Complaints management Procedure

Purpose	To lay down the rules on the management and operation of the Internal Information System or Ethical Channel, establishing the legal status of informant and reported person and the duties and responsibilities of the Responsible of the Internal Information System, its management and the report handling procedure.
Scope	MONTEPINO LOGISTICA SOCIMI, SA (hereinafter, "MONTEPINO LOGISTICA" or the "Company"), its affiliates companies and Valfondo Gestión, S.L. (hereinafter, the "Management Company").
Responsible parties	The Board of Directors and the Responsible of the Internal Information System

Versions

Version	Date	Content of the modification
0.0	13/12/2019	First draft.
0.1	25/11/2019	Approval by the Compliance Officer.
0.2	13/12/2020	Changes to the Scope, specifically including Montepino's customers, partners and stakeholders in general. Changes to the legitimate basis for processing data in connection with the Ethical Channel, introducing the public interest in having such a channel.
0.3	23/9/2021	Adaptation to the new corporate structure.
0.4	15/5/2023	Adaptation of the Procedure to the new Company name.
0.5	12/12/2023	Adaptation to Law 2/2023, of 20 February, on the protection of persons who report on regulatory and anticorruption breaches; Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights (the 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.

Complaints management Procedure

1. PURPOSE

This Procedure seeks to lay down the rules on the operation of the Internal Information System (hereinafter also referred to as the "Ethical Channel") of MONTEPINO LOGISTICA SOCIMI, S.A. (hereinafter, "MONTEPINO LOGISTICA" or the "Company"), its affiliates companies and Valfondo Gestión, S.L. (the Management Company) (all of them hereinafter also "the Companies" or "**MONTEPINO**", as this is the trade name under which the corporate group operates); and to establish the legal status of the informant and the reported person, the duties and responsibilities of the Responsible of the Internal Information System as the body in charge of managing it and the handling procedure for reports or communications.

The structure and operation of **MONTEPINO**'s Ethical Channel complies with the legal requirements and protection guarantees set forth in the following legislation:

- Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights (the 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 (Código Penal); and Circular 1/2016, of the Public Prosecutor's Office (*Fiscalía General del Estado*), which affects reports and communications on the prevention of money laundering.

2. SCOPE

2.1 Subjective scope

MONTEPINO's Ethical Channel is made available to its members and any other interested parties with which it interacts in connection with its activities (partners, customers, suppliers, public authorities, institutions, etc.) so that they can report or provide information if they suspect or have actual knowledge of any act or omission falling under the objective scope that has been, is being, or is going to be committed by a member of any of the Companies pursuant to their duties.

The following are considered members of **MONTEPINO** for this purpose:

- Its shareholders;

- The members of its management body;
- Its directors; heads of area or department and middle management; and
- In general, all personnel working for and on behalf of any **MONTEPINO** regardless of the mode or duration of the contract under which they are working.

Notwithstanding the foregoing, if the Responsible of the Internal Information System suspects or has actual knowledge of any act or omission of the types included in the objective scope, they may initiate an investigation ex officio as provided in this Procedure.

2.2 Objective scope

The following may be reported through **MONTEPINO**'s Ethical Channel:

- 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;

- Any act or omission capable of constituting a serious or very serious criminal offence or administrative infringement, specifically including any that may result in financial loss for the Spanish Public Treasury and the social security system, as well as labour law infringements relating to Occupational Health and Safety, without prejudice to their specific legislation;

- Any conduct in breach of **MONTEPINO**'s internal regulations or the values, guidelines for action or rules of conduct envisaged in **MONTEPINO**'s Code of Ethics;

- 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.

It is hereby expressly stated for the record that the EthicalChannel is not intended to be used to submit questions, queries, suggestions, claims or complaints relating to the performance of work or to report any conduct not included in the objective scope described above.

2.3 Reporting obligation

Any person belonging to **MONTEPINO** who suspects or has actual knowledge of any act or omission falling under the objective scope must report it on the Ethical Channel immediately.

In addition, the Ethical Channel shall be available for use by third parties not belonging to **MONTEPINO** in accordance with the principles of transparency and confidentiality on which this Procedure is based.

3. DISSEMINATION AND COMMUNICATION

This Procedure for the Management of the Internal Information System is made available to potential informants and reported parties, i.e. the members of **MONTEPINO** and other interested parties, and shall remain available to potential informants and reported persons at all times on **MONTEPINO**'s corporate website.

