Internal Information System Policy

December, 2023

TABLE OF CONTENTS

1. INTRODUCTION 3

2. SCOPE OF APPLICATION 3

3. COMMUNICATION CHANNELS 3

4. COMMUNICATIONS 4

5. GENERAL PRINCIPLES OF THE IIS CHANNELS 4

6. SAFEGUARDS OF THE INTERNAL INFORMATION SYSTEM 5

7. MANAGER OF THE INTERNAL INFORMATION SYSTEM 6

8. POLICY APPROVAL, REVIEW AND UPDATE 6

1. INTRODUCTION

Gestamp Group (**'Gestamp'** or the **'Group'**), in line with its Code of Conduct, is committed to achieving high levels of ethics and transparency to safeguard our customers, employees, shareholders, business partners and society as a whole.

To this end, Gestamp maintains an Internal Information System ('**IIS'**) that allows anyone to report violations of applicable external or internal regulations, including its Code of Conduct, that take place within the Group in the ordinary course of business.

The IIS also channels questions about the interpretation of our Code of Conduct and internal regulations. It is also the appropriate route for suggesting improvements to its content.

This Internal Information System Policy ('**Policy**') aims to define the scope of application of the IIS, its general principles and the safeguards it provides in order to protect both whistleblowers and affected persons.

In addition, the Internal Information System Management Procedure, the internal regulations that implement this Policy, sets out rules applicable to the procedure for receiving, processing, recording and resolving communications received through the IIS.

2. SCOPE OF APPLICATION

This Policy is applicable to all members of the governing bodies, management and employees of all the companies in the Group, i.e. Gestamp Automoción, S.A. and the companies in which it has a controlling interest.

The IIS is also intended to be used by any legal or natural person who has had, has or may have a relationship with or interest in Gestamp ('**Third Parties**') in situations governed by this Policy, as a formal mechanism distinct from other communication channels available to Third Parties. As a result, the Policy will also apply to Third Parties who make use of the IIS.

3. COMMUNICATION CHANNELS

Within the IIS, Gestamp has various channels (the '**Channels**')[1] available for the users of the IIS defined in section 2 above, promoting a culture of open, fluid and transparent communication:

- Gestamp employees can contact their **line manager or HR representatives** of their organisational department, either verbally or in writing.
- **Corporate mailbox**. Gestamp provides the following e-mail address: corporatecompliance@gestamp.com.
- **SpeakUp Line external channel**. Online tool designed as a specialised IT platform that can be accessed via the Gestamp website and intranet.

[1] Wherever permitted by applicable legislation, Gestamp encourages the use of the IIS Channels preferably to external channels. Nevertheless, where the legal system of those countries in which the Group is present has established an external channel for the communications governed by this Policy, whistleblowers shall also have the possibility of using such channels under the terms provided for in the applicable legislation.

- In-person or online meeting. Whistleblowers may also request an in-person meeting to verbally report any irregular conduct. This meeting must take place within a maximum of 7 days after the request is made

If the whistleblower opts to make a report through the corporate mailbox or the SpeakUp Line external channel, they will receive confirmation of receipt within a maximum of 7 calendar days from the reception of the report.

4. COMMUNICATIONS

The Channels can be used to report (i) questions about the interpretation of Gestamp's Code of Conduct and other internal regulations, and to suggest improvements to its content, and (ii) concerns about irregularities taking place within the Group related to:

- Internal regulations. Including:
  - Irregularities and violations of the Code of Conduct and its implementing regulations.
  - Illegal acts in the working environment.
- External regulations. Including:
  - Violations of law on anti-money laundering and terrorism financing, as well as corruption and bribery.
  - Violations of the Securities Market regulations.
  - Conduct that could be considered illegal, particularly criminal or administrative violations, infringements of the legislation in force in any jurisdiction where the Group operates or violations of European Union law.
  - Infringements of Human Rights.

All the reports received via any of the channels provided will be admitted for processing.

However, if a report is made in bad faith, i.e. the whistleblower is aware that the events reported are false or they act with clear disregard for the truth, they may be subject to disciplinary action by the Group, in addition to the criminal and/or civil liability that may arise from their behaviour.

5. GENERAL PRINCIPLES OF THE IIS CHANNELS

(a) Tone from the top: Commitment of the Board of Directors and senior management. The Board of Directors, as the body ultimately responsible for the IIS, is committed to provide the necessary resources to ensure the integration of the system in the Group, in all established processes and at all business levels.

(b) Transparency in terms of the publication of statistical data and the findings of reports received through the Channels in the reports that the Group discloses to the market.

6. SAFEGUARDS OF THE INTERNAL INFORMATION SYSTEM

(a) **Anonymity.** Whistleblowers/reporting persons who use the Channels may choose to make their communications anonymously.

(b) **Hearing.** Everyone shall be entitled to be heard in order to defend themselves, and shall be given the proper opportunities within a reasonable period of time.

(c) **Promptness**. The gathering of evidence, whether initial or as part of an investigation, will 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 communication, 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 necessary 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'.

(d) **Confidentiality**. The identity of the whistleblower and any third parties mentioned in the report and/or in the course of the actions carried out in the handling and processing of the report will be protected as confidential unless there is a legal obligation to disclose said information or if the express consent of the whistleblower or of the aforementioned persons has been granted.

(e) **Independence and impartiality of case handling.** Independence and impartiality will be upheld at all times, with full respect for the law and internal regulations. Questions, suggestions and reports will be processed with according to fairness, integrity, objectivity, independence and honesty.

In any case, all reports, whether anonymous or not, are completely confidential.

(f) **Legality.** Investigations will 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.

(g) **Presumption of innocence.** The handling of reports and subsequent processing of the case must be carried out with the utmost respect for the reputation of the person reported and the presumption of their innocence, although the special characteristics of workplace settings must be taken into consideration, as private relationships between the company and the employee are involved.

(h) **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.

7. MANAGER OF THE INTERNAL INFORMATION SYSTEM

Gestamp's governing bodies have appointed the Ethics Committee as the head of the IIS, in charge of its management. The structure, duties and operation of this committee are regulated in the Group's Compliance Policy.

The Ethics Committee, as the group in charge of the IIS, will act autonomously and independently from any other bodies, committees or commissions in Gestamp, notwithstanding the oversight powers entrusted to the Board of Directors, mainly through the Audit Committee.

The competent authorities pursuant to local regulations in each country shall be informed of the individually appointed natural person who will perform the duties of reporting and processing any cases investigated.

8. POLICY APPROVAL, REVIEW AND UPDATE

This Policy has been approved by the Company's Board of Directors.

This Policy shall be reviewed and updated whenever necessary to bring it into line with the current legal, social, economic or environmental situation at any given time. Any subsequent amendment of the Policy shall be approved by the Board of Directors.

Version	Person responsible	Supervisor	Approval	Company	Approval date
1.0	Ethics Committee	Audit Committee	Board of Directors	GESTAMP AUTOMOCIÓN, S.A.	18 December 2023