PROCEDURE OF THE INTERNAL INFORMATION SYSTEM OF THE INMOCEMENTO GROUP

7 November 2024

INDEX

0. VERSION CONTROL

Version	Date	Modifications
1	7 November of 2024	Version version. Approved by the Board Board of Directors

1. INTRODUCTION AND OBJECTIVE

This Internal Information System Procedure of the INMOCEMENTO Group (the "**Procedure**") regulates the use and operation of the Group's Internal Information System (the "**Internal Information System**" or the "**System**") in accordance with the provisions of the Code of Ethics and Conduct of the INMOCEMENTO Group (the "**Code of Ethics and Conduct**"), the Internal Information System Policy (the "**Policy**") and other applicable regulations.

This Procedure is configured as the internal rule required by the legislation transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law into Spanish law to manage the information received through the Ethics Channel, which is the channel enabled by INMOCEMENTO, S.A. ("**INMOCEMENTO**" or the "**Company**") so that all employees, managers, directors of the group of companies of which INMOCEMENTO is the controlling entity ("**INMOCEMENTO Group**" or the "**Group**"), in the sense explained below, or persons related to such companies (suppliers and contractors, shareholders, volunteers, interns and trainees) may communicate any information of which they are aware:

(i) on the existence of a possible irregularity or act contrary to the Code of Ethics and Conduct or the Criminal Prevention Model, or any other applicable internal regulations, provided that the irregularity is of particular relevance; or

(ii) on the existence of a possible irregularity or unlawful act, including conduct that may constitute a serious or very serious criminal or administrative offence, as well as an infringement of European Union law, in relation to activities subject to European Union law.

All acts contrary to the Code of Ethics and Conduct and the Criminal Prevention Model are, by definition, irregularities of particular relevance. An irregularity or act shall be understood to be contrary to the rest of the INMOCEMENTO Group's internal regulations when the irregularity in question may affect any fundamental right of the persons affected by the information received; when the irregularity may have a significant impact on the reputation of the Group; and when the rules breached and/or the breaches are particularly relevant to the Group's activity or have a significant impact on its operation.

This is without prejudice to their right to refer the matter to any competent authority or body and, in particular, to the Independent Authority for Whistleblower Protection, in the event that the matter concerns a Spanish company.

The Procedure shall also apply to those companies of the INMOCEMENTO Group established in countries outside the European Union, without prejudice to the fact that all companies of the Group shall respect any laws relating to whistleblower protection and the regulation of the Internal Reporting System that may be applicable in those jurisdictions in which such companies operate.

2. SCOPE OF APPLICATION

This Procedure regulates the management of all communications received in the INMOCEMENTO Group's Information System, and is applicable to all the companies that make up the Group. For the purposes of this rule, the INMOCEMENTO Group is understood to be: INMOCEMENTO and those companies in whose share capital the Company holds, directly or indirectly, a majority of the shares, holdings or voting rights, or in whose governing or administrative body it has appointed or has the power to appoint a majority of its members, in such a way that it effectively controls the company.

Notwithstanding the fact that the Group shall, in principle, have a single Internal Information System, the companies or subgroups of companies may establish their own Systems for the same purpose when so required by the legislation in force in each case, subject to the prior authorisation of the Compliance Committee.

These systems must be adequately coordinated with the global Internal Information System of the INMOCEMENTO Group and have their own management procedures, which must comply with the principles and criteria established in this Procedure and in the Policy, without prejudice to any specialisations that may be appropriate due to the legislation applicable to the activities of each company. Those responsible for such systems must ensure proper coordination with the Group's Internal Information System in order to guarantee the best performance of their functions. In order to ensure such coordination, the aforementioned heads shall exchange with the Compliance Committee all relevant information for such purpose.

The establishment of such proprietary systems and their governing rules shall be approved by the board of directors of the head of business company to which the company(ies) to which such systems are necessary under the relevant legislation so require.

3. MANAGEMENT OF THE INTERNAL SYSTEM OF INFORMATION

The Compliance Committee is responsible for the Internal Reporting System, in accordance with the provisions of the Policy, and the Independent Whistleblower Protection Authority shall be informed in a timely manner.

The Compliance Committee shall delegate the powers to manage the System and process investigation files to the corporate Compliance Officer, who in turn is a member of the Compliance Committee (the "**Responsible Officer**").