As an alternative to **MONTEPINO**'s Ethical Channel, and without being the preferred reporting method, reports may be made through external reporting channels to the competent administrative authorities and to the European Union's institutions, bodies or agencies where appropriate.

4. CONTENT OF REPORTS

Reports made through **MONTEPINO**'s Ethical Channel must contain at least a clear and detailed description of the reported facts (such as the time and place of the event, any possible witnesses and a factual account).

Although it is not required, we recommend that you identify the reported person(s), if you know who they are, and their relationship with the company.

All reports must be based on a principle of proof that provides at least prima facie evidence of the reported facts. Supporting documentation may be submitted through the Ethical Channel for this purpose.

All reports may be made anonymously, i.e. the identification of the person making the report is not mandatory but optional.

The informant may indicate a method for the receipt of notifications, which can be a home address or safe place or an e-mail address. If such method is provided, the informant will be sent notifications regarding the admission and resolution of the report.

5. REPORT HANDLING PROCEDURE

5.1 How to report complaints

Reports on **MONTEPINO**'s Ethical Channel may be made through the following methods:

- Through the online form available at all times on the MONTEPINO corporate website https://montepino.net/en/canal-etico
- By post, marked for the attention of the Responsible of the Internal Information System ("*Responsable del Sistema Interno de Información*"), to: Calle Felipe Sanclemente 26, planta 3a, 50001 Zaragoza (Spain); or
- In a face-to-face meeting with the Responsible of the Internal Information System, which must be held no later than 7 days after the informant's request made by any of the above methods.

If a face-to-face meeting is held, the conversation shall be documented in one of the following ways after obtaining the informant's express informed consent for the processing of their personal data:

- As a recording of the conversation, kept in a secure, durable and accessible format; or
- In a full and accurate transcript of the conversation. In such case, the informant shall be allowed to check and correct the transcript and agree to its content by signing it.

If the informant has made a report using any of the reporting channels mentioned above, they shall receive an acknowledgement of receipt, within no more than 7 calendar days following receipt of the report, confirming that it has been correctly processed.

The informant's and the reported person's personal details must only be kept for as long as necessary to decide whether to start an investigation into the reported facts. In any event, the data must be deleted once three months since it was entered have passed, unless it is being retained to provide evidence of the operation of the Internal Information System.

If a report is not received through the above channels or is sent to a member of **MONTEPINO** other than the Responsible of the Internal Information System, the recipient must immediately forward it to the Responsible of the Internal Information System, ensuring that the communication remains completely confidential.

Any information received from outside the company, such as a communication from a judicial body or public authority, shall constitute a valid way of finding out about an incident, report or claim.

5.2 Receipt and preliminary analysis of communications or reports

5.2.1 Receipt and acknowledgement of receipt of communications or reports

All communications sent or reports made through **MONTEPINO**'s Ethical Channel shall be received by the Responsible of the Internal Information System, who shall be the person in charge of the Ethical Channel, and shall be organised as provided in this Procedure.

All communications or reports received shall be entered into a register of reports, in each case with a unique reference number to identify it throughout the handling process.

In the case of non-anonymous communications or reports, the Responsible of the Internal Information System shall send an acknowledgement of receipt within 7 days following receipt.

5.2.2. Requests for further information

If the Responsible of the Internal Information System deems the information received in the communication or report to be insufficient, they shall (in cases of non-anonymous reports, at the time of acknowledging receipt) ask the informant or complainant, as applicable, for any further information they may need.

5.2.3. Creation of the file and possible accumulation of files

The Responsible of the Internal Information System shall use the information received, as well as the acknowledgement of receipt where appropriate, to create an individual file for each case, which shall be duly numbered and registered for its better identification and to track the handling process.

If several notifications or reports in relation to the same or related facts are received, the Responsible of the Internal Information System may process those cases together in a single file.

5.2.4. Preliminary analysis of the information received

The Responsible of the Internal Information System shall carry out a preliminary analysis of the information received to check the magnitude, sufficiency and plausibility of the information, the informant's credibility and the relevance of the reported facts for these purposes, establishing whether they may constitute any of the acts or omissions described in Section 2.2.

