# Internal Information System Management Procedure

14 December 2023

# TABLE OF CONTENTS

# 1. Introduction and objective

The Code of Conduct is the policy framework that sets out the criteria of conduct and principles of action to be followed by the companies of the Gestamp Group (hereinafter '**Gestamp**' or the '**Group**'). This document is intended to be the backbone of our commitment to integrity and a reference for anyone who is unsure about what they are expected to do in a given situation. Our culture includes strict respect for the law and the rights and interests of third parties, the environment and safety at work.

The Code of Conduct applies to all organisational departments and affects all members of the governing bodies, **management** and all employees contractually bound to any of the companies within the Group that **comprise Gestamp Automoción, S.A.** and the companies in which it has a controlling interest.

Gestamp has an Internal Information System ('**IIS**'), which encompasses the different communication channels (the '**Channels**') available in the Group to report any suspected breach of current legal regulations, as well as of the Code of Conduct and other internal regulations by members of the governing bodies, management or employees **of Gestamp**. Moreover, the Channels can be used to ask questions about the proper interpretation of the Code of Conduct and other internal regulations, or to suggest improvements to their content.

The IIS Policy details the scope of application, the existing Channels, the general principles and the safeguards of the IIS, particularly regarding the protection of whistleblowers and affected persons.

The purpose of this procedure (the **'Procedure**') is to govern the handling of communications submitted through the IIS Channels, from the sending, receipt and recording of them, to their processing, the investigation of the reported events and their resolution.

The Group is utterly committed to maintaining the absolute confidentiality of all information received and managed through the Channels, and not to carry out any act of retaliation against any person who, in **good faith**, discloses an inappropriate act by a Gestamp employee.

# 2. Scope of application

This Procedure applies to any person who wishes to (i) ask questions about the interpretation of the Group's internal rules or suggest improvements to their content or (ii) report any suspected breach of the external or internal regulations that apply to the Group ('whistleblowers' or 'reporting persons'). In any case, the following may have whistleblower status:

- Members of the governing bodies, management and employees of any of the companies that make up Gestamp.
- Self-employed workers.
- Volunteers, interns, trainees, regardless of whether or not they receive remuneration, as well as those whose employment relationship has not yet begun, in cases where the information about a violation has been obtained in the course of the selection process or pre-contractual negotiations.
- Any person, natural or legal, who has had, has or may have a relationship with or interest in Gestamp, (hereinafter '**Third Parties**').

It also applies to all persons involved in handling communications received through the Channels and to the reported or affected persons.

Definitions

COMMUNICATION. Any information received through the Channels, including questions, queries or suggestions regarding internal or external regulations and reports of possible breach of internal or external regulations.

AUDIT COMMITTEE. Committee of the Board of Directors whose responsibilities include supervising compliance with the Group's Code of Conduct and the operation of the Channels.

ETHICS COMMITTEE. A collegiate body appointed by the Board of Directors of Gestamp Automoción, S.A. as the Group's IIS Manager, whose duties include ensuring the correct management and implementation of all action carried out in relation to the investigation of reports received through the IIS. The Ethics Committee carries out its functions independently and autonomously.

COMPLIANCE OFFICE. Reporting directly to the Ethics Committee, the compliance office is in charge of managing the IIS in terms of both the receipt of communications and investigations.

REPRESENTATIVES. They are present within the Group's organisational departments and carry out their duties in coordination with the Ethics Committee, reporting to said committee.

REPORT. Any information received through the IIS regarding an irregularity or breach of the Group's rules.

REPORT IN GOOD FAITH. A report made truthfully and in good faith, without providing unclear, false or inaccurate information.

REPORT IN BAD FAITH. When the reporting person is aware that the report is false or they act with clear disregard for the truth.

REPORTED PERSON. Person about whom a report is made, who may be responsible for an irregularity, violation or breach of prevailing law or Gestamp's internal regulations.