The Compliance Committee and the Controller shall act in accordance with the provisions of the Policy, the Procedure and other applicable regulations. To this end, the Compliance Committee may establish the corresponding protocols that develop these rules and that, in particular, shall guarantee the confidentiality of the identity of the informant and of any third party named in any notification, and of the actions carried out in the management and processing of such notifications, as well as the protection of personal data, preventing

access to the content of investigations by staff who are not expressly authorised.

4. OPERATION AND MANAGEMENT OF THE ETHICAL CHANNEL

The Ethics Channel is the preferred means for the management of the Group-related information referred to in paragraph 1 above.

4.1. Access routes to the Ethical Channel

The Ethical Channel will be accessible through:

- The INMOCEMENTO website and, where appropriate, the websites of other Group companies.
- The telephone number enabled, where applicable, in each of the companies of the INMOCEMENTO Group. When this telephone number is used, the notification will be recorded and will be kept as an audio recording, in accordance with the applicable legislation.
- P.O. Box 19312, 28080 Madrid, Spain.
- E-mail to canaletico@inmocemento.es

At the request of the informant, the information may also be presented at a face-to-face meeting to be held within a maximum of seven calendar days of the request. Such a request may be made through any of the aforementioned channels of access to the Ethics Channel.

Verbal reports, including those made in a face-to-face meeting, by telephone or by voice messaging system, should be documented in one of the following ways, subject to the informant's consent: (i) by a recording of the conversation in a secure, durable and accessible format, or (ii) by a complete and accurate transcript of the conversation.

In the event that the informant does not consent to any of the above options, this shall be indicated and a written statement by the recipient of the communication with the content of the communication may be made, which shall not be considered as a transcript.

In case the notification received is not anonymous, the identity of the informant shall in any case be withheld and the necessary measures shall be taken to ensure the confidentiality and other rights of the informant.

In the event that a notification or complaint subject to the Ethics Channel is received through a different channel or by a person other than those responsible for its management, such person must maintain absolute confidentiality regarding the information received and immediately forward the communication to those responsible. Failure to comply with this obligation constitutes a very serious breach of this Policy. In this regard, training and awareness-raising initiatives will be designed and promoted so that employees know how to act in the event of receiving a communication.

which it is not their responsibility to manage. In such cases, for the purposes of the Policy and the Procedure, the person who initially provides the information shall be considered to be the informant.

4.2. Register of communications and acknowledgement of receipt

All communications received through the Ethics Channel shall be recorded in the database referred to in section 4.11 of this Procedure, either automatically or manually, depending on the channel through which the communication is reported.

An acknowledgement of receipt shall be sent to the reporter within seven calendar days of receipt of the communication, unless this would jeopardise the confidentiality of the communication itself.

You will also be expressly informed that your identity will in all cases be kept confidential and that it will not be communicated to the persons to whom the facts reported refer, nor to third parties, except in strictly necessary cases.

When the informant directly provides his or her personal data, he or she will be provided with the information on personal data protection and the exercise of rights established in the regulations in force.

4.3. Form and content of the notifications

When making the report, the informant must describe the conduct that is the subject of the report in as much detail as possible in terms of facts, dates, places, names, amounts, suppliers, customers, as well as any other details that may provide greater knowledge of the reported/notified event, and may also provide any documents that he/she deems appropriate to obtain a complete description of the reported event.

In cases where it is deemed appropriate and where it is possible and safe to contact the reporter, while safeguarding the confidentiality of the report, the Data Controller may request additional information from the reporter.

Anonymous communications will be admissible in jurisdictions where the applicable law so permits, such as Spain.

If the report is not anonymous, the reporter may, if he/she so wishes, provide an address, e-mail address or secure location for the purpose of receiving any communications about his/her report. The reporter shall be protected by the confidentiality guarantees of the System, which operates under the principle of non-retaliation, in accordance with applicable law.

4.4. Classification and admission for processing of the communications

The person in charge is the person responsible for receiving communications and assessing their admissibility, classifying them on a preliminary basis, according to their typology and risk, in accordance with the criteria indicated below.

In the event that the Controller becomes aware that the facts described in a communication directly affect him or her and present a conflict of interest, he or she must

to withdraw completely from the handling of such a communication and to refer it to the Compliance Committee.

The Compliance Committee shall appoint, from among the rest of its members, a person to replace the Controller in all functions related to the communication affecting the Controller, from the time prior to the classification and assessment of the admissibility of the communication, and until the end of the relevant processing.

The Controller shall not have access to information relating to communications concerning him or her, nor shall he or she participate in the processing of such communications in any way, without prejudice to the rights attributed in this Procedure and the Policy to all persons affected by a notification, which shall apply to the Controller in his or her capacity, if any, as a person affected by a notification.