The Responsible of the Internal Information System shall, within a maximum of fifteen (15) working days from the date of receipt of the communication or receipt, conduct a preliminary examination of the facts to establish whether they fall within the objective and subjective scopes of the Internal Information System, whether there is sufficient evidence or apparent evidence to admit it for processing and whether the

Responsible of the Internal Information System may have a conflict of interest.

The conclusions of the Responsible of the Internal Information System following the preliminary examination of the communication or report shall be set out in a report, which shall not contain information on the informant's identity in order to ensure their anonymity, confidentiality and impartial decision-making in the process of admitting it for processing.

5.2.5. Preliminary decision on the information received

Based on the results set forth in the preliminary analysis report, the Responsible of the Internal Information System shall consider whether the report should be admitted for processing and whether there is sufficient evidence or apparent evidence on which to base the decision to do so.

The Responsible of the Internal Information System may only decide not to reject the report if:

- The reported facts are completely implausible;
- The reported facts do not relate to any of the persons included in the subjective scope mentioned above;
- The reported facts do not fall within the objective scope of the Ethical Channel;
- The reported facts do not contain any new and significant information on the acts or omissions reported compared to a previous communication whose procedure has now concluded, unless a different treatment is justified by new circumstances.

In order to decide whether to admit the report for processing, the informant may be asked to clarify or provide new information on the reported facts, including submitting any documents that may be necessary to prove the regulatory infringement.

If the report is rejected on the grounds that the facts do not fall within the objective and/or subjective scope of the Ethical Channel, the Responsible of the Internal Information System shall inform the complainant or the informant of this decision (if the report was not made anonymously and a communication method was provided) and may refer the matter to other internal bodies that may be competent in each case to handle the communication through other internal procedures that may have been established by **MONTEPINO** for that purpose.

It is hereby expressly stated for the record that reports will not be rejected on the grounds of failure to comply with formal requirements. However, if a report is made with a false identity for the informant or if no apparent evidence of the reported facts has been provided, the Responsible of the Internal Information System may legitimately reject the report.

Once the Responsible of the Internal Information System has decided to admit the report for processing, they shall register the report under investigation and inform the informant of this decision within five (5) working days after the date of the resolution (if the report was not made anonymously and the informant has provided a communication method).

If the report is rejected, the Responsible of the Internal Information System shall ensure that the informant suffers no adverse consequences as a result of making it.

5.2.6. Additional measures

If the Responsible of the Internal Information System decides, based on the information obtained during the investigation, that there are situations requiring immediate action to be taken in order to safeguard the interests of **MONTEPINO** or third parties, they shall immediately inform the management body of the Company affected by the report, and the latter may take precautionary measures such as:

- Necessary measures to reduce or mitigate possible financial damage caused to **MONTEPINO** or third parties.
- Measures to ensure the preservation of the evidence required for the investigation into the reported facts.
- Necessary measures to address the internal control weaknesses identified.
- Immediate reporting of the reported facts to the police and/or judicial authorities.

5.2.7. Statistical report and periodic reporting

The Responsible of the Internal Information System shall be responsible for drawing up a descriptive statistical report on the main parameters of each file, particularly those that may be considered personal or in any other way relevant to the handling of reports, excluding all the data that may be subject to special protection under the current legislation. The interested parties may not be actually or potentially identifiable in this statistical report, and the personal data must be kept properly dissociated with pseudonymisation and data encryption techniques where appropriate.

Every six months, the Responsible of the Internal Information System shall inform the management body of **MONTEPINO** of all new files, providing only the data included in the statistical report.

5.3 Investigation

5.3.1 Investigation procedure

Depending on the scope, extent and people allegedly involved in the reported facts,

the Responsible of the Internal Information System shall assess the investigation strategy to be applied to the case at hand and may choose one of the following options:

- An investigation procedure designed, led and managed in its entirety by the Responsible of the Internal Information System, although without prejudice to any consultations or specific support that may be required of other departments in order to complete it.
- An investigation procedure designed, led and managed by an investigation team appointed for that purpose (which may include Management Company staff), whose members may include representatives of any department or unit that may have any knowledge of the alleged facts or whose involvement may be relevant for the investigation. The confidential treatment of the file and/or the reported facts shall be guaranteed in any case, with only the Responsible of the Internal Information System, or the above-mentioned representatives where strictly necessary, being able to access it.
- A fully or partly outsourced investigation procedure, depending on whether the circumstances of the case suggest that ad hoc expert advice should be obtained in relation to a particular aspect or that the investigation should be fully external. This strategy will be particularly advisable in cases in which it is considered that the investigation may require a higher standard of confidentiality.