CASE REPORT. Document summarising the events reported, the means and resources used in the investigation, where appropriate, as well as the conclusion reached in order to carry out the relevant measures.

INVESTIGATOR. Person appointed by the Compliance Office to investigate the events reported through the Channels. In most cases, the role of investigator is carried out by a Representative.

RECORD. Document containing the fundamental details of communications made via the Channels.

IIS MANAGER. The Ethics Committee is the body appointed by the Board of Directors of Gestamp Automoción, S.A. to oversee the Group's IIS.

# 3. Bodies involved in managing the Channels

## 3.1. Ethics Committee

Manager of the IIS whose core functions are to ensure compliance with the Code of Conduct, coordinate the mechanisms for preventing breaches and establish the means necessary for processing communications made, in line with what is set out in this procedure.

## 3.2. Compliance Office

The compliance office reports directly to the Ethics Committee. It can perform as many functions as delegated by the Ethics Committee. It promotes the proper operation of training plans, document management, the reporting system and internal investigations.

## 3.3. Representatives

HR managers that work within Gestamp's organisational departments. They are responsible for managing any communications received, including those made via the Channels.

## 3.4. Investigators

Depending on the type or seriousness of the events reported, other employees of the Group, department representatives or third-party experts may be requested to collaborate in the investigation.

# 4. Management process of the Channels

## 4.1. Sending and reception of reports

Gestamp provides details of the different ways of accessing the Channels that can be easily accessed within its intranet and on its website.

Anonymous reporting is accepted within Gestamp. If identification details are provided voluntarily, they will be kept confidential throughout the entire process.

### 4.1.1. Channels

Gestamp's available Channels are as follows:

- Gestamp employees can make the communications set out by this Procedure by speaking to their line manager or HR representative of their organisational department, either verbally or in writing. Reporting persons may also verbally request an in-person meeting with the Compliance Office and/or corresponding HR representative in order to report or ask questions. This meeting must take place within a maximum of 7 days, and the reporting person will be notified about the processing of their personal data by means of the annexed document *Annex 1*.
- In-person or online meeting: reporting persons may also verbally request an in-person meeting with the Compliance Office and/or corresponding representative, in order to report or ask questions. This meeting must take place within a maximum of 7 days, and the reporting person will be notified about the processing of their personal data by means of the document attached as *Annex 1*.

  In both cases, verbal communications will be documented in one of the following ways:

  - via a recording of the conversation in a secure, permanent and accessible way, provided that the reporting person is warned in advance that their communication will be recorded, is informed of the processing of their data by means of the document attached as *Annex 1* in accordance with applicable law, and they provide their consent, or
  - by means of a full, accurate transcription of the conversation conducted by the staff member responsible for processing it. In this case, the transcription will be provided to the whistleblower to verify, amend and accept the information by signing the transcription of the conversation, and they will be informed of the conditions regarding the processing of their personal data by means of the document attached as *Annex 1*.
- Corporate mailbox: Gestamp provides the following e-mail address: *corporatecompliance@gestamp.com*.

- SpeakUp Line external channel: online tool in the form of a specialised IT platform that can be accessed the via the Gestamp website and intranet, available in all the Group's languages:
  - Intranet: https://intranet.gestamp.com/group/code-of-conduct
  - Website: https://gestamp-speakup.i2-ethics.com/#/

This platform offers different options for making communications, which are:

- Online form: The reporting person will receive confirmation of receipt of their communication within a maximum of 7 calendar days from the reception of the report. The reporting person will be notified about the processing of their personal data via the online form itself.
- Free telephone service available 24 hours a day, 7 days a week in English and Spanish.
- Free telephone service available during working hours for other Gestamp languages.
- Call back system where the reporting person fills out an online form with their contact details, the language in which they wish to receive the call, and the preferred time to be called by the external channel, SpeakUp Line.
- In the cases involving a telephone call, the reporting person will be warned in advanced that they will be recorded and notified about the processing of their data in line with applicable law.

