**COLUMBUS VENTURE PARTNERS, MANAGEMENT COMPANY OF CLOSED-END INVESTMENT ENTITIES, S.A.U.'s**

# INTERNAL INFORMATION SYSTEM POLICY

**Date: November 13th, 2023**

## CONTENTS

## 1. OBJECT

Law 2/2023, of 20th February, regulating the protection of people who report regulatory infringements and the fight against corruption ("**Whistleblower Protection Law**"), which transposes into Spanish law Directive (EU) 2019/1937 of the European Parliament and of the Council of 23rd of October 2019, requires companies such as COLUMBUS VENTURE PARTNERS, S.G.E.I.C., S.A.U. ("**Columbus**" or the "**Company**" indistinctly) to have an Internal Information System ("**IIS**") under the terms provided.

The main objectives of the establishment of an IIS are to protect people who, in a labor or professional context, detect serious or very serious criminal or administrative violations and report them through the mechanisms regulated for this purpose, as well as to strengthen and promote the culture of information as a mechanism to prevent and detect irregular conduct.

The purpose of this Internal Information System Policy of Columbus (the "**Policy**") is to include the general principles that inspire the Columbus IIS, as well as other matters provided for in the aforementioned Whistleblower Protection Law, such as the channel enabled for the receipt of communications regarding breaches, the procedure to be followed for the processing of such communications, the person in charge of the IIS or the protection measures and guarantees established in favor of whistleblowers, which shall only apply to the communications referred to in the aforementioned Law.

## 2. SCOPE

This Policy applies to all of Columbus members who report, through the procedures provided, of:

- Actions or omissions that may constitute a serious or very serious criminal or administrative infraction. All serious criminal or administrative offenses that involve economic loss to the Tax Authorities and Social Security shall be understood to be included.

- Behaviors that may involve, by action or omission and by a member of Columbus, actions that have an significant implication on the professional relationship with Columbus of the person to whom the communication refers, related to the commission in a work or professional context of any law contrary to the rules, policies and internal procedures of Columbus.

- Any acts or omissions that may constitute any breach of European Union law[1].

We shall consider as Columbus members those who at any time are employees, directors, partners, interns, contractors, subcontractors, suppliers and other third parties. This Policy also applies to whistleblowers who, not being members of Columbus, have information about any of the actions or omissions referred to in this section in a work or professional context.

The aforementioned actions or omissions that may be reported under this Policy include those that may constitute a breach of Law 10/2010, of 28th of April, on the prevention of money laundering and terrorist financing ("**AML/FT**") and its implementing regulations, or the policies and procedures implemented to comply with them, committed within the Company as a subject bound by said Law, which may be reported by employees, managers or agents of Columbus in accordance with Article 26 bis of the aforementioned Law 10/2010.

## 3. INTERNAL INFORMATION SYSTEM (IIS)

Columbus' IIS referred to in this Policy is the preferred channel for reporting the actions or omissions referred to in paragraph 2 above.

The IIS mainly consists of the Communication Channel enabled for the reception of the communications foreseen in the scope of application of this Policy, the IIS Officer and the procedure to be followed for the processing of the referred communications, called "Procedure for the management and processing of the information received in the Internal Information System" and described in section 5 of this Policy (hereinafter, the "**IIS Procedure**").

### 3.1. General principles

Columbus IIS is managed internally and independently. The following general principles apply to it:

1. Accessibility: Allows everyone referred to in section 2 of this Policy to communicate information about the violations under that section, either in writing or orally, and may do so anonymously.

[1] This Policy shall apply to such acts or omissions provided that: (1st) Fall within the scope of the acts of the European Union listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23rd of October 2019 on the protection of persons reporting breaches of Union law, irrespective of their qualification in the internal legal order; (2nd) Affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union; or (3rd) affect the internal market, as referred to in Article 26(2) of the TFEU, including infringements of the European Union rules on competition and aid granted by the States, as well as infringements relating to the internal market in relation to acts that infringe the corporate tax rules or practices whose purpose is to obtain a tax advantage that distorts the object or purpose of the legislation applicable to corporate taxation.

