



**INTERNAL INFORMATION SYSTEM
MANAGEMENT PROCEDURE
OF THE GMP GROUP**

TABLE OF CONTENTS

1	INTRODUCTION.....	3
2	OBJECT.....	3
3	COMPETENCES AND RESPONSIBILITIES	3
4	COMMUNICATIONS PROCEDURE	4
5	MANAGEMENT OF CONFLICTS OF INTEREST.....	11
6	REGISTER OF COMMUNICATIONS.....	12
7	RETENTION OF COMMUNICATIONS OR DATA PROTECTION	12
8	REVIEW AND IMPROVEMENT	12
9	APPROVAL, PUBLICATION AND ENTRY INTO FORCE.....	13

1 INTRODUCTION

This Communications Management and Whistleblower Protection Procedure (hereinafter referred to as the "**Procedure**") is mandatory for all entities that make up the Gmp Group (hereinafter referred to as the "**Gmp Group**"), in accordance with the provisions of the Internal Information System and Whistleblower Protection Policy.

This Procedure has been carried out in application of the provisions of Law 2/2023 of 20 February on the protection of persons who report regulatory infringements and the fight against corruption (hereinafter "**Law 2/2023**").

In all matters not provided for in this Procedure, Law 2/2023 shall apply.

2 OBJECT

The purpose of the Procedure is to establish the guidelines for the management and resolution of communications that may be received through the Ethics Channel (hereinafter, indistinctly "**Ethics Channel**" or "**Channel**").

The procedure regulates the management and processing of communications, information and complaints received through the Internal Information System (hereinafter "**System**"), which includes the Gmp Group's Ethics Channel. This Procedure guarantees the correct treatment of communications, the adequate protection of informants and the appropriate management of conflicts of interest.

3 COMPETENCIES AND RESPONSIBILITIES

3.1 Responsible for the Internal Information System

The Board of Directors of the Gmp Group appoints the Compliance Officer as the Head of the Internal Reporting System (hereinafter referred to as the "**Head of the System**"). He/she has the appropriate competence, integrity, authority and independence, as well as the necessary resources to perform his/her duties.

The **responsibilities attributed to the System Officer** are set out below:

- **Ensure the confidentiality of the identity of the person** who uses the Channel and chooses to identify themselves.
- **Maintain secure communication channels with the informant**, using the Channel tool or any other means that may be enabled for this purpose, depending on the circumstances.
- **Ensure that the processing, investigation and resolution of communications or complaints** are carried out in accordance with the principles and guarantees set out in the law and in the Policy, acting with full independence and impartiality.
- **Periodically report** to Senior Management and the Board of Directors, at least annually, and whenever necessary, any information required on the activity of the System, preserving in all cases the confidentiality and security of the information, as well as the other guarantees and rights of the informants.

- **Ensure the existence of a Register Book** with information on the communications received.

3.2 Channel Managers

The System Manager shall be supported and assisted by other persons who shall be called Channel Managers and who are persons within the organisation. The functions of the Channel Managers (hereinafter referred to as "**Managers**") are detailed below:

Functions of the Channel Managers

- a. Receiving and acknowledging receipt of incoming communications;
- b. Preliminary analysis of communications and coding of communications;
- c. Assisting in the investigation of the facts;
- d. Drawing up reasoned reports on the outcome of the investigations carried out, stating whether the facts reported are accredited and proposing the appropriate measures for resolving the matter, as well as, where appropriate, the disciplinary measures to be taken;
- e. Manage the Ethics Channel and liaise through it with those involved in the processing of the communications assigned to them;
- f. Resolving the doubts and queries received in Grupo Gmp in relation to the Ethical Channel;
- g. Proposing updates to the Policy and the procedures necessary to adapt the Internal Information System and the Ethical Channel;
- h. To keep the Register Book up to date with information on the communications received.

