GLOBALIA'S POLICY ON THE INTERNAL REPORTING SYSTEM (ETHICS CHANNEL) AND WHISTLEBLOWER PROTECTION

Prepared by:	Reviewer:	Approved by:
Compliance Department	Compliance Officer	Board of Directors
Date: March 2026	Date: March 2026	Date: March 2026

UNCONTROLLED COPY IF PRINTED OR IF A DIGITAL COPY IS CREATED

Intentionally left blank

CHANGE LOG

Revision	Date	Modification
01	12/23	First draft
02	06/25	Policy Update
03	03/26	Inclusion of explicit references to the concept of harmful conduct and conceptual clarifications recommended by the AIPI

TABLE OF CONTENTS

1. POLICY ON GLOBALIA HOLDING'S INTERNAL REPORTINGAND WHISTLEBLOWER PROTECTION 5
2. PRINCIPLES GOVERNING GLOBALIA'SIN THE IMPLEMENTATION OF THE INTERNAL REPORTING SYSTEM AND WHISTLEBLOWER PROTECTION 5
3. RESPONSIBLE FOR GLOBALIA'S INTERNAL REPORTING SYSTEM 7
4. ESTABLISHMENT OF GLOBALIA'S INTERNAL REPORTING CHANNEL 8
5. WHO CAN BE A WHISTLEBLOWER AND WHAT INFORMATION IS COVERED BY GLOBALIA'S? 9
   5.1 Scope of Application 9
   5.2 Scope 9
6. PERSONAL DATA PROTECTION 11
7. MEASURES TO PROTECT WHISTLEBLOWERS AND AFFECTED INDIVIDUALS 12
   7.1 Acts Constituting Retaliation 12
   7.2 Measures to protect the whistleblower from retaliation 13
   7.3 Measures for the protection of affected individuals 14
8. MANAGEMENT OF INFORMATION RECEIVED BY THE HEAD OF GLOBALIA'S 14
9. TRAINING AND DISSEMINATION 16
10. DISCIPLINARY PROCEDURES 16
11. APPROVAL, PUBLICATION, AND ENTRY INTO FORCE OF THE POLICY 16
12. INTERPRETATION OF THIS POLICY 16

GLOBALIA GROUP COMPANIES

1. INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION POLICY GLOBALIA GROUP

Law 2/2023, dated February 20, regulating the protection of whistleblowers and the fight against corruption (hereinafter, Law 2/2023) transposes into Spanish law Directive 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law. The Directive uses the term "whistleblower," and Law 2/2023 has opted for the term "informant" and, consequently, this is the term also adopted by this document of the Globalia Group (hereinafter, Globalia, the Globalia Group, or the organization) and its constituent companies (GLOBALIA CORPORACION EMPRESARIAL SA, GLOBALIA MANTENIMIENTO AERONAUTICO SLU, GLOBALIA BROKER SERVICES SAU, GLOBALIA CALL CENTER SA, BELIVE HOTELS SL, GLOBALIA FORMACIÓN SLU, GLOBALIA SISTEMAS Y COMUNICACIONES SLU, GROUNDFORCE CARGO SLU, GLOBALIA HANDLING SAU, ALL GROUNDFORCE 2023 JOINT VENTURES, and GLOBALIA ARTES GRAFICAS SL).

Law 2/2023 explains and clarifies in its preamble that its purpose is to protect, against possible retaliation / harmful behaviors, individuals who, in a work or professional context, detect serious or very serious criminal or administrative offenses and report them through the mechanisms regulated therein.

In accordance with Law 2/2023, the organization, as a regulated entity, must have a dedicated channel for receiving and managing reports regarding the violations covered by the law, known as the "Internal Reporting System" or Ethics Channel. Likewise, the law requires the adoption of a policy establishing the general operating principles of the system and protection measures for whistleblowers; therefore, GLOBALIA has approved the Policy on the Internal Reporting System and Whistleblower Protection (hereinafter, the Policy).

Furthermore, this Policy is an integral part of the compliance culture established within our Organization.

The Board of Directors of Globalia promotes and approves this Policy, thereby fulfilling its role of establishing the necessary foundations for the proper and efficient management of the Internal Reporting System and promoting compliance with the principles and safeguards set forth in this Policy.