2. Integration: The Internal Information Channel established in Columbus is integrated within the IIS.

3. Security, confidentiality and respect for data protection regulations: Columbus IIS is designed, established and managed securely, to guarantee the confidentiality of the identity of the whistleblower and any third party mentioned in the communication, and of the actions carried out in the management and processing of said communication, as well as the rights to privacy, intimacy, honor, defense and presumption of innocence of the persons involved in the investigation process started because of the receipt of a communication made through the IIS, and data protection, preventing access by unauthorized personnel.

4. Anonymity: The identity of the whistleblower, if known, as well as that of any third parties mentioned in the communication, besides that of the third parties stated in the privacy policy, may only be communicated to the judicial authority, the Public Prosecutor's Office or the competent Administrative Authority within the framework of a criminal, disciplinary or sanctioning investigation, after notifying the whistleblower or the third party concerned, provided that such circumstance does not compromise the investigation or the judicial proceeding in progress.

5. Diligence, agility and effectiveness: The actions aimed at verifying and clarifying the facts in the communications received must be carried out with the greatest possible diligence, agility and effectiveness, considering the complexity of the facts, in order to ensure that the Company is the first to be aware of the possible irregularity, and in any case, in accordance with the provisions of the IIS Procedure.

6. Proportionality, objectivity and respect for the guarantees of the intervening parties: The actions carried out within the framework of the IIS will be developed under criteria of proportionality and objectivity, with the utmost respect for the law in force, acknowledging the rights and observing all the guarantees provided for in the IIS Procedure for the intervening parties, being expressly prohibited any law constituting retaliation against the whistleblowers.

7. Information: The person affected by the communication may be informed of the acts attributed to them and to be heard at any time. Once informed, they may request the examination of the information and documentation in the file to which the processing of the communication has given rise, although the measures must be taken to ensure that no information is disclosed that would make it possible to know the identity of the whistleblower.

8. Good faith: It is a prerequisite for protecting the whistleblower that they act in good faith and with honest awareness that serious damaging events have occurred or may occur. This principle is opposed to actions such as the

transmission of false or misrepresented information, as well as information that has been obtained unlawfully.

9. Publicity: The information necessary for whistleblowers to make use of the Columbus Communication Channel is provided in a clear and easily accessible manner and is contained in this Policy, which can be consulted on the Columbus website at the following address: https://columbusvp.com/es/.

### 3.2. Internal Information Channel

The Columbus IIS integrates the Company's Internal Information Channel, which is the preferred channel for the communication of the conducts foreseen in section 2 of this Policy.

The Internal Information Channel allows:

a) To make communications under the conditions provided for in the Whistleblower Protection Act.

b) That, when making the communication, the whistleblower may provide an address, e-mail, or safe place to receive notifications.

c) The submission and subsequent processing of anonymous communications.

d) To inform those who communicate through it, in a clear and accessible manner, about the external information channels with the competent authorities and institutions.

e) The receipt of any other communications or information not included in the scope set forth in section 2 of this Policy, although such communications and their senders shall be outside the scope of application and protection afforded by this Policy.

Measures shall be taken to ensure the confidentiality of communications sent through channels other than those established or to personnel not responsible for their processing (who shall immediately forward them to the IIS Officer).

### 3.3. External information channels

Notwithstanding the preferential channel of the Internal Channel for the communication of breaches included in the Whistleblower Protection Law. Whistleblowers may also access the channels established by the Public Administrations for these purposes ("**External Channels**"), either directly or after prior communication through the Internal Channels.