The detailed functions will correspond to the Channel Managers, who are the members of the Compliance Area, the Director of Legal and Compliance and the Director of People, Talent and Corporate Culture (hereinafter, "**D. of People**"); with respect to the matters that the Compliance Officer, as Head of the System, assigns to them. In other words, the managers will not have access to all files, but only to those whose promotion and management is entrusted to them.

In any case, any person in the Gmp Group is obliged to collaborate with the System Manager and with the Channel Managers in accordance with the terms of this Procedure.

4 PROCEDURE OF THE COMMUNICATIONS

The Gmp Group has implemented an Ethical Channel which is managed by an external tool and can be accessed from any electronic device with an Internet connection.

The purpose of the Channel is to allow any interested party to report, anonymously or not, all conduct included in the objective scope of the Internal Reporting System specified in the Policy.

The access link to the channel is located both on the website of the parent company of the Gmp Group and on the website of Las Colinas in the following easily visible and accessible locations. On entering the link, the informant will be asked to provide certain information about the facts he/she wishes to report, which must be provided in writing or by voice recording.

Once the report has been submitted, the tool will provide a password in order to establish a two-way communication between the reporter and the manager, even in those cases in which the report is made anonymously.

4.1 Receipt of the Communication

4.1.1. General considerations

The System Manager is responsible for receiving the communications, information or complaints submitted.

Once the communication, information or complaint has been communicated, it will be registered in the support tool for complaint management, assigning it a unique access code.

The submission of the communication or complaint shall generate an acknowledgement of receipt, which must be sent to the informant **within seven (7) calendar days** of receipt of the complaint, unless this could jeopardise the confidentiality of the information. By sending the acknowledgement of receipt, the informant shall be informed of the receipt of the complaint and the assigned registration number.

In the event that any information is received through a channel other than that established in the Internal Information System, the Gmp Group will guarantee confidentiality and, as far as possible, ensure that it is processed in accordance with the provisions of this Procedure.

The Channel shall have a secure, restricted-access database where all communications or complaints received, date of receipt, identification code, status and action taken shall be recorded and updated.

The personal data provided through the Channel will be processed by the Gmp Group in order to carry out any investigative actions that may be necessary to determine the existence, where applicable, of the facts that are the subject of the complaint.

The personal data that may be collected will be processed in accordance with the applicable data protection regulations and in the terms set out in section 7.

4.1.2. Special features of verbal complaints

When communications or complaints are received verbally, the System Managers shall offer the informant the possibility of formulating, ratifying, expanding or clarifying the complaint in a face-to-face meeting within a maximum period of seven (7) days from its receipt.

In this case, authorisation will be requested from the informant for the verbal communication to be recorded, informing them of the processing of their data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights.

Communication via face-to-face meeting shall be documented, subject to the informant's consent, by a recording of the conversation in a secure, durable and accessible format.

If such consent is not obtained, the communication shall be documented by a transcript of the conversation.

In the case of face-to-face communications or complaints by means of a meeting:

- The whistleblower may be accompanied, if he/she so wishes, by a lawyer or the

representative of the employees.

- To ensure due confidentiality of the research, those attending this meeting will be informed in writing of their duty of secrecy and confidentiality, as well as of all legal information on Data Protection.
- The transcript will be signed by those present at the meeting. If for any reason the informant or any of those present do not wish to sign the minutes, this shall be recorded and the proceedings shall continue.

Finally, the recording or transcript of the conversation will be attached to the Channel application and the processing of the file will continue as established in the following sections.

4.2 Assignment of Channel Manager for Communication

Once the communication, information or complaint has been registered, the System Manager shall carry out a preliminary assessment of the facts reported and the subjective elements of the complaint in order to determine the Channel manager who will process it, with the aim of avoiding conflicts of interest and ensuring the correct understanding of the alleged fact.

All Managers, by the mere fact of holding this position and being bound by this policy and procedure, are subject to a confidentiality commitment and declaration of absence of conflict of interest; therefore, if, once assigned the management of a communication, they detect that they are involved in a conflict, they must refrain from dealing with the communication and inform the System Manager so that he/she can assign the management of the communication to another Manager.