- By post to the following address:

  FAO: Corporate Compliance
  Calle Alfonso XII, 16,
  28014 – Madrid (Spain)

If the communication is sent through a channel other than the Channels established in this Procedure, the confidentiality of the information is guaranteed in all cases, and it will be processed in a secure environment in accordance with legal requirements on personal data protection. Notwithstanding access to the internal Channels referred to in this Procedure, the whistleblower may at any time contact the Independent Authority for Whistleblower Protection (AAI, its Spanish acronym) or the corresponding regional authorities or bodies, to report the commission of any act or omission included in the scope of application of Spanish Law 2/2023, EU Directives or local regulations.

### 4.1.2. Contents of communications

All communications and reports should include the following information in order to facilitate understanding and potential handling:

- Identity of the reporting person when the report is made confidentially but not anonymously. This includes the name and surname(s) of the reporting person and their e-mail address.
- Group company in which the reported event is being or has been committed.
- A clear, concise, objective description of the events being reported or of the questions/suggestions raised, together with any elements of evidence needed to support what is described in the report. Only where necessary should the details of third parties be provided.
- If applicable, the reason why the reporting person considers the events reported to be irregular.

A lack of information in a communication may make it difficult to understand and process. In the event that the communication contains insufficient details in order to be processed, the case will be 'dismissed'.

### 4.1.3. Recording of the communication

Once the communication or report has been received, regardless of the Channel used, an identification code will be assigned and the report will be securely and confidentially recorded in the SpeakUp Line tool, with restricted access for authorised persons only.

Each communication or report is classified in one of the following categories, according to the nature and seriousness of the events reported:

Breach of the Code of Conduct.

- Questions as to the interpretation of internal regulations or suggestions for their improvement.
- Public procurement.
- Services, products and financial markets, and anti-money laundering and terrorism financing.
- Product safety and compliance (quality).
- Transport safety.
- Protection of the environment, conduct against the environment and natural resources.
- Protection against radiation and nuclear safety.
- Food/animal feed safety, animal health and welfare.
- Public health.
- Privacy and personal data protection, security of networks and information systems.
- Eu's financial interests (tax fraud).
- Internal market (subsidies and aid, anti-competitive practices).
- Serious/extremely serious criminal or administrative violations.

### 4.1.4. Safeguards for the whistleblower acting in good faith

RETALIATION PROHIBITED. Nobody who makes a report of wrongdoing in good faith shall be subject to retaliation (including threats or attempts of retaliation). Retaliation is understood as any act or omission prohibited by law, or that directly or indirectly results in unfavourable treatment that places the individuals concerned at a disadvantage compared to another in the employment/professional setting, solely because they have used the IIS Channels.

A report of a breach made in good faith and in accordance with this Procedure does not constitute the disclosure of a trade secret.

With a view to disciplinary action, the Ethics Committee has the power to investigate any form of retaliation, including any threat, discrimination, harassment or other kind of formal or informal negative measure placed on the reporting person or people close to them by a Gestamp employee.

A report of a breach made in good faith and in accordance with this Procedure does not constitute the disclosure of a trade secret.

Anyone making a report in bad faith may be disciplined by the Group, independently of any criminal or civil liability that might derive from their actions.

CONFIDENTIALITY: The identity of the whistleblower and any third parties mentioned in the report will be protected as confidential, as will details of the actions carried out in the handling and processing of the report,

unless there is a legal obligation to disclose said information, provided that there is the express consent of the whistleblower or of the persons mentioned in the report.

#### 4.1.5. Rights of the reported person

During the processing of the case, the person reported has the right to the presumption of innocence, to exercise their defence and to the same protections provided for whistleblowers, keeping their identity confidential and ensuring the confidentiality of the events and details of the procedure.

To this end, a brief account of the events under investigation shall be provided to the person in question so that they may prepare their defence, provide evidence and make any submissions deemed necessary. The handling of communications must be carried out with the utmost respect for the reputation of the person reported and the presumption of their innocence. If report is false, the person reported has the right for this to be stated in the record of reports.