Among the External Channels allowed for reporting non-compliance is that of the Executive Service of the Commission for the Prevention of Money Laundering and

Monetary Offenses ("**SEPBLAC**"). The members (and, if applicable, agents) of Columbus, as a subject bound by the AML/CFT regulations, who become aware of facts or situations that may constitute infringements contemplated in Law 10/2010 or its implementing regulations, may bring them to the attention of SEPBLAC. These communications shall be sent to SEPBLAC in writing and shall include all the documents and information on the facts reported that may justify the complaint. The communications will be confidential, and SEPBLAC shall not be able to disclose the identification data of the persons who have made them.

The Whistleblower Protection Law provides that any individual may report to the Independent Authority for the Protection of Whistleblowers, or to the corresponding regional authorities or bodies, the commission of any actions or omissions included in the scope of application of said Act, either directly or after communication through the corresponding Internal Channel.

## 4. THE INTERNAL INFORMATION SYSTEM OFFICER

The person responsible for the management of the Columbus Internal Information System, appointed by the administrative body, is the General Manager of the Company, a single person that assumes the function of supervising the Internal Information System.

The designation of the person in charge of the IIS Performance shall be notified to the Independent Authority for the Protection of the whistleblower or, where appropriate, to the competent authorities or bodies of the autonomous communities, within the scope of their respective competences.

The IIS Officer will diligently assume, and in the absence of conflict of interest, resolving the procedures started because of the information received through the established Internal Channel. They will ensure the proper application of the IIS Procedure. In the event of a conflict of interest, the management body shall appoint the person in charge of such resolution, who in the exercise of this function shall be subject to the same obligations and principles as the IIS Officer.

The IIS Officer shall keep a record book of the information received and of the investigation files to which they have given rise, guaranteeing the confidentiality of the information.

The IIS Officer has the material and personal resources necessary for the proper performance of their duties, which they will conduct with full respect for the general principles of IIS, in an independent manner regarding the rest of the Company's bodies, with neutrality, honesty and objectivity towards all persons involved.

## 5. IIS PROCEDURE

The IIS Procedure regulates the management and processing of communications received through the Internal Information Channel that is integrated in the Columbus IIS.

### 5.1. Internal Information Channel Instructor

The Instructor of the Internal Information Channel is the Head of the Columbus Legal Department, and shall be the person in charge of managing the proper functioning of the aforementioned Channel in the instruction phase unless, as provided for in section 5.4, there is a conflict of interest or other obstacle, in such case the IIS Officer shall appoint another instructor. They shall carry out their work under the premises of independence, neutrality and impartiality, with honesty and objectivity towards all persons involved. They shall ensure that the entire procedure is carried out under the rules and principles set forth in this Policy.

The main responsibilities of the Instructor of the Internal Information Channel are:

i. Receiving communications made through the Internal Information Channel;

ii. Analyzing the communications received and decide on their admissibility;

iii. Investigating the corresponding files, under the rules and principles set forth in this Policy; and to submit the corresponding resolution proposal to the IIS Officer or the body in charge of resolving the matter;

iv. Preparing an annual report on the activity carried out (communications received, processed, rejected, etc.), which shall be submitted to the Board of Directors of the Company.

### 5.2. Sending of communications through the Internal Information Channel

Communications to the Internal Information Channel shall be made through any of the following channels, which may be made anonymously, without identification of the sender:

i. Using the form available on Columbus' website, https://forms.office.com/e/vvWSTr9WBa. For Columbus members it will also be available at Columbus' Microsoft 365 intranet.

ii. By sending a written communication to the attention of the Columbus Internal Information Channel Instructor, to the following postal address: Columbus, calle Jose Abascal 58, 7º Dcha., 28003, Madrid.

At the whistleblower's request made through any of the identified channels, the communication may also be presented through a face-to-face meeting within seven days. Verbal communications through a face-to-face meeting must be documented in one of the following ways, subject to the whistleblower's consent:

a. By a recording of the conversation in a secure, durable, and accessible format; or

b. Through a complete and accurate transcription of the conversation made by the staff responsible for handling it.