4.3 Formal Analysis of the Communication

Once the communication, information or complaint has been registered and assigned to a Manager, the latter will carry out a preliminary assessment of the facts reported and the formal elements of the complaint.

Prior to the decision to admit the complaint for processing, the manager may request the additional information required for its prior assessment. In the event that said information must be provided by the informant, the latter shall have a period of five (5) working days from the time he/she is requested to do so. Said communication shall be made via the tool or by any other means that allows for a record of the processing.

Depending on the subject matter of the communication, prior assessment of the same may be requested from other areas of the Organisation, in those cases in which the Manager considers it appropriate, keeping the identity of the informant confidential at all times (ensuring that it is not revealed, even indirectly, through the content of the consultation).

If, following the prior assessment, it is considered that the communication is related to matters regulated through specific procedures, such as the "Protocol for action in matters of sexual harassment or harassment for reasons of sex" and any other that may be agreed in the future, the External Managers of the Channel shall acknowledge receipt of the communication to the informant and shall forward it to the Commission against Sexual Harassment (**CAS**) for processing. These bodies will process these communications in accordance with the provisions of the aforementioned protocols or procedures which, in any case, will have the guarantees and deadlines provided for in Law 2/2023.

Without prejudice to the foregoing, and for greater safeguards, access to information for the prior assessment of a communication, information or complaint shall entail the signature of the corresponding confidentiality undertaking and declaration of absence of conflict of interest by

all persons accessing the same which, in any case, shall be the minimum necessary to carry out the said assessment.

Once the report has been categorised, it will be analysed in detail and it will be checked whether it contains all the necessary fields so that the corresponding investigation can be initiated. If this is not the case, or if the communication has a formal defect, a request for information will be made to the informant through the tool.

The essential information that all reports must contain is as follows:

- Location where the conduct complained of took place (workplace, travel, or any other place where the conduct complained of could have been verified within the scope of his or her professional activity).
- Description of the conduct or facts
- Time at which the conduct took place
- Identification of the alleged perpetrators, if known.

In the case of those cases in which a judicial decision or administrative proceedings are pending, the processing of the communication will be suspended, without prejudice to the investigation of the facts raised in the communication and the issuing of the relevant generic recommendations.

4.4 Admissibility of the Communication

Based on the assessment made by the Channel Manager, the System Manager shall decide whether to admit or reject the communication, information or complaint for processing. All of the above, without prejudice to the provisions of section 5. The decision to admit or reject for processing shall be notified to the informant and shall be recorded in the Channel's support tool.

The communication, information or complaint will be rejected for processing in the following cases:

- When the facts reported are not included in the objective scope of application provided for in section 2.2 of the Policy.
- When the facts reported lack plausibility.
- When the communication, information or complaint is manifestly unfounded or does not meet the minimum requirements for processing.
- Where the communication, information or complaint does not contain significant new information on infringements compared to a previous communication in respect of which the relevant procedures have been completed, unless there are new factual or legal circumstances that justify a different follow-up.
- When the purpose of the communication, information or complaint has been lost as a result of the cause of the same having been remedied prior to its admission for processing.
- When the information is already fully available to the public or constitutes mere rumours.
- The Directorate of Persons or the CAS, as the case may be, shall decide on the admission or inadmissibility of communications related to matters regulated through **procedures**

specific, such as the "Action protocol on sexual harassment or harassment based on sex".

In the event that the communication is not admissible, the System Manager shall inform the informant, informing him/her of its inadmissibility.

In case of admissibility, the decision will be communicated to the informant through the Channel tool. If this is not technically possible, the decision shall be communicated via an alternative communication channel provided.

The decision on admissibility shall include, when deemed necessary in view of the circumstances of the case, a pronouncement on the adoption of the protective measures provided for by law.