In no case shall the personal details of the whistleblower be disclosed to the person reported.

Where the case so requires, the person reported may testify with the support of a lawyer, and their confidentiality will be ensured to prevent retaliations. Their identity will only be disclosed where legally required.

### 4.2. Admission for processing

When a report of an irregularity is received, or when there are indications of such irregularity by any other means, it will be looked into and, if necessary, investigated. If a report is clearly implausible, lacking in good faith or are dismissed for lack of information which is requested but not provided, only then may the case file be closed without investigation, leaving a record of this fact and the reasons that support it.

In order to verify the credibility of a report and to protect the reputation of the persons mentioned in it, the competent investigative body may conduct a preliminary investigation before deciding whether to admit or close the report.

The Compliance Office decides who is in charge of conducting the investigation, whether internal or external to that body, ensuring in all cases that the investigator is not subject to any conflict of interest and has the required training to carry out the investigation.

- When the report refers to breaches of the rules contained in Gestamp's Code of Conduct, it will be sent to the Representative of the corresponding organisational department, who will be responsible for carrying out the investigation and proposing the appropriate resolution and measures in compliance with the provisions of the Collective Bargaining Agreement or applicable regulations.
- Communications received that refer to matters other than those mentioned in the above points will be handled by the Compliance Office, if necessary, with the assistance of other employees or departments that may need to be involved in the investigation.
- If the complexity of the matter so requires, the Investigator may be required to submit an investigation plan and an investigation team to the Ethics Committee, ensuring respect for the rights and safeguards of the persons under investigation in all cases. The Ethics Committee may require this in investigations within the competence of the Compliance Office and Representatives. The Compliance Office may do the same with respect to investigations of Representatives.

## 4.3. Investigation

The investigation includes all those actions aimed at verifying the veracity of the events reported and whether they constitute a breach of external or internal regulations.

### 4.3.1. Precautionary measures

At the start of or during the investigation, the Investigator (or prior to their appointment, the Compliance Office) may adopt precautionary measures to secure evidence or to prevent harm derived from the reported act or its repetition.

Precautionary measures may include:

- the suspension of rights of access to computer equipment, documents or company premises or facilities;
- the auditing of computer equipment;
- authentic copies of computer files;
- suspension of the activity of the person under investigation;
- suspension of a particular type of activity.

These measures must be useful and appropriate to their ends, and must not cause greater harm than that which is intended to be prevented by the investigation.

### 4.3.2. Means of investigation

The Investigator may have access to all company premises, offices, files and documents, where this is necessary for the investigation and proportionate to its ends.

Means of investigation may include:

- interviews with the persons reported to be behaving irregularly,
- interviews with company employees or external parties,
- requests for reports from company departments or external experts,
- access to all kinds of company records, files or documents,
- requests for documentation from third parties,
- analysis of computer files and emails,
- analysis of video or audio recordings.

In-person or online meetings that take place to carry out interviews with reported persons or anyone involved in the investigation must be documented:

- via a **recording of the conversation** in a secure, permanent and accessible way, provided that the persons reported or involved are warned in advance that they will be recorded, is informed of the processing of their data by means of the document attached as *Annex 2* in accordance with applicable law, and they provide their consent, or

- by means of a **full, accurate transcription** of the conversation conducted by the staff member responsible for processing it. In this case, the transcription will be provided to the persons reported or involved to verify, amend and accept the information by signing the transcription of the conversation, and they will be informed of the conditions regarding the processing of their personal data by means of the document attached as *Annex 2*.

**Employees and management** are obliged to respond diligently, fully and truthfully to all questions posed to them by the investigator concerning the performance of their professional activities within the company. The intentional or grossly negligent provision of untruthful or incomplete information may be considered a disciplinary violation, leading to the closure of the investigation and the case file.