Any person who has access to personal data during the procedure must ensure full confidentiality and comply with the data protection instructions given to them by the Responsible of the Internal Information System.

All investigations that are initiated shall be entered in the register of reports, retaining the unique reference number assigned to the report so that it may be identified throughout its processing.

The Responsible of the Internal Information System may carry out any actions they may deem appropriate to ascertain the facts. This shall include, among others, accessing documents, interviewing the informant (including to request further information), the reported person and witnesses, carrying out specific audits and hiring external advisers or experts.

In any event, all actions carried out in connection with the handling and processing of the investigation into the report shall be carried out respecting fundamental rights and ensuring the lawfulness and evidentiary value of the evidence obtained. Furthermore, all actions shall be carried out ensuring the confidentiality of the informant's identity and that of any third parties mentioned in the report, and access thereto by unauthorised personnel shall not be permitted.

5.3.2 Planning the Investigation

Both the Responsible of the Internal Information System and any other investigator that may be appointed shall plan the investigation with the aim of ascertaining the facts and identifying the persons responsible for them. Such planning may include the following steps:

- Identifying the legislation, policies, procedures or internal regulations concerned, as well as the reputational, economic, financial or legal risks that may arise from the allegation.
- Identifying all the information and documents that may be relevant and whose review is deemed useful for the investigator (such as e-mails, websites, audiovisual surveillance and security recordings of the company, lists of attendees, passwords or electronic security devices and accounting records). The investigator must seek approval from the Responsible of the Internal Information System before accessing any documents that are not strictly work-related and that may contain personal content, and the latter must consult **MONTEPINO**'s legal advisers if they are unsure.
- Establishing, if necessary in collaboration with the Management Company's Human Resources department (or, if applicable in the event of future changes to the corporate structure, with the relevant department of MONTEPINO LOGISTICA or its affiliates companies), the need and possible urgency of taking injunctive relief in relation to the persons under investigation. Possible injunctive relief may include, among others:
    - Temporarily relocating the persons under investigation or transferring them to another department.
    - Changing the usual duties or responsibilities of the persons under investigation.
- Suspending the persons under investigation with immediate effect. Drawing up a script of the investigation procedure to be carried out, as well as of the various interviews to be held with the affected parties, including relevant questions, the identification of witnesses, logistical aspects regarding the conduct of interviews, etc.
- Including in the investigation file all the information that may be of interest in relation to the investigated person's working life at **MONTEPINO** (such as employment history, previous incidents or any company policies, procedures and regulations that are particularly applicable to them).
- When planning the investigation, efforts shall always be made to both protect the privacy of the persons under investigation and minimise the impact of the investigation on both those persons and the company.

5.3.3 Communication to the persons under investigation

Before starting the investigation, the investigator shall contact the reported persons, identifying themselves as the person in charge of investigating the report and informing them of the acts or omissions of which they are accused and of the main likely milestones of the investigation.

This information shall be provided to the persons under investigation within no more than 15 days from the date of receipt of the report. This communication to the reported person may exceptionally be delayed if so decided by the Responsible of the Internal Information System if they suspect on well-founded and objective grounds that sending such a communication to the reported person could compromise the investigation or risk the destruction of evidence.

Pursuant to the principle that both parties must be heard and the presumption of innocence, the reported person must be given a chance to be heard and provide the necessary information and documents to guarantee their right to defend themselves through any evidentiary method permitted by Spanish law. The presumption of innocence and the reported person's honour shall be respected at all times.

In order to guarantee the reported person's right to a defence, they shall have access to the information in the file, although this may in no event contain any information capable of identifying the informant or make them identifiable.