Consultations

Queries shall be considered to be those communications received in which doubts are raised and an opinion or advice is requested on the interpretation of the INMOCEMENTO Group's internal regulations or on how to act in a given situation in application thereof, but no report is made on conduct that may constitute a breach of the provisions of section 1 of this Procedure.

In these cases, the Data Controller will respond directly to the informant as soon as possible or will redirect the notification to one of the Compliance Officers of the businesses so that they can respond to the query, also as soon as possible.

Notifications

Notifications shall be considered to be those communications in which possible irregularities or acts that may be contrary to the law, the Code of Ethics and Conduct or the Criminal Prevention Model are reported, as well as any other possible irregularity or act contrary to the rest of the Group's internal regulations that are of particular relevance, in the terms established in section 1 of this Procedure.

Once a communication has been received and classified as a notification, a determination will be made as to whether or not to process it, depending on whether or not it meets the minimum requirements for initiating an investigation. The decision to admit or not to process notifications shall be made by the person in charge.

(i) <u>Irrelevant notifications</u>

Notifications will be considered irrelevant if they are notoriously lacking in substance, plausibility or evidence of the facts reported, do not identify conduct that constitutes a breach of the Code of Ethics and Conduct or the Crime Prevention Model, or do not identify conduct that constitutes an irregularity or act contrary to any other internal Group regulation of particular relevance under the terms set out in section 1 of this Procedure, or which are not

any irregularity or unlawful act, criminal offence, serious or very serious administrative offence or infringement of European Union law.

Interpersonal conflicts that do not constitute a breach of those referred to in the previous paragraph shall be classified as non-relevant notifications, which must be communicated through the respective HR departments.

Similarly, complaints about the behaviour of other employees that do not constitute a breach of those referred to in the first paragraph of this sub-section (i) shall be classified as non-relevant notifications. These complaints shall be transferred by the Head to the corresponding management area.

Non-relevant notifications will not be accepted for processing, with reasons given by the Data Controller. The Controller shall inform the informant, within a maximum period of seven calendar days from the adoption of its decision, of the non-admission of the communication in the Ethics Channel.

False communications made in bad faith are not permitted and will also be classified as non-responsive notifications. Whistleblowers who send false communications or who must be classified as non-relevant notifications will not enjoy the protection provided for in the legislation in force for whistleblowers whose communications do refer to potential breaches included in the scope of application of the protection measures legally provided for.

(ii) <u>Relevant notifications</u>

Notifications that, if substantiated or credible, identify conduct that may constitute a possible breach of any of the Group's internal rules and legislation under the terms set forth in section (i) above, shall be considered relevant.

The relevant notifications will be accepted for processing in a reasoned manner by the Controller.

For the purposes of deciding whether a notification is admissible, the informant may be asked to clarify or complete it, providing such documentation and/or data as may be necessary to prove the existence of the conduct complained of. This request must be complied with within a maximum period of ten days. If no reply is received, the notification will be classified as irrelevant and will be inadmissible.

For the purposes of adopting the decision on the admission for processing, the Controller may request, where appropriate, the cooperation of other areas of the Group, or even of third parties, if necessary. In this case, the Controller shall ensure that the confidentiality of the content of the notification and the identity of both the informant and those affected is safeguarded.

Once a notification has been classified as relevant and accepted for processing, the Officer will classify it, in turn, into one of the three sub-categories defined below.

- ***High Risk Notifications***

  The following shall be classified as high risk notifications:

  - Corruption, bribery and influence peddling offences.
  - Natural resource and environmental crime with significant impact on the Group.
  - Fraud in the preparation of financial statements that has a material impact.
  - Money laundering offence.
  - Financing of political parties.
  - Harassment at work, sexual harassment or harassment based on sex.
  - Infringements of competition law.
  - Non-compliance with the Code of Ethics and Conduct with relevant or material impact for the Group.
  - Relevant conflicts of interest or involving senior management.
  - Leakage of relevant information.
  - Actions of senior management that constitute a breach of the Code of Ethics and Conduct.
  - Acts or omissions which may constitute breaches of European Union law falling within the scope of the European Union acts listed in the Annex to Directive (EU) 2019/1937 on the protection of persons reporting breaches of Union law; or affecting the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); or having an impact on the internal market.
  - Other actions that could have a significant reputational impact for the Group.
  - Any other actions or omissions that could constitute a serious or very serious criminal or administrative offence.

