PROCEDURE FOR MANAGING THE SM GROUP'S INTERNAL INFORMATION SYSTEM

1. DEFINITIONS

For the purposes of understanding the terms that will be used frequently in this document, please refer to the SM Group Internal Information System Policy.

2. PURPOSE

The purpose of this Procedure is to **provide essential regulations for the management and resolution of Communications received through the** SM Group **Internal Information System**, as a preventive mechanism for the detection and management of any issues related to the scope, compliance, and interpretation of the regulations applicable to the SM Group, as well as, in particular, any conduct that could potentially involve violations of European Union law or serious criminal or administrative offenses, in accordance with the definitions set out in section 1 of the SM Group Internal Information System Policy.

This Procedure has been developed in line with the regulations established in the SM Group Internal Information System Policy.

3. SCOPE

This Procedure is mandatory and applicable to all entities comprising Grupo SM, in accordance with the definition in section 1 of the Grupo SM Internal Information System Policy, which shall adhere to it through approval by their respective governing bodies. It is therefore applicable to all members of the organization, regardless of their position or geographical location.

This Procedure applies to all Whistleblowers, Related Third Parties, and Persons Affected by the Communication, in accordance with the definitions established in section 1 of the SM Group Internal Information System Policy. The scope of the Procedure also covers all Communications that may be raised by any Whistleblower.

In addition, this Procedure and the SM Group Internal Reporting System Policy shall apply to anything not expressly provided for in the specific harassment or other similar protocols approved by the entities that make up the SM Group.

4. MANAGEMENT PROCEDURE

4.1 RECEIPT OF COMMUNICATIONS

4.1.1 INTERNAL INFORMATION CHANNELS

The **internal information channels made available to Whistleblowers** are set out in the SM Group's Internal Information System Policy and will be visible, accessible, and secure.

In addition to the internal information channels of the SM Group System, all potential Whistleblowers are informed of the existence of external information channels, in accordance with the provisions of section 5 of this Procedure.

Communications may be made **either nominatively or anonymously**, as well as orally or in writing, depending on the internal information channel selected, with the identity and confidentiality of the Whistleblower, related Third Parties, and the Person affected by the Communication being protected in all cases.

The various **measures to** protect the parties involved in the Communication (Whistleblower, Related Third Parties, and Persons affected by the communication) are detailed in the SM Group's Internal Information System Policy.

Communications made through the tool will be **received by the System Manager**, who will process them in accordance with this Procedure.

In the event that a face-to-face or remote meeting is requested, the Communication shall be **submitted to the System Manager or the person designated by them,** who shall proceed to process it in accordance with this Procedure.

Communications received verbally shall be documented in one of the following ways:

a) By recording the conversation in a secure, durable, and accessible format, or

b) Through a complete and accurate transcript of the conversation made by the personnel responsible for handling it.

If the Communication is received by any other means (report to a superior, for example), the information must be forwarded immediately to the System Manager so that it can be processed in accordance with this Procedure.

Without prejudice to the rights to which they are entitled under personal data protection regulations, the Whistleblower will be given the opportunity to check, correct, and accept the transcript of the conversation by signing it.

Once the Communication has been received, the System Manager **shall record the information in the Register** (section 4.5. of this document).

4.1.2 PREVENTION AND MANAGEMENT OF POSSIBLE CONFLICTS OF INTEREST

The prevention and management of potential conflicts of interest may be carried out in any of the following ways:

- The SM Group may hire an external third party to investigate the report.
- Disqualification as soon as the conflict of interest of the member of the Ethics Committee affected by it is detected, with the Communication being processed by the other members. In addition, the member in conflict must maintain absolute confidentiality regarding the information received and respect all the principles and guarantees set out in the SM Group's Internal Information System Policy, as well as in this Procedure.

  In the event that the conflict of interest affects the entire Ethics Committee, a third-party investigator must be appointed.

4.1.3 ACKNOWLEDGMENT OF RECEIPT

Upon receipt of the Communication, an acknowledgment of receipt will be issued, confirming proper receipt and acknowledgment of the facts communicated. This acknowledgment of receipt will be sent within a maximum period of **seven (7) calendar days** from receipt of the Communication.

The acknowledgment of receipt will also inform you that your identity will be kept confidential and will not be disclosed to the persons affected by the Communication or to third parties.

4.2 EVALUATION

4.2.1 EVALUATION OF THE COMMUNICATION

Once the Communication has been received, **it** will be **evaluated** by the System Manager.

As part of the evaluation of the Communication, the need to take preliminary measures may be identified.

