Internal Information System Policy [extract]
Mutua Madrileña
Courtesy English translation
The only valid official version of the document is in Spanish

Internal Information System Policy

Mutua Madrileña

May 2023

CONTENTS:

INTERNAL INFORMATION SYSTEM POLICY

I. INTRODUCTION

This Internal Information System Policy is encompassed within the entity's Control System established by Grupo Mutua Madrileña (hereafter "MM" or "the Group") for the set of entities that formally adhere to it.

In this excerpt from the policy, information regarding the use of the Whistleblower Channel and the essential principles of the management procedure is outlined.

1. Background

The **Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, on the protection of persons who report breaches of Union law** has highlighted the need for public and private entities with more than 50 employees to have information channels in place so that any individual who, in a work-related or professional context, has obtained information about suspected breaches, may report potential breaches of European Union Law, serious or very serious administrative breaches or criminal offences.

The Directive has been transposed into Spanish legislation through **Law 2/2023, of 20 February, regulating the protection of persons who report breaches of the law in the fight against corruption.** The law aims to protect whistleblowers, establishing the minimum rules that information channels must comply with.

For the above reasons, Mutua Madrileña has drafted a regulatory policy for its whistleblower reporting system and carried out the necessary amendments in its Reporting Channel, as an internal information channel to receive the reports.

2. The objective of the policy

The objective of this policy is to establish the principles to guarantee the implementation of an Internal Information System which meets the applicable legal requirements. Moreover, the Internal Information System Policy provides a structured overview of the roles and responsibilities that correspond to each of the parties involved in the System, and the procedure in place to manage the allegations received within our entity.

3. Scope of application

The application of this Policy currently extends to Mutua Madrileña Automovilista. Furthermore, since this is a Group Policy, companies with the obligation to have an Internal Information System in place must adapt to this Policy by formal approval of this text or approve their own similarly aligned policy[1].

[1] Article 2.6: Law 2/2023: In the case of information or the public disclosure of the breaches referred to in part II of the annexe of Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, the specific law on reporting breaches in these areas (whistleblowing) shall apply.

3.1. Scope of application of the Internal Information System

- **Who can report (whistleblow)?**

The Internal Information System is made available for whistleblowers that work in the private or public sector and have obtained information about breaches in a work-related or professional context, including in all cases:

a) individuals that are considered civil servants or employed persons;

b) self-employed persons;

c) shareholders, stakeholders, and persons belonging to the administrative, management or supervisory bodies of our entity, including non-executive members;

d) any individual that works for or is under the supervision and management of contractors, subcontractors and suppliers;

e) whistleblowers who report or reveal information publicly about breaches obtained within the context of a working or statutory relationship which has already been terminated; volunteers, interns, and workers in a period of training regardless of whether they receive remuneration or not; and those whose working relationship has not yet started, in cases where the information about breaches has been obtained during the selection process or pre-contractual negotiations.

- **What can be reported?**

The following can be reported through the Reporting Channel:

a) any actions or omissions that may constitute breaches of European Union Law, under the requirements set out in the law.

b) actions or omissions that may constitute a criminal offence or a serious or very serious administrative offence. In all cases, all criminal offences, or serious or very serious administrative offences shall be deemed to be included that involve economic loss to the Public Treasury or Social Security.

c) breaches or reasonable suspicions of relevant breaches of the internal regulations of the entities and basic principles conveyed by the Code of Ethics.

4. Action principles

The general action principles of the Internal Information System, conducted by the board of directors, which govern this policy are as follows:

1. To prevent, report, and repair are the objectives of the organisation's Internal Information System.

2. To create an environment of transparency, integrating the different systems developed to prevent legal risks from occurring within the entity; maintaining the Reporting Channel as an appropriate channel to favour the reporting of potential irregularities, following the scope of this policy.

3. Reporting is not optional, and individuals must report information regarding potential breaches to the entity's Reporting Channel.

4. The use of the Internal Information System for purposes that are illegitimate, personal, or contrary to good faith are not permitted. Where reports are proven to be false, once the activity has been documented, the corresponding bodies of our entity, as indicated in the Management of the Reporting Channel section, shall apply the relevant measures to the whistleblower. The relevant entity, per the report, shall push forward disciplinary, sanctioning, and legal processes, as applicable, until they are resolved.