- ***Medium Risk Notifications***

  Notifications related to the application of the Code of Ethics and Conduct, the Crime Prevention Model and possible irregularities.

or acts contrary to the rest of the Group's internal rules that are of particular relevance in the terms set out in paragraph 1 of this Procedure shall be considered medium risk notifications when they do not have a significant impact on the reputation of the Group and the legal person.

Main categories (including but not limited to):

- Inappropriate use of company assets.
- Breaches of specific criminal risk mitigating controls.
- Conflicts of interest of non-management personnel.
- Notifications relating to actions of employees at or below managerial level.
- Breaches of the Code of Ethics and Conduct with no relevant or material impact for the Group.
- Practical issues relating to the implementation of the Code of Ethics and Conduct specific to each business.

Other Communications

Other communications shall be considered to be those that do not contain information on conduct of the type envisaged in section 1 of this Procedure, but which refer to alleged breaches or claims of a purely contractual nature or breaches of internal Group rules that are not particularly relevant, which shall be sent by the Head to the area of the Group competent for their management and resolution. Among others, "other communications" may be considered to be those relating to:

- Issues related to commercial matters.
- Comments or suggestions for improvement.
- Other communications not directly related to the above points.

4.5. Designation of Instructor

When a notification is admitted for processing by the Head, the latter will inform the Committee in order to initiate the investigation and processing of the file. For such purposes, the Committee shall designate the corresponding instructor (the "**Instructor**"), who may be the Compliance Officer of the business to which the notification refers, when the notification is classified as medium risk, or another person with authorised access to the System who, in view of the facts, is relevant.

In certain cases, the Instructing Officer may be a third party external to the INMOCEMENTO Group, in accordance with the Investigations Protocol established by the Compliance Committee.

In cases of medium risk notifications in which the Compliance Officer of a business has been appointed as Instructor, references hereinafter made to the Compliance Committee shall be understood to be made to the Committee of the corresponding business.

4.6. Procedural safeguards, investigative steps and general duty to cooperate

The appointed investigating officer shall take whatever steps he deems necessary to verify the veracity of the facts referred to in the communication.

Where the preliminary review of the report reveals a risk of damage, loss or any other serious event as a result of the reported facts, the Head shall submit to the Committee a proposal for the adoption of precautionary measures. Such proposed measures may include, where appropriate, and in the case of appropriate notifications classified as high risk, decisions on remuneration, such as the suspension of an employee from the variable remuneration plan.

If the Committee considers the proposal for precautionary measures to be appropriate, it shall send the proposal for the adoption of such measures to the relevant departments of the corporate areas and/or businesses affected, as the case may be.

In any investigation, all necessary measures shall be taken to prevent any form of retaliation against the whistleblower and persons or entities related to the whistleblower, in accordance with the provisions of the Policy.

Persons under investigation shall have the right to the presumption of innocence and the right to be heard and to refute any accusation using the means of evidence they deem appropriate for that purpose. Therefore, the persons under investigation shall know the facts attributed to them, without disclosing information that could identify the informant and without compromising the outcome of the investigation. In any case, in the event that the information provided to the person under investigation could compromise the confidentiality of the informant, all necessary measures must be taken to preserve such confidentiality.

The Instructing Officer shall verify the truthfulness and accuracy of the information provided and, in particular, shall verify the conduct reported, with full respect for the rights of those affected. In particular, the rights to privacy and honour of the persons under investigation shall be guaranteed.

The investigator must act proportionately and ensure that the investigation procedure is conducted independently and free from any conflict of interest, including potential conflicts of interest, and in full compliance with the provisions of this Procedure, the Policy and all other applicable internal rules.

All information, documentation, evidence, deliberations, etc. relating to the internal investigation shall be kept confidential. In this respect, only persons specifically designated for this purpose shall participate in internal investigations.

The Investigator appointed to carry out the investigation may have access through the person in charge, if he/she is a person external to the Group, to any information of the companies of the Group required for the successful completion of the investigation.

Likewise, they may, at any time during the procedure, seek the advice and collaboration of any area of the Group's companies, adopting at all times the appropriate measures to safeguard the confidentiality of the information contained in the Ethics Channel and the protection of personal data. When the instructor is a person external to the INMOCEMENTO Group, this collaboration must also be channelled through the person in charge.

All directors, officers and employees of INMOCEMENTO Group companies are obliged to cooperate loyally in the investigation. Failure to cooperate in an investigation process will be considered a breach, in accordance with the Company's internal regulations.