Notwithstanding your rights under data protection regulations, the whistleblower shall be given the opportunity to verify, rectify and agree to the transcription of the conversation by signing it.

When submitting the communication, the whistleblower may inform of an address, e-mail or safe place to receive notifications. They may also expressly waive the receipt of any communication of the actions carried out by the Instructor of the Internal Information Channel because of the information.

Any communication that may be included in the Internal Information Channel received by another Columbus manager shall be included in the aforementioned Channel when it reaches the Instructor's knowledge, guaranteeing its confidentiality.

### 5.3. Acknowledgement of receipt of communication and registration

Once the communication has been received in any of the means provided for in the previous section, Columbus' Internal Information Channel Instructor shall issue an acknowledgement of receipt to the whistleblower within seven calendar days from the receipt, unless this could jeopardize the confidentiality of the communication, it is not possible due to the anonymous nature of the communication, or the whistleblower has expressly waived receipt of communications relating to the investigation.

Within the period of seven calendar days, the Instructor of the Columbus Internal Information Channel will incorporate the communication into the IIS' Information Record Book, giving it an entry number and showing a date of receipt, and will inform the IIS Officer of its receipt and registration.

### 5.4. Admissibility of the communication

Once the communication has been registered, the Instructor of the Internal Information Channel must check whether it falls within the scope of the application set forth in section 2 of this Policy.

Once this preliminary analysis has been carried out, the Instructor of the Internal Information Channel shall decide, within a period that may not exceed ten calendar days from the date of entry of the communication in the Information Record Book:

a. The communication is inadmissible, which it may do if any of the following events occur:

   i. When the facts reported lack any credibility.

   ii. When the facts reported do not constitute an infringement of the legal system included in the scope of the application of the Columbus' IIS Policy.

   iii. When the communication is unfounded or there are, in the Instructor's opinion of the Internal Information Channel, reasonable indications of having been obtained through the commission of an offence.

   iv. When the communication does not contain new and significant information on infringements in comparison with a previous communication, in respect of which the corresponding proceedings have been concluded, unless there are new factual or legal circumstances that justify a different follow-up. In such cases, the Instructor of the Internal Information Channel shall notify the resolution in a reasoned manner.

   The whistleblower shall be notified of the rejection within five calendar days of the decision, stating the reasons, unless the communication was anonymous, or the whistleblower has waived the right to receive communications.

b. Admitting the communication for processing, which shall be communicated to the whistleblower within the following five calendar days, unless the communication is anonymous, or the whistleblower has waived the right to receive communications.

   If the communication has been admitted, even if it does not fall within the scope of application of the Whistleblower Protection Law, the protection measures and other matters provided for in said Law shall not apply.

c. Immediately forward to the Public Prosecutor's Office or the European Public Prosecutor's Office, the information, when the facts could be indicative of a criminal offence.

d. Forward the communication to the authority, entity or organism considered competent for its processing.

There are two circumstances that may result in the Instructor of the Internal Information Channel not ruling on the admissibility of the communication within ten calendar days:

i. If the preliminary analysis of the communication leads to the conclusion that there is any circumstance related to it that may involve a conflict of interest for the Instructor of the Internal Information Channel or that it affects or may affect their neutrality or independence of action, in such case they must inform the IIS Officer within three calendar days following the date of registration of the communication. In this case, it will be the responsibility of the IIS Officer to decide on the admission of the communication for processing and the appointment of an Instructor for the procedure, who must continue with the processing of the file under the established procedure, meeting the maximum period for resolution.

ii. If after this preliminary analysis, the Instructor of the Internal Information Channel has doubts about the admissibility of the communication. In this case, and provided that it is possible to have a way to contact the whistleblower, within three calendar days following the date of registration of the communication, they shall request the whistleblower to clarify or complete their communication within three calendar days following the request, providing as much documentation and data as may be necessary.