2. PRINCIPLES GOVERNING GLOBALIA'S ACTIONS IN THE IMPLEMENTATION OF THE INTERNAL REPORTING SYSTEM AND WHISTLEBLOWER PROTECTION

The basic principles of action on which this Policy is based are detailed below:

- **Regulatory Compliance**: Legality and corporate ethics are integral pillars of the System. Therefore, communications will be handled with integrity and professionalism, in compliance with applicable laws, internal regulations, and, in particular, data protection regulations.
- **Independence and impartiality:** The System will guarantee an impartial hearing and fair treatment for all persons involved. All persons participating in the procedure will act in good faith in the pursuit of the truth and the clarification of the facts.
- **Transparency and accessibility:** Care will be taken to ensure that information about the System and its regulations is communicated clearly and comprehensibly,

as well as ensuring the System's publicity and accessibility.

- **Traceability and security:** The System will incorporate all necessary measures to ensure the integrity, traceability, and security of information.
- **Confidentiality and Anonymity:** The System will guarantee the anonymity and, in any case, the utmost confidentiality of the whistleblower's identity, the information reported, and the actions taken in the management and processing of such information. Furthermore, the System will allow for the submission of anonymous reports.
- **Confidentiality:** The System will ensure that individuals involved in the processing and investigation of reports act with the utmost discretion regarding the facts they become aware of by virtue of their position or role.
- **Diligence and Speed:** The System will ensure that the investigation and resolution of reported incidents are handled with due professionalism and diligence and without undue delay, so that the procedure can be completed in the shortest possible time while respecting due process.
- **Good faith:** The System will ensure that information is communicated honestly, with integrity, and truthfully, notwithstanding any inaccuracies or omissions that the informant may unintentionally make.
- **Respect for and protection of individuals:** The System will ensure that appropriate measures are taken to guarantee the right to protection of the dignity and privacy of the individuals concerned.
- **Respect for fundamental rights:** The System guarantees the right to information, the right to privacy and data protection, the right to defense, the right to be heard, the right to the presumption of innocence, and the right to honor for all persons involved in the proceedings. Furthermore, these persons have the right to be heard at any time, in the manner deemed appropriate, to ensure the successful conclusion of the investigation.
- **Principle of Prohibition of Retaliation or Adverse Action Against the Whistleblower** (also known as harmful behaviors).
- **Principle of Objectivity, Neutrality, and Integrity.**

The principles underlying this Policy apply to all entities within the Globalia Group.

In implementing the Internal Whistleblower Reporting and Protection System, Globalia designates the Compliance Officer as the System Manager, ensuring the swift resolution of cases with guarantees of continuous operation, objective and multidisciplinary review of information, and compliance with legally established deadlines.

Globalia will ensure, through the independent actions of the System Administrator, the completeness, integrity, and confidentiality of the information; the prevention of unauthorized access; the long-term storage of the information; the comprehensive protection of the whistleblower; and the observance of good faith. To this end, in addition to the provisions of this document, the aforementioned principles will be incorporated into the information management procedure required by Law 2/2023, which the System Administrator must follow when reviewing the information received. Access to the Ethics Channel or Internal Reporting System is public and available via the following link:

https://globalia.canaletico.es/

Globalia will also ensure, through respect for the independent actions of the System Manager, objectivity and impartiality in the examination of the information received; it will

avoid conflicts of interest; it will respect the presumption of innocence; and it will guarantee the right to defense. These principles will likewise be reflected in the information management procedure, which is public and accessible on Globalia's website.

Globalia ensures access to the internal whistleblower reporting and protection system through an external web-based platform, the purpose of which is to receive, process, record, and retain all actions taken as a result of reports submitted by whistleblowers.

3. HEAD OF THE INTERNAL REPORTING SYSTEM FOR THE GLOBALIA GRO

The Head of the Internal Reporting System (hereinafter, RSII or System Head) is the Compliance Officer.

The RSII may delegate the powers to manage and conduct investigative proceedings to a person in the Compliance Department, who shall be considered a delegated manager.

In the exercise of their duties, neither the RSII nor the person designated by them shall receive instructions from any superior at Globalia, nor are they subject to an external hierarchy of said collegiate body, nor may they be removed from their positions for matters related to their legitimate participation in the Internal Reporting System. Therefore, they must perform their duties independently, impartially, and autonomously, with executive authority to decide on the actions to be taken upon learning of indications of any alleged criminal act that may have criminal consequences or any other type of consequences for the Organization. Likewise, the Compliance Officer has the authority to report alleged criminal acts to the Board of Directors whenever deemed necessary and, in any case, when such acts could seriously affect the Organization's reputation or Globalia's corporate interests.