Additionally, when the Communication is considered relevant, but its content is insufficient, incomplete, or does not provide the necessary detail to initiate the investigation of the case, a notification may be sent informing the Informant of the acceptance of the Communication and requesting the necessary additional information.

Furthermore, if the Whistleblower includes information from a related third party (witnesses, for example) in the Communication, said third party must also be informed, at the time of the first communication with them or within a maximum period of one (1) month, of the relevant issues regarding personal data protection in accordance with the applicable regulations.

If there are indications of a crime, the Communication must be forwarded immediately to the Public Prosecutor's Office or the competent body.

4.2.2 ADMISSION FOR PROCESSING OR CLOSING OF THE REPORT

The reasons for admitting a communication for processing or for filing it shall be documented in **a report or minutes**, taking into account the following points:

- Descriptive information about the report, including the date of receipt.
- Data provided in the report, with a breakdown of objective and subjective data.
- Assessment of the content of the report and the reliability of the informant.
- Presentation of the information and documentation submitted with the communication.

- Preliminary measures adopted prior to the decision on whether or not to admit the Communication, in the event that they have been deemed necessary or appropriate for reasons of urgency.
- Decision on whether to accept the Communication for processing, stating, if deemed appropriate, the actions to be taken and the preliminary measures to be adopted.
- Decision on the appointment of an external third party or any other SM Group body—for example, the Ethics Officer of the corresponding country—as investigator, for reasons other than conflicts of interest and in accordance with section 4.2.3.

  In the event that the appointment of a third party—whether external or another person within the Organization itself—is made as a result of a conflict of interest with respect to the members of the Ethics Committee, this must be done as soon as it becomes known.

If the communication received is a simple query, it will be handled directly by the Corporate Director of Human Resources, who will respond to the interested party. If the Corporate Director of Human Resources is unable to respond to the query, it will be referred to the Ethics Committee for resolution in accordance with the provisions of the following sections.

4.2.3 APPOINTMENT OF AN INVESTIGATOR

Once the Communication has been assessed, the System Manager **may decide on the possibility of appointing an external third party to investigate the Communication**, taking into account the subject matter, complexity, specific needs relating to the reported infringement, and the existence of conflicts of interest.

Where appropriate, this external third party—appointed by formal resolution of the System Manager—shall proceed with the subsequent stages, with the assistance of the Ethics Delegates in each country and the departments that, in view of the specific circumstances of the case, deem it necessary.

Likewise, depending on the specific circumstances of the case, the subject matter, and the effectiveness of the investigation, the Ethics Officer of the country where the reported violation occurred may be appointed as the investigator of the Communication. In this case, a formal appointment of the System Manager is also required.

Ethics Officer of the country where the reported violation occurred may be appointed as the investigator of the Communication. In this case, a formal appointment of the System Manager is also required.

In the event that, due to a conflict of interest, it is necessary to remove any of the members of the Ethics Committee from the investigation of a Communication, their recusal must be documented by means of a formal resolution as soon as it becomes known.

The decision on the recusal of any member of the Ethics Committee shall be made by the Corporate Director of People as the person individually designated as System Manager within the collegiate body, after deliberation with the remaining members.

In the event that the conflict of interest affects the Corporate Director of People and he or she does not recuse himself or herself *voluntarily*, his or her recusal may be agreed upon by all the remaining members of the Ethics Committee.

4.3 PROCESSING

4.3.1 PRINCIPLES OF COMMUNICATION HANDLING

The Organization has implemented a procedure for investigating Communications that guarantees professionalism, fairness, and impartiality, as well as their management by qualified personnel (the System Manager).

In the event that the Communication is sent by any other means, or to Members of the Organization not responsible for its processing, these principles are also guaranteed, and the Communication will be forwarded immediately to the SM Group System Manager.

4.3.2 INVESTIGATION OF THE CASE

Once the Communication has been accepted for processing, the Informant (and, where applicable, related Third Parties) has been notified of this circumstance, and the corresponding file has been opened, its **investigation** will be carried out in accordance with criteria of impartiality, specialization, and knowledge of the subject matter.

The investigation will be aimed at obtaining sufficient evidence to resolve the case and prepare the corresponding investigation report and conclusions.

The person affected by the communication will then be informed of the processing of their personal data, as well as the actions or omissions attributed to them, within a reasonable period of time once the data has been obtained, and no later than one (1) month from receipt of the communication, unless the aforementioned period must be extended for justified reasons to ensure the successful completion of the investigation.