Principles and limits of the investigation

- **PROMPTNESS**. The gathering of evidence, whether initial or as part of an investigation, must be carried out as quickly as possible without jeopardising its purpose. Extra emphasis must be placed on the speed of an investigation when it may impact on the reputation of the people involved or the company.

  Cases received via the different Channels will be managed within a maximum of **3 months** from the reception of the report, except in particularly complex cases or for valid reasons that justify an extension for a further 3 months.

  In cases where additional information from the whistleblower is required in order to begin or continue with the investigation, the information will be requested and must be provided within 15 days. Otherwise, the case will be closed and marked as 'dismissed due to insufficient information'.
- **CONFIDENTIALITY.** The investigation is carried out confidentially. The investigative body may disclose any necessary details in order to ensure the preventive effect of disciplinary action and enable the fulfilment of Gestamp's preventive system. The investigator and/or the persons interviewed/whistleblower may be required to sign confidentiality agreements.
- **PROPORTIONALITY.** Measures taken must always be useful and appropriate to their ends, and must not cause greater harm than that which is intended to be prevented by the investigation.

  The resources provided by Gestamp to its employees for carrying out their professional activities, including computers and e-mail accounts, must not be used for other purposes. There is no expectation of privacy with regard to them and they may therefore be controlled by the company proportionately for productive or disciplinary purposes.
- **AUTHENTICITY.** The Investigator must ensure the security all means of evidence, particularly computer files and e-mails.
- **LEGALITY.** Investigations must respect the current legislation of the country in which they are carried out, particularly with regard to data protection, privacy and relations with judicial and administrative authorities.

### 4.3.3. Rights of people under investigation

The person under investigation has the right to have impartial persons to lead and decide on the results of the investigation, guided only by the regulations governing their functions and under the applicable Code of Conduct.

The person under investigation is entitled to be notified of the existence of the investigation and the reason behind it as soon as possible, so long as this does not jeopardise the aim of the investigation. In any case, they must be notified before the investigation is completed.

The person under investigation is entitled to make any statements that they deem appropriate in their defence at any time, and to provide evidence.

If the person under investigation is subject to criminal proceedings for the same matter under investigation, or if it is reasonable to expect that they will be, they will be informed that they have the right not to make a statement against themselves and not to admit guilt. They will also be advised that it is part of Gestamp's interest in the investigation to provide its own possible criminal defence, which will not necessarily be the same as that of the person under investigation.

The existence of a criminal procedure against the person under investigation, even if it is initiated or brought to the attention of the authorities, by Gestamp, will not prevent the processing of the investigation procedure provided for in this document to the extent that labour disciplinary measures may be adopted against the person under investigation, regardless of the decisions adopted by the criminal judicial authority.

The person under investigation has the right to the protection of their identity and confidentiality of the events and details of the procedure.

### 4.3.4. Mechanisms to avoid conflicts of interest

Furthermore, the following mechanisms have been put in place to avoid conflicts of interest:

- Receipt of reports through an external online/telephone platform SpeakUp Line, which guarantees the integrity of reports and the traceability of access by the investigation team.
- The Compliance Office receives all reports and, in turn, will pass them on or involve the corresponding department in accordance with the provisions of this Procedure.
- Identification and profiling of the persons who have access to the reporting platform.
- The Compliance Office will assess the person to whom it will assign the investigation to avoid a potential conflict of interest.

### 4.3.5. Investigator's report

Once the investigation is over, in the event that the investigation is conducted by a Representative, the Representative will report to the Compliance Office; if the Compliance Office has been investigating the case, the Compliance Office will report to the Ethics Committee.

The case report must contain:

- details of the reported events and evidence put forward by the whistleblower in support of said events;
- the classification of the report of the breached regulations;
- the action taken to verify the credibility of the reported events;
- the conclusions reached in the investigation and assessment of the evidence and indications supporting it;
- and, where appropriate, an assessment of the prevention systems applicable to the conduct or irregularity under investigation and possible recommendations for improvement.