    In such cases, the Instructor of the Internal Information Channel must decide on the admissibility of the communication within seven calendar days from the end of the period of three calendar days granted to the whistleblower to complement their communication (whether they have or not provided additional information).

## 5.5. Instruction

Once the communication has been admitted for processing, the Instructor of the Internal Information Channel will conduct the corresponding contradictory proceedings, carrying out the necessary investigations and prosecution respecting, at all times, Columbus IIS' general principles.

The Instructing Officer shall verify the truthfulness and accuracy of the information in the communication and, particularly, of the reported behavior, regarding the rights of the affected parties, especially the presumption of innocence and the honor of the people involved. For these purposes, they shall give a hearing to all those affected and witnesses and shall carry out as many proceedings as they deem necessary.

All of Columbus members must loyally cooperate in the investigation, with the intervention of witnesses and affected parties being strictly confidential.

During the investigation, unless they have been previously informed, all affected parties shall be informed about the processing of their personal data. They shall also be informed of their need to comply with any other duty required by the legislation on the protection of personal data.

Initially, the investigation shall not be extended beyond 30 calendar days from the admission of the communication, unless there are justified circumstances, based on the complexity or the number of proceedings to be carried out, which justify the extension of said period.

The person affected by the information shall be notified, as well as of the facts related briefly. They shall be informed of their right to present written allegations and of the processing of their personal data, unless they have been previously informed. However, this information may be provided during the hearing if it is considered that its prior provision could facilitate the concealment, destruction, or alteration of the evidence.

In no case shall the identity of the whistleblower be communicated to the subjects concerned, nor shall they be granted access to the communication. Only notice of the communication, with a brief account of the facts, shall be given to the person under investigation.

Notwithstanding the right to submit written allegations, and whenever possible, the investigation shall include an interview with the person concerned in which, always with absolute respect for the presumption of innocence, they shall be invited to explain their version of the facts and to provide the means of proof that they consider adequate and relevant. To guarantee the affected person's right of defense, they shall have access to the file without disclosing information that could identify the whistleblower, and they may be heard at any time, and shall be advised of the possibility of having the assistance of a lawyer.

### 5.6. Resolution

Once all the proceedings have concluded, within 15 calendar days, the Instructor shall submit it, together with a resolution proposal, to the IIS Officer. Said Proposal will contain at least:

i. A statement of the facts reported together with the identification code of the communication and the date of registration.

ii. The classification of the communication for the purpose of knowing its priority or not in its processing.

iii. The actions carried out in order to verify the authenticity of the facts.

iv. The conclusions reached in the investigation and the assessment of the proceedings and the evidence supporting them.

Within ten calendar days from receipt of the proposed resolution, the IIS Officer must issue a resolution on the case, in which they may agree:

i. The archiving of the file because the reported infringements are not found to have occurred, and the whistleblower shall be notified (unless this is not possible because of the anonymous nature of the communication or because they have waived the right to receive communications related to the investigation) and, if applicable, the person concerned. In such cases, the whistleblower shall be entitled to the protection provided for in this Policy, unless, because of the proceedings carried out in the investigation phase, it is concluded that the information, in view of the information gathered, should have been inadmissible.

ii. That the concurrence of some infraction is appreciated, with the adoption of the corresponding sanction.

In the case of professionals with an employment relationship, the sanction will be applicable in accordance with the corresponding labor regulations. The resolution shall be transferred to the person responsible for the management of the Human Resources of Columbus for the application of the appropriate disciplinary measures and, where appropriate, to the Administrative Body for the purpose of initiating the corresponding administrative or legal actions that may apply. If the file affects a Senior Manager of the Company, the Board of Directors shall be in charge of the resolution.

For the rest of the systems or relationships that may exist, as regards to penalties, the provisions agreed in each case in the corresponding contractual document in which such a relationship has materialized shall apply.

Whatever the decision, it shall be communicated to the whistleblower, unless the whistleblower has waived, or the communication is anonymous.