Likewise, the person who has been the subject of a communication, information or complaint, provided it is admitted, shall be informed of (i) the admissibility of the communication, information or complaint and (ii) the actions or omissions attributed to him/her. This communication shall be made within an appropriate period of time for the proper conduct of the investigation.

Exceptionally, if there is a significant risk that notifying the respondent would jeopardise the effectiveness of the investigation or evidence gathering, notification shall not take place until such risk ceases.

4.5 Investigation Phase

4.5.1 Appointment of an investigator

Admission of the complaint for processing will entail the opening of the investigation file. Once the complaint has been admitted for processing, the Manager assigned to the case will designate an investigator within five (5) working days and will request that they initiate the investigation procedure.

In general, the investigation of the investigation files shall be carried out by the Channel Managers in continuous coordination with the System Manager. However, both internal and external experts may be involved in the investigation, as well as requesting the collaboration in the investigation that is deemed pertinent.

Depending on the nature of the facts reported, and without limitation, the investigation of the case may be attributed to: the CAS or the People Department when the facts reported are linked to a breach of workplace harassment, sexual harassment, harassment based on sex, gender identity and/or sexual orientation, including in the digital sphere.

The designated instructors who do not form part of the Legal and Compliance area shall sign the corresponding confidentiality undertaking and declaration of absence of conflict of interest prior to the start of the investigation.

In any case, the System Manager shall supervise the management and investigation of the communications that are processed by the investigator appointed in accordance with the above procedure (the "**Instructor**") and shall provide them with support, assistance and advice at all times.

4.5.2 General Principles of Investigation

Throughout the investigation file, the principles and guarantees enshrined in the Internal Information System Policy shall be respected and complied with.

In any case, the designated Instructing Officer shall at all times ensure the confidentiality of the persons involved and, in particular, that of the informant, protecting their identity and may not grant any third party the right of access to the file and, under no circumstances, to the initial communication or to any other documents from which suspicion or revelation of the informant's identity may arise.

The right of defence and the right to the presumption of innocence and the honour of the persons affected by the information, complaint or communication shall be guaranteed. The person denounced has the right to know of the actions or omissions attributed to him/her by means of a brief communication of the facts and to be heard at any time, in the manner deemed appropriate to ensure the proper conduct of the investigation.

4.5.3 Instruction

The Instructing Officer will carry out all those actions or verifications that he considers necessary for the investigation of the facts reported. To this end, the following actions, among others, shall be carried out:

- **Documentary analysis.** The Instructing Officer will analyse in detail the information and documentation provided by the informant, affected person or witnesses. Likewise, he/she may request any additional information and/or documentation of a professional nature that may be necessary, always in accordance with criteria of proportionality and reasonableness.
- **Witness proceedings.** The Instructing Officer shall give a hearing to the interested parties, including in any case the informant, the affected person and witnesses. All of them must be aware of the rights, guarantees and duties of the parties.
- The interviews held shall be duly documented, either by means of a recording (upon request and authorisation of the interested party) or by means of minutes of the meeting held. In the latter case, the minutes shall be accompanied by details of the rights, guarantees and duties of the parties, signed by all those present.
- **Technical or expert opinions or reports.** At any time during the investigation phase, the investigator may request a technical opinion or report, either from other professionals of the Gmp team or from external experts in the field. These external opinions or reports must be attached to the Investigation Report.

4.5.4 Report

Once all the investigative measures and actions have been completed, the investigator will issue an investigation report, which will include, at least:

- Facts related in the communication or complaint.
- Proceedings carried out in the investigation of the case.
- Allegations made by the person complained of
- Result of the proceedings carried out
- Assessment of the facts denounced
- Conclusions

4.5.6 Time limits for the investigation

The investigation may not exceed a maximum period of three (3) months from the receipt of the communication. In cases of particular complexity that require an extension, this period may be extended by up to an additional three (3) months.