5.3.4 Conduct of the Investigation

The investigation shall include all investigative steps that may be appropriate to ascertain the facts and the persons responsible for them and decide on the adoption of any corrective measures. Below are some of the main steps that may be included in the investigation:

- Holding an interview with the informant to obtain further information about the report.
- Obtaining statements from the persons under investigation.
- Conducting interviews with witnesses and asking them to complete questionnaires, in both cases under conditions of confidentiality.
- Holding hearings with the persons under investigation, their superiors, their colleagues and any other persons that may be deemed necessary.
- Obtaining as much information as possible through the company's documentation.
- If essential in order to ascertain the facts, adopting surveillance measures through private detectives or computer, telematic or audiovisual methods, provided that they comply with reasonableness, suitability and proportionality criteria, and protecting the employee's right to privacy and the right to the secrecy of communications at all times.
- Obtaining external assistance from other professionals.

- Any other steps that may be deemed necessary by the investigator to ascertain the facts.

5.3.5 Investigation documents

It is essential to include detailed documentation of the whole investigation procedure in the file, including the initial investigation plan, all the documents obtained and records of the interviews held.

In all interviews conducted by them, the investigator shall write down the relevant facts of the interview and include them in a record of the interview, which must be signed by the investigator and the parties present. In addition, all the information required by the current data protection legislation must be provided in all interviews.

5.3.6 Final report

Once all the investigative steps have been completed, the investigator shall draw up a report of findings within no more than 15 days. This must contain a description of:

- **The subject matter of the report:** The persons involved, the nature of the facts, the date, place and circumstances of the alleged facts and the legal provisions or internal regulations that have been breached or compromised shall be identified where possible.
- **The investigator's identity:** The member(s) of the team who carried out the investigation shall be duly identified.
- **A list of relevant facts and discoveries:** A list of the most relevant facts established during the investigation shall be provided, with a distinction between those obtained from MONTEPINO's documents, the information provided by the informant and the interviews held with witnesses and the persons under investigation.
- **Breakdown of the evidence:** A description of the evidence obtained during the investigation procedure shall be provided.
- **Findings and assessment of the facts:** The report shall set out the investigator's findings and their assessment of the reported facts, and two possible lines of action may be proposed:

    - Proposal to continue with the procedure if the investigator considers that, based on the outcome of the investigation, it has been sufficiently proven that the person under investigation has committed an offence or infringement of any of the types included in the objective scope of this Procedure.

    - Filing of the report if the investigator considers that the facts do not constitute an offence or infringement falling under the objective scope

of this Procedure, that its commission has not been sufficiently proven or that the offender's identity has not been proven or such person does not fall under the subjective scope of this Procedure.

- **Proposed sanction:** When the investigator's report concludes with a proposal to continue with the procedure, it must include a final section identifying the sanctions that may be applied by **MONTEPINO** against the persons responsible for the facts, as well as any other additional measures of any kind, including possible actions for compensation which may be taken in respect of any injured party, all in any person harmed by the facts,, all this as provided in the Code of Ethics, based on the seriousness of the infringement and within the applicable legal framework in accordance with the Workers' Statutes (*Estatuto de los Trabajadores*) and the applicable collective agreements.

5.4 Final steps

The Responsible of the Internal Information System must draw up a final investigation report, which must be filed together with the rest of the investigation file.

Furthermore, the Responsible of the Internal Information System shall draw up a resolution proposal and submit it to the governing body of the Company affected by the report within five (5) working days from the date of the final investigation report. To ensure impartiality and independence at each stage of processing of reports, the final decision on whether to file a report or apply disciplinary measures shall be taken by the Company's management body.

The report may only be filed if the governing body of the affected Company considers that either the reported facts or the identity of the alleged perpetrator has/ve not been sufficiently proven or do(es) not fall under the objective or subjective scope of the Internal Information System.

After taking the resolution decision, which must be recorded in writing and be sufficiently reasoned, the governing body of the Company affected by the report shall inform the Head of the Internal Information System of the resolution.

The Responsible of the Internal Information System must similarly inform the informant (unless the report was made anonymously and no notification method was provided) and the reported person of the outcome of the resolution within five (5) working days from the day immediately following that on which the governing body's decision was received.

In any event, the communication of the resolution on the outcome of the investigation must be sent no later than 3 months from the date of receipt of the communication

or report, except in particularly complex cases requiring a longer period, in which case the deadline may be extended by up to a further 3 months.

6. DISCIPLINARY MEASURES

Any disciplinary or corrective measures taken must be effective and proportionate and dissuasive and shall always be applied fully in accordance with the applicable regulations and the sanctioned person's fundamental rights, and in each case as provided in the collective agreement applicable from time to time or in the Workers' Statute.