The term to complete the proceedings and respond to the whistleblower, when applicable, may not exceed three months from the receipt of the communication, except in cases of particular complexity that require an extension of the term, in which case, this may be extended up to a maximum of three additional months.

## 6. PROTECTION OF PERSONAL DATA

### 6.1. Information on data protection

Under the regulations on personal data protection, all interested parties are informed that the data collected through the IIS will be processed by Columbus Venture Partners, SGEIC, S.A.U. acting as data controller.

The purpose of the data processing is only the one described in section 5 of this Policy. The controller will process the personal data provided by the whistleblower in compliance with a legal obligation in compliance with the whistleblower protection law.

Users of the IIS Procedure may, under the applicable legislation, in each case, exercise their rights of access, rectification, suppression, opposition and limitation of processing of their personal data by writing to the registered office of Columbus Venture Partners, SGEIC, S.A.U. indicating the specific right they wish to exercise or via the e-mail address inversor@columbusvp.com.

Columbus has also designated a Data Protection Delegate to whom IIS users may address their questions, recommendations, or complaints about the processing of their personal data. They may be contacted at the following e-mail address: fmoya@businessadapter.es.

In particular, the data we will process may include the following categories: identification data, data concerning your personal characteristics and social circumstances, contact data, academic and professional data, economic, financial and insurance data and/or specially protected data. The personal data processed may have been provided either by the data subject or by third parties.

For further information on data protection, please see the Privacy Policy at the following link: https://columbusvp.com.

### 6.2. Obligations of the IIS Officer in data protection matters

Among other obligations, the IIS Officer will ensure the respect of:

- The principle of transparency, providing the required information on personal data protection.

Particularly, the whistleblower shall be informed that their identity will in all cases be kept confidential and that it shall not be communicated to the person involved or to third parties except, where appropriate, under the Whistleblower Protection Law, to the Judicial Authority, the Public Prosecutor's Office or the competent administrative authority in the framework of a criminal, disciplinary or sanctioning investigation.

- The principle of minimization, only the strictly necessary and essential data shall be collected for the proper functioning of the IIS. In the event of collecting more data than is strictly necessary for the processing and investigation of the actions or omissions described in section 3 of this Policy, shall be deleted as soon as possible.

- The principle of purpose limitation. The personal data collected through the IIS shall not be processed for any purpose other than the management of the communication and processing of the file.

- The principle of limitation of the storage period, whereby personal data must be processed only for the essential time.

  Once three months have elapsed since the receipt of the communication without having started the investigation proceedings, the personal data must be deleted, unless the purpose of the conservation is to leave evidence of the operation of the system.

- Communications that have not been acted upon may only be retained in anonymized form, without the blocking obligation provided for in the personal data protection regulations applying.

- The principle of accuracy, having to eliminate all personal data included in the information communicated that is not truthful. All this, unless the lack of truthfulness may constitute a criminal offence, in such case the information shall be stored for as long as the legal proceedings take place.

- The principle of integrity and confidentiality, guaranteeing the confidentiality of the whistleblower and third parties as stated in this Policy. All technical and organizational security measures needed to protect the information against any unauthorized processing and against its accidental loss, destruction or damage shall be established.

### 6.3. Limiting access to IIS' personal data

Only the IIS Officer, the Instructor and the person who directly manages it, the third-party service providers who are considered data processors and the Data Protection Officer may access the personal data in the IIS.

To comply with the purposes described above, the Data Controller may provide access to the personal data contained in the IIS:

- To the person in charge of Human Resources management, who will have access to personal data solely and exclusively when disciplinary measures may be taken against an employee.

- To the person in charge of the legal services, who will have access solely and exclusively to the personal data if legal measures should be taken in relation to the facts reported in the communication.

- To other people, only when necessary for the adoption of corrective measures in the Company or the processing of sanctioning or criminal proceedings.

In the event the facts that are the subject of the information could indicate a crime, the Public Prosecutor's Office or the European Public Prosecutor's Office must be informed.

