CORPORATE CRIMINAL LIABILITY

COMPLAINTS AND INFORMATION MANAGEMENT PROCEDURE OF THE INTERNAL INFORMATION SYSTEM CHANNEL

Document generated by _____

ELABORATED	REVISED	APPROVED
Compliance Officer	Responsible S.I.I.	Board of Directors

INDEX

.

GESTAIR GROUP COMPLAINTS AND INFORMATION MANAGEMENT PROCEDURE .

Compliance

1. Objective

The purpose of this document is to regulate the procedure to be applied to communications received through the Gestair Group's internal information channels, within the scope of application of the Gestair Group's Internal Information System General Policy ("IIS General Policy").

The drafting of this Information Management Procedure was approved, together with the IBS General Policy, by the Board of Directors of the parent company of the Gestair Group in November 2023.

Scope of application

The SII is the preferred channel for reporting the actions and omissions listed in the SII's General Policy, provided that the violation can be dealt with effectively and if the whistleblower believes there is no risk of retaliation.

In all proceedings and investigations, the rights to privacy, defense and the presumption of innocence of the persons under investigation shall be guaranteed.

The procedure shall be transparent and the right to information of those involved shall be guaranteed, which they must necessarily know:

- The very existence of this procedure and the SII's general policy.
- The processing of the data involved in the formulation of the complaint.
- The possible consequences that the complaint may have for the defendant.

Access to data received through the Internal Information System is limited to the persons indicated in the Gestair Group's Internal Information System Policy.

The confidentiality of the processing of the files will be guaranteed, as well as the identity of the persons involved, which may not be communicated or revealed without their consent.

Of all investigative actions, and in particular of the interviews and explanations given by the persons related to the reported event, written minutes shall be taken at the same

meeting and shall be duly signed by the person entrusted with the investigation, offering the interviewee the opportunity to verify, rectify and accept the transcription of the conversation by signing it.

3. Whistleblowing

Any informant may make use of the following internal information channels:

- Through the Gestair Group's SII platform, available through the Whistleblower Channel link at the bottom of the Gestair Group's corporate website and on the Gestair Group's Employee Portal (whistleblowersolfware).
- Sending a written communication to the Whistleblower Channel to the following e-mail address dpd@gestair.com.
- Sending a written communication to the Compliance Officer, Responsible for the SII to the following postal address: Compliance Officer, Grupo Gestair, calle Anabel Segura, nº 11, 28108 Alcobendas, Madrid, Spain.
- At the written request of the informant, a complaint may also be filed by means of a face-to-face meeting within seven days of receipt of the request.

Complaints may be made in accordance with the principle of anonymity as indicated in the SII.

In the event that an employee, collaborator or person related to the Gestair Group who is not responsible for the processing of information receives a communication regarding the commission of an infringement, he/she must immediately redirect it to the System Manager via the e-mail address indicated, maintaining the confidentiality of the communication and/or anonymity of the informant. Breach of confidentiality is classified as a very serious offence under Law 2/2023.

In any case, the complaint must be made in good faith and include the following information:

Complete the required fields of the SII platform.

When the complaint is made by e-mail, postal mail or any other channel, it must contain, at least, the following information:

(i) Fact denounced: arguments and, if applicable, truthful and accurate evidence on which the complaint is based,
(ii) Reported: name of the person and position or group reported;

(iii) In those cases where anonymous reporting is not chosen, indication of the name and department of the informant.

Upon receipt of the report, the IBS Manager will send to the informant within seven (7) calendar days acknowledgement of receipt of the report, indicating an entry number assigned to the report together with the date of receipt.

Within a period not to exceed seven (7) calendar days from the sending of the acknowledgment of receipt by the person in charge of the SII, it will be determined whether or not to process the complaint, paying special attention to the following criteria:

No complaint will be admitted for processing if it lacks all plausibility, is not within the competence of the SII, is unfounded or there are indications that the information was obtained through the commission of a crime or does not contain new or significant information.

In these cases, the whistleblower will not enjoy the appropriate protection guarantees, as indicated in the SII Policy.

After a period of ten (10) calendar days from receipt of the complaint, the person who made the complaint may be asked to clarify or supplement it, providing such documentation and data as may be necessary, in order to assess whether or not it is admissible.

If there is any circumstance related to a communication that may imply for the IBS Officer, or for the members of the OIC, a conflict of interest or that in any way affects or may affect their neutrality or independence, before deciding to admit it for processing and, in any case, no later than five (5) calendar days following the date of receipt of the complaint, must refrain from taking any decision and immediately inform the other members of the OCI or, when they are in the same situation, the Management Committee of the Gestair Group.

In this case, the Management Committee, excluding those members who may also have a conflict of interest, shall be responsible for deciding, within the aforementioned time limits, whether to admit the complaint for processing, as well as for appointing a person for the subsequent processing of the case who meets the appropriate requirements of neutrality and independence.

The complainant must be informed of the final decision to reject a complaint, using secure means that guarantee receipt of the information by the informant.

If the complainant provides data of a third party other than the respondent (e.g., witnesses), the third party must also be informed of the processing of the data and the origin of the data, in accordance with the provisions of the SII Privacy Policy.

In addition to the foregoing, when the facts reported by the informant could be indicative of a crime, at the discretion of the Head of the Information System, he/she shall immediately refer the reported facts to the Public Prosecutor's Office. In the event that the facts affect the financial interests of the European Union, they shall be referred to the European Public Prosecutor's Office.