4. ESTABLISHMENT OF GLOBALIA'S INTERNAL REPORTING CHANNEL

Globalia has established an internal channel for receiving reports (hereinafter, "CII") regarding acts or omissions that may constitute a serious or very serious criminal or administrative offense, as well as other actions provided for in Article 2 of Law 2/2023, which are listed in Section 5.2. The scope of this document includes all situations that violate GLOBALIA's Code of Ethics, its Anti-Corruption Policy, or any other internal or external regulations applicable to us.

The channel is administered by the RSII. Access to this channel shall be limited, within the scope of their powers and functions, to:

a) The System Manager (Compliance Officer) and the designated manager.

b) The Director of Human Resources or the duly designated competent person in the relevant area, only when disciplinary measures against an employee may be warranted.

c) The external investigating expert, if applicable.

d) The Data Protection Officer.

e) The head of the entity's legal services or whoever performs such functions internally, if legal action is warranted in relation to the facts described in the report.

The CII must technically guarantee the confidentiality or, where applicable, the anonymity of the whistleblower, to protect them from any leaks and subsequent retaliation/ harmful behaviors they may face.

5. WHO CAN BE A WHISTLEBLOWER AND WHAT INFORMATION DOES GLOBALIA'S INTERNAL REPORTING SYSTEM COVER?

5.1 Subject Scope

Any person who has an employment or professional relationship with Globalia may use the internal reporting channel and benefit from the protection afforded by Law 2/2023 as a whistleblower to report information regarding the acts or omissions described in Article 2 of Law 2/2023. This employment or professional relationship, which entails a dependency on Globalia, is what makes special protection against possible retaliation/ harmful behaviors necessary and appropriate.

In any case, for the purposes of Law 2/2023, the following are considered whistleblowers by Globalia:

a) Individuals who are employees of Globalia.

b) Self-employed individuals who currently engage in, or have previously engaged in, a professional activity with Globalia.

c) Shareholders, partners, and members of Globalia's administrative, management, or supervisory bodies, including non-executive members.

d) Any person working for or under the supervision and direction of Globalia's contractors, subcontractors, and suppliers.

e) Whistleblowers who report or publicly disclose information regarding violations obtained in the course of an employment or statutory relationship with Globalia that has already ended, including volunteers, interns, and trainees—regardless of whether they receive compensation—as well as those whose employment relationship has not yet begun, in cases where the information regarding violations was obtained during the selection process or pre-contractual negotiations.

5.2 Scope

With regard to the subject matter of the information, natural persons who report any of the following matters are protected:

a) Any acts or omissions that may constitute violations of European Union law, provided that:

1.º They fall within the scope of the European Union acts listed in the annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons reporting on breaches of Union law, regardless of how such acts are classified under domestic law;

2.º They affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); or

3.º Affect the internal market, as referred to in Article 26(2) of the TFEU, including infringements of European Union rules on competition and State aid, as well as infringements relating to the internal market in connection with acts that violate corporate tax rules or practices intended to obtain a tax advantage that undermines the object or purpose of the legislation applicable to corporate tax .

b) Acts or omissions that may constitute a serious or very serious criminal or

administrative offense. In any case, this shall be understood to include all serious or very serious criminal or administrative offenses that result in financial loss to the Treasury and to Social Security.

Furthermore, as set forth in Law 2/2023 itself, cases governed by specific regulations are excluded from the scope of application; that is, regulations governing the mechanisms for reporting violations and protecting whistleblowers as provided for by sector-specific laws or by the European Union instruments listed in Part II of the Annex to Directive (EU) 2019/1937.

Matters relating to potential harassment situations, regardless of their nature, and given their criminal nature and the potential implications for the company's criminal liability, will be handled in accordance with Globalia's existing Harassment Protocol, following the deadlines specified therein. Similarly, the team responsible for implementing the Harassment Protocol must maintain constant communication with the System Manager, to whom it must report in writing on all matters related to the case, from its initiation until its closure.

Furthermore, this internal reporting channel is not the appropriate avenue for expressing dissatisfaction or disagreement with the criteria established by Globalia in the legitimate exercise of its functions. Nor is it the appropriate channel for reporting on equal employment opportunities, labor disputes, or employee complaints related to issues such as schedules, vacations, salaries, etc. These matters shall be referred to the People or Human Resources department, which is the competent area for their management.