Such sanctions shall be graduated based on the seriousness of the facts, taking into account recurrence, the damage or harm caused, the circumstances of any victims and other circumstances.

Depending on who committed the offence or infringement, **MONTEPINO**'s Head of Human Resources shall be informed of the enforcement of these sanctions.

Finally, if the reported facts suggest that a criminal offence may have been committed, the Public Prosecutor's Office shall be informed. If the reported facts affect the EU's financial interests, the case shall be referred to the European Public Prosecutor's Office. The management body may also take additional measures, such as:

- Reporting the facts to any administrative or judicial authority with competence in relation to the facts.
- Adopting compensatory action against any person or entity that may have been detrimentally affected by the facts.
- Making decisions regarding communication, training or internal dissemination of the facts, both to any body or unit of **MONTEPINO** and to its workforce as a whole if this is considered an effective way to prevent similar incidents from taking place in the future (always with all proper precautions as regards data protection).
- Proposing any organisational or preventive measures of any kind.

The reported persons shall be immediately informed of the governing body's decisions.

The reported persons' managers shall also be informed of those decisions. The communication to managers must not include any information on the nature of the procedure carried out, the facts or the measures adopted (save as strictly necessary) or the informant's identity.

7. DOCUMENTATION

7.1 Media

All actions carried out in connection with the processing and investigation of a report, as well as the decisions of the Responsible of the Internal Information System and the governing body, must be properly justified and documented in a report or record signed by all the parties present, as applicable.

The Responsible of the Internal Information System shall record the communications or reports received, including the following information:

- The unique identification number of the communication or report received.
- The date of the acknowledgement of receipt sent by the Responsible of the Internal Information System.
- Traceability of the milestones of the investigation.
- Final report of the investigation.
- Communication to the governing body.
- Resolution.

7.2 Storage periods

ITEM		RETENTION PERIOD	TOTAL TIME
Full/preliminary investigation		Duration of the investigation (which may in general not exceed 3 months)	3 months
Following the completion of the full/preliminary investigation	Reports on facts that have not been proven	Up to 2 months from the end of the investigation	5 months
	Reports about proven facts when starting criminal, labour or other proceedings	The time taken to process the procedure	3 months + the time taken to process the procedure
	Following the completion of the procedure	Up to 2 months from the end of the procedure	3 months + the time taken to process the procedure + 2 months

If the facts under investigation allegedly constitute a criminal offence, and in order to collaborate as much as possible with any courts and competent public authorities conducting the investigation, the retention period shall be extended until the end of the limitation period for the alleged offences.

The data shall be stored in blocked form in any event. In other words, it shall be identified and reserved to prevent it from being processed except for the purpose of making it available to the courts, judges and public authorities. Once the periods set forth in the above table have elapsed, the file and all the documents relating to the investigated events shall be destroyed.

8. ETHICAL CHANNEL SAFEGUARDS AND PROTECTION FOR INFORMANTS

8.1 Transparency and accessibility

MONTEPINO's Internal Information System and this Complaints Management Procedure are available on the corporate website, where they can be easily accessed by all interested parties.

8.2 Autonomy and independence

The Responsible of **MONTEPINO**'s Internal 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 informant's identity under any circumstances and that they are not involved in the handling of the communication or report shall be put in place.

8.3 Confidentiality and anonymity

MONTEPINO guarantees the informant's anonymity when making reports, utmost confidentiality in the treatment of all the information and personal data collected and processed in the management of the Ethical Channel, particularly as regards the informant's identity and that of any third parties mentioned in
To further reinforce this confidentiality, the informant's identity shall not be disclosed in the preliminary and final reports drawn up by the Responsible of the Internal Information System.

In order to ensure the utmost confidentiality, the persons involved in the handling of

reports shall sign a specific confidentiality agreement.

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

8.4 Conflicts of interest

If the Responsible of the Internal Information System or any member of the governing body of the Company affected by a report is affected by an actual or potential conflict of interest, the necessary mechanisms to ensure that they do not find out the informant's identity in any event shall be put in place. In addition, they must not be involved in the handling of the report and may not vote on any decisions relating to its processing.

