Policy on the Internal Information System.

Aim	To establish the general principles of the Internal Information System in accordance with Law 2/2023, of 20 February, on the protection of persons who report breaches of regulations and infringements relating to the fight against corruption.
Scope	MONTEPINO LOGISTICA SOCIMI, S.A. (hereinafter, "**MONTEPINO LOGISTICA**" or the "**Company**"), its affiliates companies and Valfondo Gestión, S.L. (hereinafter, the "**Management Company**").
Responsible parties	The Responsible of the Internal Information System or Ethical Channel

Versions

Version	Date	Content of the modification
0.0	12/12/2023	First draft and approval

1. INTRODUCTION

Law 2/2023, of 20 February, on the protection of persons who report on regulatory and anticorruption breaches ("**Law 2/2023 on the Protection of Informants**") aims, among other things, to adequately protect from possible retaliation any natural persons who have obtained information about serious or very serious criminal offences or administrative infringements in a work or professional setting that affect the general interest and have reported them using the mechanisms regulated in it.

In this context, the Board of Directors of MONTEPINO LOGÍSTICA has approved this Policy on the Internal Information System, to which its affiliates companies and the Management Company (all of them hereinafter also "the Companies" or "MONTEPINO", as this is the trade name under which the corporate group operates); thus adapting the Ethical Channel implemented in 2019 to the requirements of Law 2/2023 on the Protection of Informants and providing MONTEPINO with an Internal Information System with all guarantees for the protection of informants.

2. GENERAL PRINCIPLES

The structure and operation of the Internal Information System complies with the legal requirements, principles and guarantees of protection set forth in the following legislation:

- Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights (Data Protection Law); and Organic Law 7/2021, of 26 May, on the Protection of Personal Data processed for the purposes of the prevention, identification,

investigation and prosecution of criminal offences and the enforcement of criminal penalties.

- Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law; and Law 2/2023, of 20 February, on the protection of persons who report breaches of the law and infringements relating to the fight against corruption.
- Art. 31 bis of the Criminal Code; and Circular 1/2016, of the Public Prosecutor's Office, which affects reports and communications on the prevention of money laundering.

This Policy on the Internal Information System is based on the following general principles and guarantees of the Internal Information System:

a) **Transparency and accessibility**: The information on the Internal Information System shall be available and easily accessible on the Company website with the necessary information to use it.

b) **Confidentiality and anonymity**: The anonymity of the information to be communicated shall be guaranteed at all times, and the confidentiality of all the information collected and processed in the management of the Internal Information System shall be treated in strict confidentiality, especially the informant's identity and that of any third parties mentioned in the communication, as well as any actions carried out in connection with its management and processing; and access by unauthorised personnel will not be permitted.

Furthermore, it is hereby stated for the record that the right of access granted by the personal data legislation shall be restricted to the informant's or complainant 's personal data, and the reported person will under no circumstances have access to the informant's or complainant's identification details.

c) **Autonomy and independence**: The Responsible of the Information System shall be independent and autonomous in respect of all the other bodies in the organisation and will therefore be fully impartial and unaffected by any conflicts of interest when handling communications, ensuring objectivity at all stages of the process. If the Responsible of the Internal Information System has an actual or potential conflict of interest, the necessary mechanisms to ensure that they do not find out the complainant's identity under any circumstances and that they are not involved in the handling of the communication or report shall be put in place.

d) **Prohibition on retaliation**: All retaliatory action against any persons who submit a communication as provided in the Policy, including retaliation threats and attempts, is expressly forbidden. To that end, the necessary mechanisms and procedures to protect the indemnity of the informants against possible retaliation shall be put in place, with the possibility of using the protection measures set forth in Law 2/2023 on the Protection of

Informants, provided the circumstances specified therein apply.

e) **Reports made in bad faith**: All information provided must be true, complete, and provided in good faith, and the informants should avoid any confusing, false or illegally obtained information. On the other hand, disciplinary or other measures shall be adopted as may be deemed appropriate in each case against any persons who report acts or omissions knowing them to be false or with clear disregard for the truth or for the sole purpose of causing harm to the reported person.

3. SCOPE

3.1 Subjective scope

This Policy shall apply to shareholders and/or partners, members of the governing bodies, executives, heads of areas or departments and middle management and to all staff at MONTEPINO, regardless of the type or duration of the contract under which they are working, as well as to customers, suppliers, service providers, collaborating parties and other stakeholders with which MONTEPINO interacts in connection with its activities.

In addition, the Policy shall also apply to informants who publicly report or reveal information on breaches that has come to their knowledge in the context of a past employment or statutory relationship, volunteers, interns, trainees (paid or otherwise), as well as persons whose employment relationship has yet to begin, if the information about the breach came to their knowledge during the recruitment process or pre-contractual negotiations.

3.2 Objective scope

This Policy shall apply to all natural persons who report any act or omission capable of constituting:

- A breach of EU law, provided it falls within the scope of the EU set forth in the Annex to Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 and it affects the EU's financial interests or has a bearing on the internal market.

- Serious or very serious criminal offences or administrative infringements falling within the scope of Spanish law. All serious or very serious criminal offences or administrative infringements that may harm the Spanish Public Treasury and Social Security System, as well as labour law infringements relating to Occupational Health and Safety, without prejudice to their specific legislation, shall also be deemed to be included.