Finally, potential customer complaints are also not to be addressed through this internal channel; rather, they must be redirected to the Customer Service department of the relevant Division for resolution, noting that the System Administrator is not responsible for these matters.

UNCONTROLLED COPY IF PRINTED OR A VIRTUAL COPY IS CREATED

6. PERSONAL DATA PROTECTION

The processing of personal data arising from the application of Law 2/2023 shall be governed by the provisions of the GDPR and Organic Law 3/2018 of December 5 on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDPGDD).

The internal reporting system prevents unauthorized access, protects the identity of, and ensures the confidentiality of data pertaining to the individuals concerned and any third parties mentioned in the information provided, particularly the identity of the whistleblower, if identified. The identity of the whistleblower may only be disclosed 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 such cases shall be subject to the safeguards established in applicable regulations.

Under no circumstances shall personal data that is not necessary for the investigation of the acts or omissions be stored or processed; such data shall be immediately deleted where appropriate. Likewise, all personal data that may have been communicated and that relates to conduct not falling within the scope of the Whistleblower Protection Act shall be deleted.

If the information received contains special categories of personal data subject to special protection, it shall be immediately deleted, unless the processing is necessary for reasons of substantial public interest in accordance with the provisions of Article 9.2.g) of the GDPR, as provided for in Article 30.5 of Law 2/2023.

In any case, personal data whose relevance to processing specific information is not evident shall not be collected; if collected accidentally, it shall be deleted without undue delay.

Communications that have not been acted upon may only be retained in anonymized form, and the blocking obligation provided for in Article 32 of the LOPDPGDD shall not apply.

The data being processed may be retained in the information system only for the time strictly necessary to determine whether to initiate an investigation into the reported facts. If it is established that the information provided, or part thereof, is untrue, it must be immediately deleted as soon as such circumstance is confirmed, unless such lack of truthfulness constitutes a criminal offense, in which case the information will be retained for the time necessary to conduct the judicial proceedings.

In any case, if three months have elapsed since the receipt of the report without any investigative proceedings having been initiated, the information must be deleted, unless the purpose of retention is to provide evidence of the system's operation. Reports that have not been acted upon may only be retained in anonymized form.

The maximum data retention period in any case is 10 years.

7. MEASURES TO PROTECTION OF INFORMANT AND PERSONS AFFECTED

7.1 Acts Constituting Retaliation/Harmful Behavior

Acts constituting retaliation/harmful behavior, including threats of retaliation and attempts at retaliation against persons who file a report in good faith in accordance with the provisions of the law, are expressly prohibited.

Retaliation/Harmful Behavior are understood to mean any act or omission that is prohibited by law, or that, directly or indirectly, constitutes unfavorable treatment that places the persons suffering it at a particular disadvantage compared to others in the workplace or professional context, solely because of their status as whistleblowers or because they have made a public disclosure.

For the purposes of Law 2/2023, and by way of example, retaliation/harmful behavior includes actions taken in the form of:

a) Suspension of the employment contract, dismissal, or termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract after the probationary period has been completed, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, demotion, or denial of promotions, and any other substantial modification of working conditions, as well as the failure to convert a temporary employment contract into a permanent one, in the event that the employee had legitimate expectations that they would be offered permanent employment; unless these measures are carried out within the regular exercise of managerial authority under labor law or regulations governing the status of public employees, due to proven circumstances, facts, or violations, and unrelated to the submission of the complaint.

b) Intimidation, harassment, or ostracism.

c) Negative evaluations or references regarding work or professional performance.

d) Inclusion on blacklists or dissemination of information within a specific sector that hinders or prevents access to employment or the contracting of works or services.

e) Denial or revocation of a license or permit.

f) Denial of training.

g) Discrimination, or unfavorable or unfair treatment.

All of the above applies, unless these measures are carried out within the regular exercise of managerial authority under labor law, due to proven circumstances, facts, or violations, and unrelated to the submission of the report.

In the event of retaliation, the Head of the Internal Reporting System must be informed immediately. The Head of the System will conduct an investigation and periodically monitor the situation of the whistleblower and, where applicable, of those individuals covered by the protection regime. If the System Manager determines that, during the term of the protection regime, retaliation, stigmatization, or harassment has occurred in addition to any disciplinary measures and/or administrative sanctions that may apply to the perpetrators , the necessary and available measures will be

taken to restore the victim of retaliation to the situation prior to the harm suffered.