4. Instruction

Once the complaint has been admitted for processing, the person in charge of the SII shall:

Instruct the corresponding contradictory file or designate a person responsible for the investigation of the file, who may be a person from the Gestair Group not affected by the file or an external person if the circumstances so require.

The person in charge of the investigation shall verify the truthfulness and accuracy of the information contained in the complaint and, in particular, of the conduct denounced, with respect for the rights of the affected parties. For these purposes, he/she will give a hearing to all the affected parties and witnesses and will carry out as many diligences as he/she deems necessary.

All Gestair Group employees are obliged to cooperate loyally in the investigation. The intervention of witnesses and affected parties shall be strictly confidential. This process shall be carried out, as far as possible, maintaining the anonymity of both the accused and the complainant, as well as the reasons for the complaint.
Any person involved in the research will be asked to sign a confidentiality agreement or, if applicable, a data processing agreement, prior to the support provided.

Likewise, when necessary, the IBS Manager will inform the Management Committee in order to adopt the appropriate measures to eliminate or mitigate the risk and its consequences based on the available information and applying in any case the necessary precautions inherent to this pre-investigation phase.

There is no standard procedure for the conduct of the investigation, which will depend on your particular circumstances. However, a precautionary principle will be applied, in

order to avoid the risk of extending possible regulatory breaches, destruction of evidence, litigiousness, reputation, loss of assets, etc.

It shall be ensured that the person affected by the reported facts has notice of the same once the complaint has been admitted for processing, as well as of the facts related in a succinct manner. In addition, he/she shall be informed of his/her right to submit written allegations and of the processing of his/her personal data. However, this information may be delayed if it is considered that its provision in advance could facilitate the concealment, destruction or alteration of evidence. In any case, this period shall never exceed thirty (30) calendar days from the date the complaint is admitted for processing.

In no case will the identity of the informant be communicated to the subjects concerned, nor will access to the communication be given.

During the investigation, notice of the communication with a succinct account of the facts will be given to the investigated party. This information may be provided during the hearing if it is considered that its prior provision could facilitate the concealment, destruction or alteration of the evidence.

The hearing, which shall be held within thirty (30) days following the admission of the complaint for processing (unless justified reasons, based on the complexity or the number of proceedings to be carried out, make it advisable to extend the term for the time strictly necessary), shall include in any case and without prejudice to the possibility of submitting written allegations, a private interview with the person denounced or allegedly responsible for the irregularity in which, respecting the guarantee of the presumption of innocence, he/she will be informed of the facts that are the subject of the file, will be invited to give his/her full version of the facts, will be allowed to provide the relevant evidence and will be asked the appropriate questions depending on the circumstances of the case and the facts denounced.

Likewise, all affected parties shall be informed about the processing of their personal data, as well as to comply with any other duty required by the legislation on the protection of personal data.

If at any time there is a Works Committee in the Gestair Group or any of the companies that form it, and the accused is a member of the Works Committee or personnel delegate or is a union delegate, he/she will be consulted on the granting of a hearing to the remaining members of the Works Committee, personnel delegates or union delegates, if any. In any case, the provisions of the applicable regulations on the matter shall be complied with.

5. Resolution of files

Once the investigation of the case has been concluded and within a maximum period of thirty days, the person in charge of processing the case will submit it together with a resolution proposal to the person in charge of the SII so that he/she may decide what he/she deems appropriate.

The maximum time limit for responding to the investigation proceedings may not exceed three months from the receipt of the communication or, if no acknowledgement of receipt was sent to the informant, three months from the expiration of the seven-day period after the communication was made. In cases of particular complexity requiring an extension of the time limit, this may be extended for a maximum of three additional months.

In the event that the resolution issued concludes that a Gestair Group Employee has committed an irregularity, said resolution shall be transferred to the Human Resources Department for the application of the appropriate disciplinary measures and, where appropriate, to the competent authorities for the purpose of initiating the pertinent administrative or judicial proceedings.

Additionally, in such a case, the Management Committee and Board of Directors will be informed with the recommendations it deems appropriate to improve the Gestair Group's Code of Ethics and the Gestair Group's Crime Prevention Program.

6. Information on external reporting channels to the competent authorities.

The following is clear and accessible information on the main external reporting channels to the competent authorities and, where applicable, to the institutions, bodies, offices or agencies of the European Union.

Any natural person may report to the AAI. Independent Authority for the Protection of the Informant or before the corresponding regional authorities or bodies of any actions and omissions provided for in Law 2/2023.

- Money laundering related offenses
- Labor Inspection and Social Security
- Complaints channel of the Ministry of Consumer Affairs
- Ministry of Industry, Commerce and Tourism
- Infringements derived from data protection regulations, AEPD. Spanish Data Protection Agency

7. Disciplinary regime

The violation of any of the rules, procedures, policies, instructions, orders or mandates of the Gestair Group within the scope of its Code of Ethics of the Gestair Group, its Crime Prevention Program or its SII by any Employee to whom they are applicable, will imply an infraction. In such a case, the Gestair Group Disciplinary Regime shall apply.

Infringements and, if applicable, penalties shall be determined in accordance with the applicable general regulations and the regulations of the Gestair Group.

These sanctions are of a disciplinary nature and are contemplated independently of the sanctions provided for in the applicable labor regulations, as well as the possible civil and criminal actions that may arise, so that the Board of Directors, through the Compliance Officer and Head of the SII, reserves the right to report the person who violates the rules to the competent authorities and/or to exercise the appropriate legal actions before the Courts of Justice.