For example, and without limitation, a conflict of interest shall be deemed to exist in the following cases:

- Being involved or having a personal or professional interest in the reported facts.
- Being related to the informant or the reported person to the fourth degree or consanguinity or the second degree of affinity.
- Being a close friend or clear enemy of the informant or the reported person.

Any person to whom any of the above circumstances apply must immediately inform the Responsible of the Internal Information System, or the governing body of the Company affected by the report if the person with a conflict of interest is the Responsible of the Internal Information System. The party thus informed in each case shall decide whether there is a conflict of interest within five (5) working days, after considering any reports, sworn statements and checks they may deem appropriate.

Failure to report any possible conflicts of interest or to recuse oneself when it has been decided by the Responsible of the Internal Information System (or by the governing body of the Company affected by the report if the person with a conflict of interest is the Responsible of the Internal Information System) that they should do so shall give rise to liability for the person affected by the conflict of interest.

Notwithstanding the foregoing, the actions carried out by persons who have reason to recuse themselves shall not necessarily void the acts in which they have been involved.

8.5 Prohibition on retaliation

All retaliatory action of any kind against informants who make a report that meets the requirements of the Policy on the Internal Information System and this Procedure in

good faith through **MONTEPINO**'s Ethical Channel, including making retaliation threats and attempts, penalising them or causing them harm, is strictly forbidden.

MONTEPINO shall put in place the necessary mechanisms and procedures in each specific case to ensure the protection of bona fide informants, issuing appropriate sanctions in response to any retaliation of any kind to which they may be subjected as a result of making a report.

Any informant who feels that they are the victim of an act of retaliation or negative consequences for their job as a result of making a report must immediately inform the Responsible of the Internal Information System, or the governing body of the Company affected by the report if the possible retaliation could come from the Responsible of the Internal Information System, who shall investigate this complaint and take appropriate corrective action if necessary.

The complainant shall be granted protective measures against any potential retaliation involving:

- Suspension, dismissal, removal from their position or equivalent actions;
- Demotion or denial of access to promotion;
- Change of position, relocation, salary reduction or change of working hours;
- Denial of access to training;
- Negative assessments or references regarding their performance at work;
- Any disciplinary measures, reprimands or other sanctions, including financial ones;
- Pressure, intimidation, harassment or ostracism;
- Discrimination or adverse or unfair treatment;
- Failure to convert a temporary employment contract into a permanent one in cases in which the employee had a legitimate expectation that this would happen;
- Failure to renew a temporary employment contract, or early termination thereof;
- Damage, including reputational damage, particularly on social media, or financial loss, including loss of business and income;
- Blacklisting based on a formal or informal sectoral agreement capable of affecting their ability to find employment in that sector in the future;
- Early termination or cancellation of contracts for goods or services;
- Cancellation of a licence or permit;
- Medical or psychiatric references.

8.6 Reports made in bad faith

A report shall be deemed to have been made in good faith if it is based on reasonable belief or apparent evidence and is not motivated by a wish for revenge or

to harm the reported person.

On the other hand, disciplinary or other measures shall be adopted as may be deemed appropriate in each case against any persons who make a report, knowing it to be false or with clear disregard for the truth, for the sole purpose of causing harm to the reported person.

8. DATA PROTECTION

The personal data contained in the communication or report in accordance with the terms of this Procedure, as well as all the data to which the Management Company and/or the Compliance Officer has/ve access in connection with this report handling, investigation and response protocol (the "Data") shall be processed by the Management Company as **Controller**, with the following identification and contact details:

- Identity: VALFONDO GESTIÓN, S.L.
- Address: Calle Felipe Sanclemente, 26, 3º, 50001 Zaragoza (Spain).
- Data Protection Officer's contact details: protecciondatos@valfondo.com

The only persons authorised to process the personal data obtained through the Ethical Channel are:

- The Responsible of **MONTEPINO**'s Internal Information System and the governing body of the Company affected by the report;
- The Head of Human Resources, but only for the management of disciplinary measures;
- The members of MONTEPINO's legal team if appropriate legal action is taken;
- The data protection officer;
- Advisers and investigators as provided in this Procedure.

All the persons specified above are contractually bound by a duty of secrecy, discretion and confidentiality.

The personal data processed in connection with the management of the Ethical Channel shall be limited to the data voluntarily provided by the informant (for non-anonymous reports) or to the data that is strictly necessary to process the reports received and, where appropriate, to investigate the facts reported in accordance with this Procedure.