Any person whose rights have been infringed upon as a result of their communication or disclosure, after the two-year period has elapsed, may request protection from the competent authority, which, in exceptional and justified cases, may extend the period of protection, following a hearing with the persons or bodies that may be affected.

Administrative acts intended to prevent or hinder the submission of communications and disclosures, as well as those constituting retaliation/harmful behavior or causing discrimination following the submission of such communications and disclosures under Law 2/2023, shall be null and void and shall give rise, where appropriate, to disciplinary or liability measures, which may include the corresponding compensation for damages to the aggrieved party.

7.2 Measures to protect whistleblowers from retaliation/harmful behavior

Persons who communicate information regarding the acts or omissions referred to in paragraph 3, or who make a public disclosure in accordance with Law 2/2023, shall not be deemed to have violated any restriction on the disclosure of information and shall not incur any liability whatsoever in connection with such communication or public disclosure, provided they had reasonable grounds to believe that the communication or public disclosure of such information was necessary to reveal an act or omission under said law, all without prejudice to the provisions of the specific protection rules applicable in the workplace. This measure shall not affect criminal liabilities.

The provisions of the preceding paragraph extend to the communication of information by representatives of employees, even if they are subject to legal obligations of confidentiality or non-disclosure of confidential information. All of this is without prejudice, likewise, to the specific protection rules applicable in the labor sphere.

Whistleblower protection measures shall also apply, where applicable, to:

1) individuals who, within the framework of Globalia, assist the company in the process;
2) individuals who are related to the whistleblower and who may be subject to retaliation/harmful behavior, such as the whistleblower's coworkers or family members; and
3) a legal entity for which the informant works, with which the informant has any other type of relationship in a work context, or in which the informant holds a significant interest. For these purposes, an interest in the capital or in the voting rights corresponding to shares or equity interests is considered significant when, due to its proportion, it allows the person holding it to exert influence over the legal entity in which the interest is held.

Whistleblowers shall not incur liability with respect to the acquisition of or access to information that is communicated or publicly disclosed, provided that such acquisition or access does not constitute a crime.

Any other potential liability of whistleblowers arising from acts or omissions not related to the communication or public disclosure, or that are not necessary to disclose a violation under Law 2/2023, shall be enforceable in accordance with applicable regulations.

In proceedings before a court or other authority concerning harm suffered by whistleblowers, once the whistleblower has reasonably demonstrated that they have

reported or made a public disclosure of in accordance with Law 2/2023 and that they have suffered harm, it shall be presumed that the harm occurred as retaliation/harmful behavior for reporting or making a public disclosure. In such cases, the burden of proof shall rest with the person who took the harmful measure to demonstrate that such measure was based on duly justified grounds unrelated to the communication or public disclosure.

In legal proceedings, including those relating to defamation, copyright infringement, breach of confidentiality, violation of data protection regulations, disclosure of trade secrets, or claims for compensation based on labor or statutory law, whistleblowers shall not incur any liability whatsoever as a result of communications or public disclosures protected by Law 2/2023. Such persons shall have the right to assert in their defense, within the framework of the aforementioned legal proceedings, that they communicated or made a public disclosure, provided they had reasonable grounds to believe that the communication or public disclosure was necessary to bring to light a violation under Law 2/2023.

7.3 Measures for the Protection of Affected Individuals

During the processing of the case file, the persons affected (under investigation) by the report shall have the right to the presumption of innocence, the right to a defense, and the right to access the case file under the terms provided for in Law 2/2023, as well as the effective protection of their rights. The person under investigation shall be entitled to the same protection established for whistleblowers, with their identity protected and the confidentiality of the facts and details of the proceedings guaranteed. The presumption of innocence and the right to honor and privacy of the affected person shall be guaranteed at all times and under all circumstances.

Individuals who have been reported through the Channel may never be penalized based on a mere notification; in all cases, the veracity of the report must first be verified, and the individuals involved must be given the opportunity to provide an explanation regarding the reported situation.

In order to guarantee the affected person's right to a defense, they may be heard when the Organization so determines, and they will be informed of the possibility of appearing with legal counsel and of providing such evidence as they deem appropriate and relevant.

8. MANAGEMENT OF INFORMATION RECEIVED BY THE HEAD OF GLOBALIA'S INTERNAL REPORTING SYSTEM

Information may be reported to Globalia anonymously. Otherwise, the identity of the whistleblower will be kept confidential and will be known only to Globalia's RSII and the person delegated by the RSII.