In addition to the information relating to the protection of their personal data, the person affected by the communication will also be provided, verbally or in writing, with a summary of the facts for which the investigation is being carried out so that they can provide any explanations they deem appropriate and submit any evidence they deem necessary to support their position regarding the facts under investigation.

The person affected by the communication shall enjoy the rights, guarantees, and protective measures established in the SM Group's Internal Information System Policy. Specifically, they shall have the right to be heard at any time, adjusting the channels in a timely manner, as deemed appropriate to ensure the successful outcome of the investigation.

Similarly, Grupo SM must guarantee at all times the confidentiality of the Whistleblower and the absence of reprisals for Communications made in good faith. Therefore, the identity of the Whistleblower will be excluded from the information provided to the Person affected by the Communication in the exercise of their right of access or, where appropriate, from any circumstances that could make them identifiable to the Person affected by the Communication.

The designated investigator shall be responsible for verifying the truthfulness and accuracy of the facts and information contained in the Communication and, in particular, the conduct reported, in order to verify the existence of a violation within Grupo SM. To this end, they shall have the power to conduct interviews with the Whistleblower, the Person affected by the Communication, and related Third Parties.

The designated investigator shall have the authority to carry out as many investigative procedures as deemed necessary, respecting the rights of those affected and documenting their actions in the Registry Book.

In line with the above, the investigator may maintain communication with the informant and, if deemed necessary, request additional information.

The investigation sessions and interviews conducted in the course of the investigation shall be recorded or, if not authorized by any of the participants, minutes shall be taken.

4.4 CONCLUSION

4.4.1 ISSUE OF THE REPORT ON THE COMMUNICATION

Once the previous phase has been completed, the investigator shall prepare an **investigation report and conclusions**, which may contain any of the following information:

- Descriptive information about the Communication, including its unique identification number and date of receipt, as well as the internal information channel used.
- A statement of the facts as reported.
- The classification of the Communication.
- The actions taken to verify the veracity of the facts.
- The conclusions reached in the investigation and the assessment of the proceedings and the evidence supporting them.
- Proposed action in accordance with the terms established in section 4.4.1 of this Procedure.

The report with the proposed action drawn up by the System Manager shall be sent to the relevant bodies or individuals within Grupo SM, depending on the proposed action agreed upon.

In the event that it has been prepared by a person or body other than the System Manager, the report shall be sent to the latter, who shall then forward it to the relevant bodies for them to decide on the proposed action.

Once an infringement has been committed, the Organization shall:

- Take appropriate measures to resolve the violation and monitor the effectiveness of those measures.
- Administer appropriate sanctions (disciplinary or contractual) that are legitimate and proportionate to the reported facts.
- Promote the referral of matters to the relevant authorities, where appropriate, and monitor the results of the decisions taken.
- Record and document the actions agreed upon in the Register.

The System Manager shall notify the Whistleblower and the Person affected by the Report in writing and in a reliable manner of the completion of the investigation, indicating whether or not a violation has occurred.

Subsequently, the file will be blocked to prevent further processing.

4.4.2 MAXIMUM TIME LIMIT FOR RESOLUTION

The maximum time limit for responding to investigative actions may not exceed **three (3) months** from receipt of the Communication, except in cases of particular complexity that require an extension of the time limit, in which case it may be extended for a maximum of three (3) additional months.

Communications that have not been processed may only be recorded in anonymized form, without the obligation to block them as provided for in the regulations on personal data protection. In any case, if three (3) months have elapsed since receipt of the Communication without any investigation having been initiated, it must be deleted, unless the purpose of its retention is to leave evidence of the functioning of the System.

4.5 REGISTRY BOOK AND PROTECTION OF PERSONAL DATA

The Register is a database with high-level security protection, in which all communications received are recorded, as well as any decisions and/or actions taken in relation to them. It is the tool that the System Manager will use to organize and document the performance of their duties.

Personal data relating to the information received and internal investigations will only be kept for as long as is necessary and proportionate.

In particular, the following aspects and time limits shall be taken into account:

- The data being processed may be stored in the information system only for the time necessary to decide whether to initiate an investigation into the reported facts. If it is proven that the information provided, or part thereof, is not true, it must be deleted immediately upon discovery of this circumstance, unless such lack of truthfulness may constitute a criminal offense, in which case the information will be kept for the time necessary for the legal proceedings to be processed.
- In any case, if three (3) months have elapsed since the receipt of the Communication without any investigation having been initiated, it must be deleted, unless the purpose of its retention is to leave evidence of the functioning of the system. Communications that have not been acted upon may only be recorded in anonymized form.
- Under no circumstances may the data be kept for a period exceeding ten years.