## 7. PROTECTION MEASURES AND GUARANTEES

### 7.1. Scope of application

The protection measures and guarantees referred to in this section shall be mandatory for the Company if the Whistleblower Protection Law applies.

The whistleblowers must act in good faith, observe the criteria of truthfulness and proportionality in their communications and refer only to facts that have a bearing on the Company. False communications or information may cause the imposition of sanctions.

People who report or disclose breaches within the material scope of this Policy shall be entitled to the protection measures set forth in this Policy provided that the following circumstances apply:

a) Have reasonable grounds to believe that the information referred to is true at the time of communication or disclosure, even if they do not provide conclusive evidence, and that such information falls within the scope of this Policy.

b) The communication or disclosure has been made according to the requirements of this Policy.

This protection extends to any natural person who, within the framework of the organization in which the whistleblower provides services, assists them in the communication process, or is related to them, as a representative of the employees, co-worker or family member, and to any legal person for whom the whistleblower works or with whom they maintain another type of relationship within the framework

of an employment context or in which they hold a participation that allows them to have capacity and influence over it.

The protection measures provided for in this Policy are understood to be, notwithstanding those established in the specific regulations that may apply and shall not exclude the application of the rules relating to criminal proceedings, including investigation measures.

In particular, the Company shall take measures to ensure that employees, officers, or agents who report violations committed within the scope of the AML/FT Law 10/2010 within Columbus are protected against retaliation, discrimination and any other type of unfair treatment.

Any person who communicates or discloses any of the information in this Policy is expressly excluded from the protection provided for in this Policy:

a) Information in communications that has been rejected by any internal information channel or for any of the following reasons:

   - When the facts reported lack any credibility.
   - When the facts reported do not constitute a violation of the legal system included in the scope of application of this Policy.
   - When the communication is manifestly unfounded or there are reasonable grounds to believe that it was obtained through the commission of a crime.
   - When the communication does not contain significant new information on infringements in comparison with a previous communication in respect of which the corresponding procedures have been concluded, unless there are new factual or legal circumstances that justify a different follow-up.

b) Information related to complaints about interpersonal conflicts or that affect only the whistleblower and the persons to whom the communication or disclosure refers.

c) Information that is already fully available to the public or that constitutes mere hearsay.

d) Information relating to infringements in the processing of contracting procedures that contain classified information or that have been declared secret or reserved, or those whose execution must be accompanied by special security measures under the legislation in force, or in which the protection of essential interests for the security of the State so requires.

### 7.2. Prohibition of retaliation

Under the Whistleblower Protection Act, acts constituting retaliation, including threats of retaliation and attempted retaliation against individuals who make a disclosure under this Policy are expressly prohibited.

Retaliation is understood to be any acts or omissions that are prohibited by law, or that, directly or indirectly, involve unfavorable treatment that places the peolpe who suffer them at a particular disadvantage compared to another in the work or professional context due to their status as whistleblowers.

For example, the following are considered retaliation:

- The suspension of the employment contract, dismissal or termination of the employment or statutory relationship; the imposition of any disciplinary measure; the demotion or denial of promotions and any other substantial modification of working conditions; and the failure to convert a temporary employment contract into a permanent one, if the person making the communication had legitimate expectations in this regard.

- Damages, including those of a reputational nature, or economic losses, coercion, intimidation, harassment or ostracism.

- Negative evaluation or references regarding job or professional performance.

- The inclusion in blacklists or the dissemination of information in a certain sectorial area, which hinder or prevent the person from accessing employment or contracting works or services.

- The denial or cancellation of a license or permit.

- Denial of training.

Columbus will take measures to ensure that employees, officers or agents who report AML/CFT violations are protected against retaliation, discrimination and any other unfair treatment for that reason.

