of any third party mentioned in the report.

The Internal Information System Officer shall maintain the confidentiality of the whistleblower at all times, unless such information is required by an administrative or judicial authority.

Persons who have reported or publicly disclosed information on breaches anonymously, but who are subsequently identified and suffer retaliation, shall nonetheless be entitled to protection under Chapter VI of Directive (EU) 2019/1937.

4.4. RECORD-KEEPING

For each report, a file shall be opened in which the actions taken and the documentation generated in the course of its processing and resolution shall be kept up to date.

Reports shall be retained only for as long as is necessary and proportionate in order to comply with the requirements imposed by Directive (EU) 2019/1937 or other requirements imposed by Union or national law.

5. INTERNAL INFORMATION SYSTEM OFFICER

The Company has an Internal Information System Officer whose mission is the periodic supervision of the risk control and prevention systems established by the Company, so that the main risks are properly identified, managed and communicated internally for the purpose of their prevention.

The Internal Information System Officer:

- Is supported by such areas or organisational units as he or she deems appropriate to ensure the proper and effective performance of his or her duties.
- Is responsible for handling the reports received through the Whistleblowing Channel.
- Guarantees the confidentiality of all information received and is structured as set out in the following section.

5.1. COMPOSITION OF THE BODY

The person appointed to the Body must possess certain qualities that ensure his or her suitability, competence, integrity, autonomy and independence. The Internal Information System Officer shall perform the functions detailed below:

The Officer shall treat with the utmost confidentiality all information and documentation to which he or she has access or which is at his or her disposal, and may not use it for any purpose other than the investigation of incidents in this area.

In carrying out the supervisory and compliance duties, the Officer shall have the specific support of the Internal Audit function and the Risk Management function.

In the performance of the supervisory functions, the Officer shall act with the highest degree of autonomy and, in the exercise thereof, may:

- Access and obtain, where necessary for the performance of his or her duties, the information held by the Company.
- Request the support of any area or organisational unit, employee, director, adviser or any person having a professional and/or employment relationship with the Company in the context of an investigation.
- Have the appropriate means and necessary resources to carry out his or her duties, including the management of the financial resources allocated for the proper performance thereof.

6. PROCESSING OF PERSONAL DATA

Any processing of personal data carried out pursuant to Directive (EU) 2019/1937, including the exchange or transmission of personal data by the competent authorities, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680. Any exchange or transmission of information by Union institutions, bodies, offices or agencies shall be carried out in accordance with Regulation (EU) 2018/1725.

Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

7. APPLICABLE INTERNAL REGULATIONS

- Internal Code of Conduct
- Anti-Money Laundering and Counter-Terrorist Financing Manual
- Data Protection Procedure

8. APPLICABLE LEGISLATION

- 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.
- Law 10/2010, of 28 April, on the prevention of money laundering and terrorist financing.
- Law 35/2003, of 4 November, on Collective Investment Undertakings.
- Organic Law 10/1995, of 23 November, on the Criminal Code.
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights.
- Royal Legislative Decree 4/2015, of 23 October, approving the consolidated text of the Securities Market 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 (General Data Protection Regulation)