5. To ensure that whistleblowers that submit a report under the provisions of this policy do not suffer any reprisals of any type as a result, including threats or attempts at reprisals. To this effect, we refer to the section of this policy, which expressly lays out the protection measures for whistleblowers established by the entity.

6. To guarantee the respect of presumption of innocence and honour of the individuals affected, in addition to guaranteeing the right of the affected individual to be informed of the actions or omissions attributed to them, and to be heard at any time.

7. To foster and promote a preventive corporate culture based on the principle of "zero tolerance" towards committing illegal acts and fraud by applying the principles of ethics, encouraging the responsible behaviour of all professionals within the entity, regardless of their hierarchical position.

8. To inform the entity's employees transparently of the existence of this Policy, in addition to the procedures for reporting breaches and of the protection measures for whistleblowers.

9. To investigate all reports of events that allegedly constitute breaches subject to this Policy.

10. To guarantee the confidentiality of the information and identity of the whistleblower, or anonymity in cases where the whistle-blower so wishes, withholding from the collection of personal details where the relevance is unclear, to managing specific information. If they are collected accidentally, they shall be deleted without any undue delay. Furthermore, the rights referred to in articles 15 to 22 of the GDPR will be guaranteed.

11. To provide all necessary assistance and cooperation that may be required by the external provider of the Reporting Channel, as well as the competent authorities, legal and administrative bodies, or institutions and national or international bodies which may investigate the facts that allegedly constitute breaches of European Union Law, serious and very serious administrative offences, or criminal offences.

12. To ensure a fair, non-discriminatory, and proportional application of sanctions under the provisions of the sanctions system and the legislation in force at any time.

13. If serious shortcomings or breaches are detected, the measures required to remedy them must be adopted.

II. GOVERNANCE, ROLES, AND RESPONSIBILITIES

The role of the board of directors is listed below:

- Approving the organisation's Internal Information System Policy.
- Implementing the Internal Information System after consultation with the workers' legal representation.
- Designating a person responsible for managing the System (hereafter, the "System Manager"), in addition to their dismissal or termination

The Criminal Risks Prevention Committee (Responsible for the Internal Information System) has delegated to whoever holds the Role of Regulatory Compliance, the powers of management of the Internal Information System to handle investigation cases, apart from the employment aspect, which shall be managed by whoever holds the role of Sub-Directorate General of People, Talent, and Culture. The Criminal Risks Prevention Committee has to comply with the obligations of knowledge, investigation and issuing of proposals about the reports that are declared admissible under the management procedure of the Reporting Channel provided for in this policy.

Any member of staff that receives a whistleblowing report has to immediately send the report to the System Manager, where the communication:

- Has been sent by reporting channels other than those established for that purpose.
- Has been received by members of staff that are not responsible for its processing.

In all cases, the confidentiality of information is guaranteed, the violation of which shall be deemed a very serious breach.

III. STRATEGY, PROCESSES AND PROCEDURES

1. Dissemination measures

The implementation of this Policy must be accompanied by the appropriate dissemination of it, with an emphasis on the importance of its compliance. To this effect:

- The Policy and documents that are the basis of the Internal Information System must be communicated via the intranet or similar system to enable access to the documentation.

- The Internal Information System must be communicated both through the organisation's website and the intranet. Concerning the website, in a separate and an easily identifiable section of the home page, appropriate information shall be provided in a clear and easily accessible manner about the use of the Reporting Channel and the essential principles of the management procedure.

2. Management of the Reporting Channel

Entities with 50 or more employees will have access to a Reporting Channel, managed externally, which will be the gateway through which allegations relating to all entities will be channelled.

The Internal Information System must be independent and separate from the information systems belonging to other entities or bodies.

2.1 Submission of reports

Reports will be submitted through the Reporting Channel, in writing and accordance with the following:

Access to the Reporting Channel will be via an external entity, which has the resources with the ability, autonomy, and independence to carry out the relevant investigations. The management of the Internal Information System by this third party is not to the detriment of the guarantees and requirements laid out in this policy, and the System Manager shall be responsible for it. The tool can be accessed either through the corporate website or the employee portal.