- Any other infringements of the Code of Ethics or any other internal policies, protocols

and procedures approved by MONTEPINO.

- Any conduct that may be deemed to give rise to an ethical dilemma or that may reveal significant exposure to risk or pose a risk to MONTEPINO's reputation.

4. RESPONSIBLE OF THE INTERNAL INFORMATION SYSTEM

The Board of Directors of MONTEPINO LOGÍSTICA has appointed the Compliance Officer as Responsible of the Internal Information System ("the Responsible of the System").

The Responsible of the System must carry out their duties independently and autonomously from the Company's other management and steering bodies. They may not receive instructions of any kind on how to carry them out, and they must have the necessary personal and material resources to properly carry out their duties.

The Responsible of the System shall have the necessary authority and standing to obtain information from any department at any time and freely access any records and documents they may need to carry out their duties.

The Responsible of the System must also have suitable technical and organisational measures in place to preserve the identity and ensure the confidentiality of the information on the persons concerned and any third parties mentioned in the information provided, particularly the informant's identity if it has been provided.

5. DATA PROTECTION

The processing of personal data arising from the application of the Internal Information System shall be governed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016; Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights; Organic Law 7/2021, of 26 May, on the Protection of Personal Data processed for the purposes of the prevention, identification, investigation and prosecution of criminal offences and the enforcement of criminal penalties; and Law 2/2023 on the Protection of Informants.

At MONTEPINO, each company's management body shall respectively be the Controller for the personal data processed in connection with the management of the Internal Information System because of both the information reported and the related investigation that may be carried out in response to it.

The personal data processed in connection with the management of the Internal Information System shall be limited to the data that is either voluntarily provided by the informant or

complainant (for non-anonymous information) or strictly necessary to process the communications or reports received and investigate the facts where appropriate.

This data shall be processed for the sole purpose of processing, investigating and/or making a decision on the communications or reports concerned and to make any communications and notifications that may be appropriate in each case. Information obtained through the Internal Information System may not be used for any other purpose.

The legal grounds forming the legitimate basis for the processing of the personal data in connection with the management of the Internal Information System are the fulfilment of a legal obligation as provided in Law 2/2023, of 20 February, on the protection of persons who report breaches of regulations and infringements relating to the fight against corruption and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights.

The personal data held in the Internal Information System may only be accessed by persons who are contractually bound by the duty of secrecy and confidentiality, and more specifically by:

- The Governing Body;
- The Responsible of the Internal Reporting System;
- The Head of the Human Resources department, only when there is a possibility of disciplinary measures being adopted against an employee;
- The Head of the Legal and Compliance department, if legal measures are to be adopted in relation to the facts reported in the communication;
- The Data Protection Officer;
- Where applicable, the organisation to which the management of the Internal Information System has been outsourced.

The information processed in connection with the investigation into a report may be disclosed to external legal advisers and to judicial bodies and the state security and law enforcement forces or administrative authority to which the outcome of the investigation may be referred, whenever necessary in order to adopt disciplinary measures or conduct any court proceedings that may be appropriate.

Under no circumstances may any personal data that is not necessary to investigate or ascertain the actions or omissions capable of constituting an offence or infringement be processed, and any such data shall be immediately deleted.

The personal data processed in connection with the management of the Internal Information System shall be retained in the Internal Information System only for as long as absolutely necessary to decide whether to start an investigation into the reported facts and, where

applicable, during the investigation and resolution of reports, and never for more than 3 months from the date of the original communication or report.

Notwithstanding the foregoing, the personal data may be processed for longer than this outside the Internal Information System if the outcome of the investigation process started by reason of the facts in the communication or report makes it necessary to take appropriate legal action and/or may give rise to court proceedings, in which case it shall be retained until a final court ruling has been issued.

In any event, if no investigation is started within three months from the date of receipt of the communication, the personal data must be deleted or blocked outside the Internal Information System if it is retained in this way as evidence of the Ethical Channel's operation or to audit or improve it.

The personal data of the communications in relation to which no action has been taken or that have not been admitted for processing may only be recorded in anonymised form. This means that no personal data will be associated with them and the obligation to block the data as provided in Article 32 of Organic Law 3/2018, of 5 December, will not apply.

The personal data, if any, provided through the Internal Information System shall in no event be the subject of an international transfer of data.

The Internal Information System must have appropriate technical and organisational measures in place to ensure the confidentiality of the data relating to the persons concerned and any third parties mentioned in the communication, particularly the informant's identity if they have disclosed it.

However, the informant's identity may only be disclosed to the competent administrative or judicial authority or the Public Prosecutor's Office in connection with a criminal, disciplinary or sanction-related investigation.

6. SANCTIONS

The Internal Information System shall be governed by the provisions on sanctions set forth in Law 2/2023 on the Protection of Informants as may be necessary to effectively address any retaliatory actions against informants, as well as infringements in the establishment of communication channels.

Acts or omissions of the types described in Article 62 of Law 2/2023 on the Protection of Informants shall be deemed to constitute infringements and shall be subject to the sanctions set forth in Article 65 of that Law.

Authority to issue sanctions pertains to the Independent Informants Protection Authority ("AAI") and the competent bodies of the autonomous regions and is without prejudice to the internal disciplinary powers of each organisation's own competent bodies.