4.6 Proposed Resolution

In view of the investigation report, the Channel Manager assigned to the case shall issue a resolution proposal that shall contain, at least:

- **The communication or complaint shall be filed in** the event that, after the appropriate investigation, it is considered that the facts reported have not been sufficiently accredited, or that they do not constitute an infringement included in the objective scope of the Internal Information System. In this case, and if appropriate, it shall be agreed to forward the information to other areas of the organisation for its management.
- **The declaration of the existence of non-compliance**, in which case the following measures may be taken:
 - ✓ **Corrective action:** when the commission of any non-compliance falling within the scope of this Procedure has been accredited.
 - ✓ **Proposal for the initiation of disciplinary proceedings:** When the facts reported are likely to constitute an offence liable to disciplinary sanction, the Manager in charge of the case shall inform the D. of People for, where appropriate, the initiation of disciplinary proceedings.
 - ✓ **Referral of the information to the Public Prosecutor's Office:** When the facts may be indicative of a criminal offence, provided that no other fundamental rights are affected.
 - ✓ **Referral of information to the European Public Prosecutor's Office:** When the facts affect the financial interests of the European Union, provided that other fundamental rights are not affected.
 - ✓ **Referral to the Board of Directors** (directly or through the Audit Committee): When the facts may be indicative of a criminal offence that may affect the criminal liability of the legal person, so that it may take the decisions it deems appropriate. In this respect, the provisions of article 21 of the Board Regulations shall apply in the event of the existence of any kind of conflict of interest.
 - ✓ **Referral of the information to other competent authorities or bodies**, where appropriate, in accordance with the provisions of the regulations in force.

Regardless of whether or not the facts that are the subject of the communication have been accredited or whether or not any type of non-compliance has been evidenced, **improvement measures** may be agreed when, within the framework of the investigation, the advisability of implementing any improvement to prevent future non-compliance is detected.

4.7 Communication

At least the following communications shall be made during the processing of the dossier:

- **Communication to the informant:** In the event that the communication, complaint or information is accepted for processing, the decision will be communicated to the informant who identifies himself/herself and provides a means of communication (e-mail, telephone number, platform, etc.) or via the Channel tool within five (5) working days, provided that it does not compromise the investigation. The latter may be informed of the final decision. This is unless the person has waived the right to receive notifications. It will be understood that the person has waived this right when an unsuccessful attempt is made to contact them via Gmp.
- **Communication to the reported person:** Whoever has been the subject of a complaint, provided that it is admitted, will be informed by the Manager assigned to the case, within a maximum period of thirty (30) calendar days from the receipt of the complaint, of (i) the receipt of the complaint, (ii) the fact that he/she is accused in a succinct manner, (iii) how to exercise his/her data protection rights, for which the provisions of the Privacy Policy will apply. The latter may be informed of the final decision.

5 MANAGING CONFLICTS OF INTEREST

A conflict of interest exists when the objectivity of the decision-maker on a communication is compromised by his or her relationship with the reporter, the reported, the persons concerned or the facts.

In the event that the complaint is directed against the System Manager or any of the Managers, or there is a conflict of interest between them or any other persons who have to intervene in the processing of the file, they shall abstain from intervening in the processing and resolution of the file (except in what is appropriate in their capacity as the accused).

The conflict of interest may be:

- a) Direct, when you are the subject of the complaint.
- b) Indirect, when, without being the person reported, objectivity is at risk of being compromised for other reasons, such as:
 - The existence of a relationship of affection or kinship with the reported person.
 - Friendship or manifest enmity with the informant or the reported person or, if there are several of them, with any of them.
 - Relationship by reason of marriage or analogous relationship of affectivity or kinship with the informant or the reported person or, if there are several of them, with any of them.
 - The presence of personal interests (e.g. financial or professional development) that may be compromised by the investigation of the reported facts.
 - The existence of vicarious liability (e.g. through inaction) in relation to the reported facts.
 - The direct team relationship with the informant or the reported person.