Information will be communicated through the ethics channel available via the following means:

- ✓ External web platform: https://globalia.canaletico.es/ - accessible from the Globalia website
- ✓ Email: cumplimos@globalia.com

Any information received by Globalia through other channels regarding the subject matter of Law 2/2023 shall be forwarded to the ethics channel administered by the Head of Globalia's Internal Reporting System.

At the whistleblower's request, the report may also be submitted via an in-person meeting,

videoconference, or telephone call with the RSII or a designated representative from the Compliance Department, which must take place within a maximum of seven days.

Where applicable, the whistleblower will be notified that the communication will be recorded and informed of the processing of their data in accordance with the provisions of the GDPR and the LOPDPGDD.

When submitting the information, the whistleblower must provide an address, email address, or secure location for the purpose of receiving notifications, unless they expressly waive the right to receive any communication regarding actions taken by the RSII as a result of the information.

In the case of verbal communication, including that made during an in-person meeting, the RSII must document it in one of the following ways:

a) By recording the conversation in a secure, durable, and accessible format, or,

b) through a complete and accurate transcript of the conversation prepared by the staff responsible for handling it.

Without prejudice to the rights to which the informant is entitled under personal data protection regulations, the informant will be given the opportunity to review, correct, and sign off on the transcript of the message.

Once the information or communication has been submitted, it will be recorded in the information management system through the automatic assignment of an ID code and a tracking number. This information will be stored in a secure database with access restricted exclusively to duly authorized Globalia RSII personnel, where all received communications will be recorded with the following details:

a) Date of receipt

b) Tracking number

c) Type of communication/incident

d) Details of the communication

e) Date and time the incident occurred

f) Person or persons reporting the issue

g) Person to whom the incident is reported

h) Actions taken

i) Measures taken

j) Investigation (yes or no)

k) Conclusions

l) Closure date

Upon receipt of the information, within a period not exceeding 7 calendar days from such receipt, an acknowledgment of receipt will be sent to the whistleblower, unless the whistleblower has expressly waived the right to receive communications regarding the investigation or unless Globalia's RSII reasonably considers that acknowledging receipt of the information would compromise the protection of the whistleblower's identity.

Once the information has been recorded, the RSII will proceed to analyze its admissibility in accordance with the material and personal scope set forth in Articles 2 and 3 of Law 2/2023. The resolution of the investigation file may not exceed three months from the date of the acknowledgment of receipt of the communication ( ) or, if no acknowledgment of

receipt was sent to the whistleblower, three months from the expiration of the seven-day period following the communication, except in cases of special complexity in which the investigation may be extended for up to an additional three months.

Likewise, all stakeholders of the Organization have at their disposal regional, national, and European external channels, including the Independent Whistleblower Protection Authority (A.A.I.), in accordance with Law 2/2023. However, the internal reporting channel is established as the preferred means for reporting potential violations, ensuring effective and confidential handling.

9. TRAINING AND DISSEMINATION

The content of this policy will be included in the training materials linked to GLOBALIA's criminal risk prevention training plan, as well as in any additional dissemination activities determined from time to time.

This Policy, which forms part of Globalia's Compliance System, will be published on Globalia's corporate website and on the corporate intranet. It will also be sent to all employees of the companies listed and communicated, to the extent applicable, to third parties with whom Globalia does business.

In any case, the admission process and subsequent actions will be carried out in accordance with the information management procedure adopted for this purpose by Globalia.

10. DISCIPLINARY PROCEDURES

Failure to comply with the provisions of this policy may result in the imposition of disciplinary sanctions (including disciplinary dismissal) or in appropriate actions depending on the relationship the offending individual maintains with GLOBALIA.

11. APPROVAL AND PUBLICATION OF TH

The Board of Directors, as Globalia's highest governing body, is responsible for implementing the Internal Whistleblowing System and overseeing this Policy, which has been approved by Globalia's governing body.

This Policy will be reviewed, updated, approved, and disseminated periodically and whenever necessary to implement any modifications. Any modifications made will also be published on the Globalia website.

Once approved by Globalia's governing body, it will be implemented through a system management procedure and communication channels.

12. INTERPRETATION OF THIS POLICY

The provisions of this Policy constitute the minimum standards applicable to all companies in which Globalia Holding holds a majority stake, without prejudice to applicable law. The Principles and Guarantees are intended as interpretive guidelines. However, in the event of any conflict between this Policy and applicable law, the law shall always prevail.