The aforementioned data shall be processed for the sole purpose of processing, investigating and/or making a decision on the reports concerned and to make any

communications and notifications in accordance with this procedure. Information obtained through the Ethical Channel may not be used for any other purpose.

The aforementioned data shall be processed for the sole purpose of processing, investigating and/or making a decision on the reports concerned and to make any communications and notifications as provided in this Procedure. The Data may also be processed for the purpose of handling any queries or consultations on legal compliance and to advise informants on the process to be carried out in relation to their report.

The legitimate basis for processing the Data in connection with the management of the Ethical Channel is based on the following legal grounds:

- The performance of the employment relationship with the company in accordance with the terms and conditions of the contract on which the employment relationship between the employee and MONTEPINO is based. In particular, the performance of its powers of surveillance and control under Article 20.3 of the Workers' Statute;

- The performance of a legal obligation pursuant to Law 2/2023, of 20 February, on the protection of persons who report breaches of regulations and infringements relating to the fight against corruption; Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights; and Circular 1/2016, of the Public Prosecutor's Office, which affects reports and communications on the prevention of money laundering.

- MONTEPINO's legitimate interest in avoiding the corporate penal liability to which it might be subject under Article 31 bis of the Criminal Code.

The personal Data processed in connection with the management of the Ethical Channel shall be retained in the Ethical Channel 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 report.

Notwithstanding the foregoing, the personal Data may be processed for longer than this outside the Ethical Channel system if the outcome of the investigation process started by reason of the reported facts may make 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.

After the specified time, the personal Data must be deleted or blocked outside the Ethical Channel if it is retained in this way as evidence of the Ethical Channel's

operation or to audit or improve it.

The personal Data contained in reports that have not been admitted for processing may only appear therein in anonymised form. This means that no personal data may be associated with them and the blocking obligation therefore does not apply.

The personal Data provided through the Channel shall in no event be the subject of an international transfer of data.

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 for the adoption of disciplinary measures or conduct any court proceedings that may be appropriate.

The data subjects whose personal Data is processed in connection with the management of the Ethical Channel may exercise their data protection rights in accordance with the terms of the current legislation and with the scope envisaged in it from time to time, by sending a written communication, marked for the attention of the Data Protection Officer ("*Delegado de Protección de Datos*"), either by post to the address provided above or by e-mail to protecciondatos@valfondo.com.

The request must expressly include the data subject's full name; a copy of their ID card, passport or other valid identity document of their own or of their representative if they are acting through one (including in such case documentary evidence of their representative authority); address for notices; and the purpose of the request or the right they are exercising.

In addition, the data subject may file a complaint at any time with the Spanish Data Protection Agency (AEPD) as the competent supervisory authority in the field of personal data, particularly if they have not received a satisfactory response to the request to exercise their rights, by writing to: Agencia Española de Protección de Datos, Calle Jorge Juan, 6, 28001 Madrid (Spain); or through the website https://www.aepd.es.

Data subjects are hereby informed in any case that:

- They have the right to obtain confirmation as to whether **MONTEPINO** is processing their personal Data in connection with the management of the Ethical Channel and to request the rectification of any inaccurate Data, or its deletion if appropriate, when, among other reasons, the Data is no longer required for the management of the Ethical Channel.

- They have the right to access only their own personal data. In other

words, the reported person will not be given any information on the identity of the informant or complainant.

- When the informant requests a meeting with the Responsible of the Internal Information System in order to make a report, **MONTEPINO** shall, after informing them of the processing of their personal Data and obtaining their express consent, ensure that a record of the meeting is retained in a durable and accessible format that can be checked, rectified and accepted by the informant by means of their signature.

If the reported person exercises their right to object to the processing of their data, the existence of compelling legitimate grounds for its processing for the stated purpose shall be presumed unless there is evidence to the contrary.

The data subject may exercise their rights of access, rectification and erasure of data, as well as to restrict or object to the processing of their personal data or request its portability, at any time in accordance with the current legislation.

All persons who make a communication through the communication channels warrant and represent that the personal data provided is true, accurate, complete and up to date; and they shall hold MONTEPINO harmless in relation to any liability that may arise from breach of these representations and warranties.

* * * * * * *