In this case, information relating to the file shall be restricted to the person involved in the conflict of interest. In any case, the person with a conflict of interest shall notify the person with a conflict of interest.

In any case, the person involved in a conflict of interest must notify it in the Conflict of Interest Management Procedure (available in the Intranet Library).

6 REGISTER OF COMMUNICATIONS

The System Officer shall keep an up-to-date record, preferably in digital format, of the communications made and the proceedings conducted in relation to them.

The persons authorised to manage the Internal Information System may record, in the Channel management tool, the information received and the internal investigations to which they have given rise in order to ensure compliance with the requirements of Law 2/2023.

7 PRIVACY POLICY. RETENTION OF COMMUNICATIONS

In accordance with the provisions of current legislation on the protection of personal data, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights, we hereby inform you that Gmp Property SOCIMI S.A., with registered address at C/ Luchana 23, 28010 Madrid and tax identification number A-28396042, will process the personal data provided through the established complaints channel in order to clarify the reported facts.

The basis that legitimises the aforementioned processing is the public interest, based on article 31 Bis of Organic Law 10/1995, of 23 November, of the Penal Code. Exclusively in the event that an offence is detected, the data provided may be communicated to third parties (Courts and Tribunals, Security Forces and Corps or Public Administration), for the strict protection of public interests.

Personal data processed as a result of communications shall be kept for the period necessary for the purposes for which they were collected or for which they are to be further processed and, in any case, to guarantee the principle of proportionality of the processing of personal data.

In any case, the personal data processed as a consequence of the processing of a communication shall be deleted within a maximum period of three (3) months after the end of the procedure for processing the communication or, as the case may be, from the end of the disciplinary, administrative or judicial procedure to which they had given rise.

In the case of communications that have not given rise to the initiation of an investigation phase because they are manifestly unfounded or do not have the minimum essential content, the personal data relating thereto shall in any case be anonymised.

The data will be kept in the external software for a maximum period of three (3) months from the submission of the communication. After this time, if the data are necessary to continue the investigation of the facts, they may continue to be processed for the purposes of the investigation carried out.

Once the communication has been completed, personal data may be kept in the company's computer systems exclusively to guarantee the traceability, compliance and effectiveness of the system for the prevention of criminal risks implemented at Grupo Gmp.

and effectiveness of the system for the Prevention of Criminal Risks implemented in Grupo Gmp.

The rights of access, rectification, cancellation, portability and, where appropriate, opposition, may be exercised by the interested parties by writing to the registered office of Grupo Gmp at Calle Luchana, 23 Madrid (Spain), or by e-mail to the following address: [.privacidad@grupogmp.com](mailto:privacidad@grupogmp.com)

In any case, the rights of cancellation or opposition will be limited, as long as the facts communicated are being investigated or, if applicable, the exercise of judicial or extrajudicial actions, and the identity of the informant must be preserved.

8 REVISION AND IMPROVEMENT

The Procedure must be reviewed periodically, at least once a year, in order to detect possible weaknesses or points for improvement, updating and/or perfecting the contents that are considered necessary.

It shall also be reviewed in the event of any updating of regulations and/or internal business processes that may be affected by this Procedure.

In each of the revisions, Grupo Gmp must take into account, in any case, any modifications to the Penal Code and other regulations that may be applicable to the activities covered by this procedure.

9 APPROVAL, PUBLICATION AND ENTRY INTO FORCE

This procedure was approved by Gmp's Board of Directors in July 2023 and was updated in July 2025 and again in March 2026, coming into force at the same time.

The Board of Directors of Gmp promoted the approval and updating of this Procedure, thus fulfilling its function of establishing the necessary bases for an adequate and efficient management of the Internal Information System and promoting compliance with the principles and guarantees set out in the Internal Information System Policy.

This Procedure is published on the Gmp intranet and corporate website, together with the Internal Information System Policy.