### 7.3. Support and protection measures

The Whistleblower Protection Law also provides for a series of support and protection measures for whistleblowers who report the actions or omissions listed in Article 2 and reproduced in section 2 of this Policy. These measures, which, when applicable, would be provided by the Independent Whistleblower Protection Authority or other competent authority or body, notwithstanding the specific support and assistance measures that may be articulated by the Company, are:

***Support measures***

Individuals who report or disclose breaches within the scope of this Policy through the procedures set forth in it will be eligible for the following support measures:

a) Complete, independent, and free information and advice on procedures and remedies, protection against retaliation and the rights of the affected person.

b) Effective assistance from competent authorities before any relevant authority involved in their protection from retaliation, including certification that they are eligible for protection under the Whistleblower Protection Act.

c) Legal assistance in criminal proceedings and cross-border civil proceedings under Community regulations.

d) Financial and psychological support, exceptionally, if so decided by the Independent Whistleblower Protection Authority, following an assessment of the circumstances arising from the submission of the communication.

In particular, and as stated in Article 65.5 of the AML/FT Law 10/2010, people exposed to threats, hostile actions or adverse employment measures for reporting through the Columbus Internal Reporting Channel or to SEPBLAC (External Channel) on activities related to money laundering or terrorist financing may file a complaint with the Independent Whistleblower Protection Authority, under the terms set forth in the Whistleblower Protection Law.

***Protective measures***

As established in the Whistleblower Protection Law:

a. The whistleblower shall not be deemed to have violated any disclosure restrictions and, therefore, shall not incur any liability of any kind in connection with such disclosure, provided that the whistleblower had reasonable grounds to believe that the disclosure was necessary to disclose a breach as defined in the Whistleblower Protection Act. The measure shall not affect criminal liabilities.

   The preceding paragraph extend to the communication of information made by the workers' representatives, even if they are subject to legal obligations of confidentiality or not to disclose confidential information. This is notwithstanding the specific rules of protection applicable under labor legislation.

b. The whistleblower shall not incur liability regarding the acquisition of or access to the information that is reported, provided that such acquisition or access does not constitute a crime. Any other potential whistleblower liability arising from acts or omissions that are unrelated to the communication or that are

not necessary to disclose a violation under this Policy will be enforceable under applicable law.

c. In proceedings before a court or other authority concerning prejudice suffered by whistleblowers, once the whistleblower has demonstrated that they have made a communication and suffered prejudice, it shall be presumed that the prejudice occurred in retaliation for reporting. In such cases, it shall be for the person who has taken the harmful measure to prove that the measure was based on duly justified reasons not linked to the communication.

d. In legal proceedings, including those relating to defamation, copyright infringement, breach of secrecy, violation of data protection regulations, disclosure of trade secrets, or claims for damages based on labor or statutory law, the reporting person and those to whom whistleblower protection is legally extended shall not incur liability of any kind as a result of communications protected by the Whistleblower Protection Act. Such individuals shall be entitled to plead in their own defense and in the context of such legal proceedings that they have communicated, if they had reasonable grounds to believe that the communication was necessary to disclose a violation under the aforementioned Act.

e. During the processing of the file, those affected by the communication shall have the right to the presumption of innocence and the right of defense. Likewise, restricted access to the file shall be allowed, their identity shall be preserved and the confidentiality of the facts and data of the procedure shall be guaranteed.

## 8. INFORMATION RECORD BOOK

The IIS will keep a record of the information received and the internal investigations to which they have given rise, ensuring due confidentiality and compliance with personal data protection regulations.

The following data relating to such information shall be entered in the record:

i. Date of receipt
ii. Actions carried out
iii. Actions taken
iv. Closing date

The record is not publicly accessible 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 guardianship of such authority, may its contents be accessed in whole or in part.

## 9. PROTECTION OF PERSONAL DATA

The processing of personal data carried out within the framework of the IIS shall be carried out in full compliance with the general principles and obligations established in the personal data protection regulations and in the Whistleblower Protection Law.

The data collected in the IIS will be processed by Columbus acting as data controller.