The body to whom the case report is submitted, whether it be the Compliance Office or the Ethics Committee, must adopt an appropriate resolution in accordance with circumstances mentioned above. If the resolution involves disciplinary action, the action to be taken may be proposed to the disciplinary body.

### 4.3.6. Resolution of the communication

Once the case report described above has been approved, the Investigator must complete a document giving a brief description of the event reported, the rule breached, the body in charge of investigating, the conclusion of the investigation, the measures taken and the response to be given to the whistleblower.

This document is filed in the SpeakUp Line tool and the Compliance Office considers the report to be closed.

### 4.3.7. Record of investigations

The investigation file, regardless of the body that has carried it out, will be kept by the Compliance Office, ensuring that no unauthorised third parties have access to it.

When it is no longer necessary for the purpose of the investigation, personal data will be anonymised within a maximum period of 3 months from receipt of the report, except in particularly complex cases or for valid reasons that justify extending it for a further 3 months.

# 5. Personal data protection for the whistleblower and affected persons

The management of the IIS will comply with personal data protection law applicable to the different companies within the Group. In particular, the following aspects will be taken into account:

- The data controller is GESTAMP SERVICIOS, S.A.
- The personal data collected in relation to the report will be processed for the sole purpose of investigating, processing and resolving the reported events in accordance with the Group's Code of Conduct, its corporate rules and governing regulations.
- The legitimate basis for the processing of the data and potential disclosure to the data processors, is compliance with a legal obligation, as well as Gestamp's legitimate interest in ensuring legality and order in its workplaces and processes.
- The data will be transferred to the company ETHICS CHANNEL, S.L., which administers and manages the external channel SpeakUp Line. Where necessary, it will also be transferred to other companies of the Group who act as data processors for the sole purpose of investigating the reported events. Such data transfers shall always be carried out in compliance with the required legal safeguards.
- Notwithstanding the foregoing, all Gestamp companies shall implement applicable personal data security measures in accordance with the risk of each of them and the applicable data protection regulations.
- Confidentiality of the identity of whistleblowers and affected persons, as well as of reports, must be guaranteed. Furthermore, the presumption of innocence is guaranteed to all persons concerned. All reporting persons shall enjoy due protection, without any retaliation occurring as a result of the event reported.
- Access to the data contained in these systems shall be limited exclusively to those in charge of the IIS, or to the persons in charge of the procedure established for this purpose. Other persons may also have access for the exercise of their functions, as assigned by the Compliance Office when necessary for the processing of the internal file; in exceptional cases, if the report reaches the courts, the file will be shared with the competent authorities.
- If disciplinary measures are to be taken against an employee within the company itself, access shall be granted to the human resources department or to staff with management functions, since they must have access to the personal data in order to implement the sanction.
- At the time of obtaining the personal data, an acknowledgement of receipt shall be sent within seven (7) calendar days of receipt, notifying the person concerned that their data will be processed in accordance with applicable law. Where applicable, the person concerned will also receive prior warning that their report will be recorded.

# 6. Data handling and storage

As regards the handling and storage of both personal data and all information provided by the whistleblower, this will be processed by the Group, ensuring restricted access, and will be protected by appropriate security measures in accordance with current data protection law.

The data of the whistleblower (if identified), employees and third parties will only be kept in the reporting system for the time required to decide whether to initiate an investigation into the reported events.

In any case, three months after the entry of the data, it shall be removed from the record of reports, unless being stored to keep evidence of the prevention model for the commission of offences by legal persons, requiring it to be kept in a system other than the internal reporting system.

Reports not admitted for processing may only be recorded in anonymised form.

Furthermore, in the event that legal action or litigation is foreseen, the data shall be kept for as long as it is necessary for the exercise of the Group's rights in court.

Personal data shall be deleted when it is no longer required for the purpose of the investigation, including any potential legal proceedings that may arise following the investigation.

# 7. Entry into force

This document shall enter into force on the day following its approval by the Gestamp Ethics Committee, which is responsible for the Internal Information System.