If reports are made in writing, once the report has been submitted, the whistleblower can request a face-to-face meeting with the external provider of the Channel within a maximum of seven days. The external provider will take minutes of the meeting, which will contain an exact and full transcription of the conversation, and will offer the whistleblower the opportunity to check, rectify and accept the transcription of the conversation with their signature. However, the minutes must also be signed by the other attendees. Without prejudice to the rights corresponding to them under the data protection regulation, the whistleblower will be offered the opportunity to check, rectify and accept the transcript of the conversation with their signature.

At the time the reports are submitted through the Reporting Channel, the external provider will ask for the identification of the whistle-blower, although identification is not required under any circumstances, if the whistle-blower prefers to remain anonymous, except in the case regarding breaches or reasonable suspicions of relevant breaches of the internal regulations of the entities and basic principles conveyed by the Code of Ethics, which do not also involve a breach of European Union Law, serious or very serious administrative offences or criminal acts. In the case of anonymous allegations, the whistleblower shall be required to declare the status regarding access to the Internal Information System under the provisions of the scope of the Policy.

In any case, all reports submitted through the Reporting Channel shall be anonymous for the entity subject to the report, equally guaranteeing their confidentiality.

Without prejudice to the above, concerning reports of harassment, the provisions of Article 97 of the Collective Agreement for the Insurance Companies sector shall apply (or, if applicable, the conventional or specific employment legislation that applies to each company). To this effect, any member of Management that receives a report of harassment must send it through the Reporting Channel for the maximum guarantees to be applied in terms of its processing.

[For the purposes of Article 97 of the Collective Agreement for the insurance company sector, the possibility of following this channel is without prejudice to submitting a report of harassment to a person from the company's management team, the director of People, Management and Culture, unless the accused is that person, in which case it would be submitted to the Deputy Director General of Technology and People.]

2.2 Procedure for handling the reports received

The process for handling the reports received shall be as follows:

A. External management:

The external provider of the Channel will receive and/or record the report on the Reporting Channel web application and send the whistleblower an acknowledgement of the report within seven calendar days of its receipt, unless this may put the confidentiality of the information at risk.

Upon receipt of the report, the external supplier shall carry out a preliminary review of the content of the report and, if applicable, request additional information from the whistle-blower to create a report evaluation. In the case of an allegation of workplace harassment, the Workers' Legal Representation will be made aware of the situation, if requested by the person affected, and if deemed necessary, the external supplier shall put the appropriate measures into place to prevent the harassment from continuing.

Additionally, there will be an opportunity to maintain communication with the whistleblower and, if the provider deems it to be necessary, to request additional information from the whistleblower. Interviews may be held with the alleged perpetrator and any individuals that may be of interest when establishing the facts. Minutes will be taken of the interviews, which must be signed by all individuals present except for the whistleblower, and the opportunity shall be given to them to check, rectify and accept the transcript of the conversation via their signature.

Once the assessment of the allegation has been completed and the possibility of the actions or omissions reported constitute a crime, the provider of the channel sends the information and analysis carried out to the Criminal Risk Prevention Committee, removing the identifying information of the whistleblower, unless a national law includes a provision for it to be revealed, false allegations or where requested as part of legal proceedings, situations that result in the loss of anonymity before the entity subject to the allegation. If the report relates to the workers' rights or workplace harassment, the external provider will send the result of the preliminary investigation to the Sub-Directorate General of People, Talent, and Culture at Mutua Madrileña or the HR & Quality Department at Centauro, as applicable.

Reports received through the Reporting Channel will only be kept in the tool for the time required to decide on whether to begin an investigation and, in any case, within a maximum period of three months.

On the expiry of that period, they will be deleted from the tool, except to retain evidence of the operation of the Reporting Channel. However, reports that have not been pursued may be kept anonymised.

B. Internal management:

To investigate reports received, the whistleblower must provide sufficient information, and the report must be duly substantiated, reasoned and provide reasonable evidence of a breach having taken place.