4.7. Formalities at hearing

The investigating officer shall grant a hearing to the persons affected by the investigation, in which they may make allegations and propose the means of evidence they deem appropriate.

The intervention of witnesses and persons concerned shall be strictly confidential. As with informants, their identity shall be preserved and the confidentiality of the facts and data of the procedure shall be guaranteed.

4.8. Deadline for the procedure

The files shall be resolved as quickly as possible and with due diligence. The maximum period for carrying out the investigation and replying to the informant shall not exceed three months from receipt of the notification or, if no acknowledgement has been sent to the informant (because the notification is anonymous, because such acknowledgement is insecure for the confidentiality of the investigation, or for any other reason), from the expiry of the period of seven days from receipt of the notification.

This three-month period may be extended up to a maximum of three additional months in duly justified cases of particular complexity.

4.9. Resolution

Once the investigation has been completed, the Instructing Officer shall issue a detailed report of conclusions, which shall be submitted through the Head, together with a proposed resolution, to the Compliance Committee, for it to adopt the decision it deems appropriate.

In the light of the content of this report, the Committee shall take one of the following decisions:

- **In case of non-existent non-compliance:**

If the facts referred to in the notification are not deemed to have been accredited or when they do not constitute: (i) an irregularity or act contrary to the Code of Ethics and Conduct or the Criminal Prevention Model, or an irregularity or act contrary to any other applicable internal regulations of particular relevance; or (ii) an act contrary to the law, an offence, a serious or very serious administrative infringement, or an infringement of European Union law, in relation to the activities provided for by law, it shall be agreed to close the file without the need to adopt any measure, lifting any precautionary measure that may have been adopted and closing the file, which shall be notified to the informant and to the persons affected by the investigation. The closure of the file on the grounds of non-compliance shall be without prejudice to the Committee being able to contact any department to discuss possible actions whose advisability has been revealed as a result of the investigation, always safeguarding the confidentiality thereof.

- **In the event of non-compliance:**

  If the existence of an infringement is deemed to have been accredited, the decision adopted shall be transferred: (i) to the HR manager of the company in question, so that the appropriate disciplinary measures may be adopted in accordance with the applicable legal or conventional regulations; and/or (ii) to the body responsible for the business in which the breach has occurred, for the adoption of corrective and/or preventive measures of an organisational and/or training nature that may be appropriate.

  In the event of an irregularity or any act contrary to the law or internal regulations that is of particular relevance pursuant to section 1 of this Procedure affecting a member of the governing body of a Group company, instead of applying the measures contemplated in the preceding paragraph, the Compliance Committee shall transfer the decision adopted to the governing body itself, through its secretary, for the application, where appropriate, of any of the measures contemplated in the company's corporate governance regulations and any others provided for by law.

  In any case, when as a result of the investigation it becomes clear that the facts accredited in the investigation could be indicative of a crime, or in any other legally established case, the Legal Department will be notified for referral to the competent authorities in accordance with the law in force in the corresponding jurisdiction.

  Likewise, the Compliance Committee, when it deems it appropriate, may transfer the file to the Legal Advisory staff so that they may assess the advisability of initiating administrative or legal proceedings of any kind.

  Finally, the Controller shall communicate the decision to the informant, within the maximum period referred to above and always adopting the appropriate measures to safeguard the confidentiality of the information and the protection of personal data.

In any event, the Compliance Committees of the businesses shall forward their resolutions to the Controller within the aforementioned deadlines.

4.10. Reporting general

The Head shall report monthly to the Compliance Committee on all activity related to the Ethics Channel and the processing of notifications and investigations and, in particular, on those specific matters in which the relevance of non-compliance could have a legal or reputational impact for the INMOCEMENTO Group.

The information to be provided to the Committee on a monthly basis shall include the following information:

- Number of total notifications received in the month.
- Number of relevant and non-relevant notifications and their timely explanation.
- Status of notifications received.
- Number of notifications resolved.

4.11. Filing of notifications and protection of personal data

The documentary support of the notifications shall be recorded in a database set up for this purpose, with access restricted to the members of the Compliance Committee and the Controller and duly protected.

This system allows for the storage and/or retrieval of key information about each report/complaint, including the date and source of the original complaint, interview results, investigation results, outstanding tasks, final resolution, the chain of custody of any evidence or key information.

With regard to the conservation of the data contained in each notification/complaint, the Data Protection regulations in force shall be complied with at all times.