Access to personal data contained in the internal information system shall be limited, within the scope of their powers and functions, exclusively to:

a) The System Manager and the person directly managing the file.
b) The head of human resources or the duly designated competent body, only when disciplinary measures against an employee may be warranted.
c) The head of the legal services of the entity or body, if legal measures are to be taken in relation to the facts reported in the communication.
d) The data processors who may be appointed.
e) The Organization's data protection officer, where applicable.

The processing of data by other persons, or even its communication to third parties, shall be lawful when necessary for the adoption of corrective measures within the

entity or the processing of any applicable disciplinary or criminal proceedings.

Under no circumstances will personal data that is not necessary for the knowledge and investigation of the actions or omissions referred to in the scope of application of the regulation be processed, and, where appropriate, it will be immediately deleted. Likewise, any personal data that may have been communicated and that refers to conduct not included within the scope of application of this Procedure and the SM Group's Internal Information System Policy shall be deleted.

If the information received contains personal data included in the special categories of data, it will be deleted immediately, without being recorded or processed.

5. EXTERNAL INFORMATION CHANNELS

Notwithstanding the existence of this internal reporting system, interested parties have the right, if they deem it appropriate, to submit the corresponding communications to the competent authorities in their territory.

In order to comply with Spanish regulations on whistleblower protection, all potential whistleblowers are hereby informed of the existence of external reporting channels, including, but not limited to, the following:

- External reporting channel of the Independent Whistleblower Protection Authority (A.A.I.): Information on other external reporting channels - proteccioninformante.es
- AEPD: https://www.aepd.es/es/preguntas-frecuentes/13-reclamaciones-ante-aepd-y-ante-otros-organismos-competentes/FAQ-1301-como-puedo-interponer-una-reclamacion-si-han-vulnerado-mis-datos-de-caracter-personal
- Treasury: https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/paginas/comunicacionsnca.aspx
- Catalonia Anti-Fraud Office: https://denunciesanonimes.antifrau.cat/#/?lang=es

6. CONSEQUENCES OF NON-COMPLIANCE

All persons covered by this document are obliged to comply with its contents. In the event of a serious breach being identified, the SM Group's internal information system is the preferred channel for reporting the infringing action or omission.

When such a breach is investigated and confirmed, disciplinary measures (in the workplace) or contractual measures (in commercial relations with third parties) will be taken that are considered proportionate to the risk or damage caused.

The measures adopted from an employment perspective will comply with applicable regulations, without losing their forcefulness or proportionality to the seriousness of the events that gave rise to them, informing the workers' legal representatives if appropriate.

In the event that the accusations described in the Communication are determined to be false or malicious, to the extent that they have been made deliberately, with knowledge of their falsity or recklessly, they will be considered a serious breach of the SM Group's Internal Information System Procedure and Policy.

Based on the above, when there is sufficient evidence or when actual and effective breach of any of the provisions contained in the Procedure or Policy of the Internal Information System has been demonstrated, Grupo SM shall be entitled, in compliance with the applicable labor regulations in the case of employees, and the contracts signed in the case of professionals, to take any of the actions listed below, with the ultimate aim of ensuring compliance with both documents:

- Request that the employee or professional permanently cease the activity that led to the breach of this procedure.
- Access, block access, interrupt the connection, and recover devices, equipment, and other technological means of the corporate network that have been used

or are being used by employees or professionals for the performance of their work or the provision of their professional services.

- Terminate the employment or service contract signed with the professional, in accordance with current regulations and without prejudice to any claim for damages incurred as a result of such breach.
- Grupo SM may take all disciplinary measures applicable to the specific case, taking into account the type of breach that has occurred and the consequences of said breach for Grupo SM, which may constitute disciplinary dismissal, without prejudice to any damages caused as a result of said breach.
- Grupo SM is authorized to take all legal action it deems appropriate, in accordance with current legislation, arising from the employee's or professional's breach of this Procedure.

7. ADVERTISING

This Procedure is available to all Members of the Organization through its publication on the employee portal, in the "Information, documents, and procedures" section, under "Policies and procedures."

People Space

Similarly, Grupo SM may, if it deems necessary, make this Procedure available to Third Parties by publishing it on the following internal information channel:

https://whistleblowersoftware.com/secure/smcanalinterno

8. ENTRY INTO FORCE AND MODIFICATIONS TO THE PROCEDURE

The SM Group Internal Information System Management Procedure shall enter into force on the day following its approval.

This Procedure will be reviewed if possible improvements are identified or if regulatory, organizational, or any other changes occur that justify such a review.