The timeframe for completion of the investigation may not exceed three months from the receipt of the report or, if acknowledgement of receipt was not sent to the whistleblower because this would jeopardise the confidentiality of the information, from the expiry of the deadline of seven days after the report has been made. In particularly complex cases, the timeframe may be extended to a maximum of three additional months.

If the report relates to workplace harassment in insurance companies, the investigation will be carried out in a maximum of 10 days, under the provisions of the applicable Collective Agreement (or, if applicable, within the timeframe established by conventional or specific employment law applicable to each company).

Once the investigation is complete, the result will be communicated to the decision-making body. The decision-making body will make the decision relating to the evidence subject to the report and, to that effect, will communicate the evidence subject to the report to the Sub-directorate of People, Talent and Culture or the Management of the Centauro HR & Quality Department, as applicable, for the application, as appropriate and where necessary, of the relevant disciplinary proceedings. Where the irregular conduct has been committed by a service provider, the Legal Advisory Department, or Legal Department of Centauro if it relates to this entity, will apply where applicable, and if necessary, the actions to terminate the contract and claim compensation for damages.

The entity will keep a logbook of all of the reports received through the Reporting Channel and the investigations carried out as a result of those reports.

3. Allegations received outside of the Reporting Channel

If an allegation is reported via means other than the Reporting Channel or to an employee that is not responsible for its management, the recipient of the information shall immediately pass it on to the System Manager. In these cases, confidentiality is guaranteed, under the same terms as the reports received through the Reporting Channel. The System Manager will incorporate the allegations reported to the Reporting Channel for it to be processed in the normal manner.

4. External information channels

Individuals that can address the Internal Information System may inform the Independent Whistleblower Protection Authority or corresponding autonomous authorities or bodies, of any actions or omissions included within the scope of this policy, either directly or after submitting a report through the Reporting Channel.

5. Protection measures for whistleblowers

Individuals that whistleblow or reveal breaches provided for within the scope of application of this policy, in addition to the individuals, referred to in articles 3.3 and 3.4 of Law 2/2023[2] will have the right to protection, provided that the following circumstances are met:

a) they have reasonable grounds to believe that the information referred to is true at the time of the report or disclosure, even where they do not provide conclusive evidence, and that the information falls within the scope of this policy,

b) the report or disclosure has been carried out following the requirements provided for in this policy.

Individuals who report or disclose the following are expressly excluded from protection:

a) Information contained in reports that have been rejected by an internal information channel or by the Independent Protection Authority for any of the reasons provided for by law:

   i. Where the evidence lacks full credibility.
   ii. Where the evidence does not constitute a breach of the legislation included in the scope of Law 2/2023.
   iii. Where the report manifestly lacks any basis or, in the view of the Independent Whistleblower Protection Authority, there are reasonable indications that the information has been obtained by committing a crime. In the latter case, in addition to being rejected, a detailed description of the facts that are deemed to constitute a crime shall be sent to the Prosecution Service.

---

[2] *Article 3.3*: The protection measures of the whistleblower provided for in Title VII will also apply, where applicable, specifically to the legal representatives of the workers while performing their duties of advising and supporting the whistleblower.

Article 3.4: The whistleblower protection measures provided for in Title VII will also apply, where applicable, to a) natural persons who, within the organisation in which the whistleblower provides their services, assist them in the process, b) natural persons who are related to the whistleblower and who may suffer reprisals, such as work colleagues or family members of the whistleblower, and c) legal entities that they work for or with whom they maintain any type of relationship in a work-related context or in which they have significant shareholding. To this end, participation in the capital or voting rights corresponding to shares or holdings is understood to be significant when their proportion enables the individual holding them to have the ability to influence the legal entity involved.

iv. Where the report does not contain new and significant information regarding breaches compared to a previous report for which the relevant procedures have been concluded unless new factual or legal circumstances arise that justify a different course of action. In these cases, the Independent Whistle-blower Protection Authority shall substantiate the decision.

b) Information linked to claims regarding interpersonal conflicts or that only affect the whistleblower and the people referred to in the report or disclosure.

c) Information that is already fully available to the public or that constitutes mere rumour.

d) Information that refers to actions or omissions not covered by Article 2 of Law 2/2023.

Individuals who have reported or publicly disclosed information about actions or omissions that refer to the scope of application of the Internal Information System anonymously but have subsequently been identified and meet the conditions provided for in this policy will have the right to protection.

Individuals who report breaches to the institutions, bodies or offices of the European Union which fall under the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, will have the right to protection under the provisions of Law 2/2023 under the same conditions as an individual that has reported using external channels.

Protection does not exclude the application of regulations relating to criminal proceedings, including investigations.

The protection provided in the policy for employees that report breaches of Employment Law concerning health and safety in the workplace is understood to be without prejudice to the protection established in its specific legislation.

Furthermore, this protection will not apply to information affecting classified information and will not affect obligations arising from the protection of professional secrecy of medical or legal professionals, of the duty of confidentiality of the Law Enforcement Authorities in the scope of their activities, in addition to the secrecy of court deliberations.

5.1 Prohibition of reprisals

Acts that constitute a reprisal are expressly prohibited, including threats and attempts at reprisals against individuals that submit a report under the provisions of this policy. Reprisals are understood to include any acts or omissions that are prohibited by law, or which, directly or indirectly, involve unfavourable treatment that places the individuals subjected to the reprisals at a specific disadvantage concerning another in the work or professional context, solely because of their condition as a whistleblower, or for having made a public disclosure. For the purposes of this policy and, by way of example, reprisals are those adopted in the form of:

a) Suspension of the employment contract, dismissal or termination of the working or statutory relationship, including the non-renewal or early termination of a temporary employment contract once the trial period is over, or early termination or cancellation of contracts for goods or services, implementation of any disciplinary measure, delay and denial of promotion and any other substantial modification of working conditions and the non-conversion of a temporary employment contract into a permanent contract, if the worker had legitimate expectations of being offered permanent employment; except where these measures are carried out within the regular exercising of power of management within the scope of employment legislation or governing legislation of the corresponding public sector employment statute, due to circumstances, events or breaches that have been proven, and not related to the submission of the report.

b) Damage, including that of a reputational nature, financial loss, coercion, intimidation, harassment or ostracism.

c) Negative assessments or references concerning work or professional performance.

d) Inclusion on black lists or dissemination of information in a specific sector area, which hinders or prevents access to employment or contracting of work or services.

e) Refusal or cancellation of a licence or permit.

f) Denial of training.

g) Discrimination, or unfavourable or unfair treatment.

Individuals whose rights have been violated as a result of their report or disclosure once the two-year period has lapsed may request protection from the competent authority which, exceptionally and justifiably, may extend the protection period, after a hearing with the individuals or bodies that may be affected. The refusal of the extension of the protection period must be substantiated.

5.2 Protection measures against reprisals

Individuals that report information about actions or omissions contained within the scope of application of this policy or that make a public disclosure under Law 2/2023 will not be considered to have breached any restrictions on the disclosure of information, and those individuals will not be held liable in any way concerning that report or public disclosure, provided that they had reasonable grounds to believe that the report or public disclosure of that information as necessary to reveal an action or omission according to the law, all without prejudice to the provisions of article 2.3[3]. **This measure will not affect criminal liabilities.** This provision extends to the reporting of information made by representatives of the employees, even if they are subjected to legal obligations of secrecy or not to disclose classified

[3] Article 2.3: "The protection provided for in this law for employees that report breaches of Employment Law concerning health and safety in the workplace, is without prejudice to the protection established in its specific legislation."

information. All of this is without prejudice to the specific protection rules that apply under employment regulations.

Whistleblowers will not be held liable for the acquisition or access to information that is reported or publicly disclosed, provided that this acquisition or access does not constitute a crime.

Any other potential liability of whistleblowers arising from acts or omissions that are not related to the report or public disclosure or that are not required to reveal a breach under this policy will be enforceable by the applicable legislation.

In proceedings before a court, or other authority about the harm suffered by the whistleblowers, once the whistleblower has reasonably demonstrated that they have made a report or public disclosure in accordance with the law and that they have suffered harm, it will be presumed that the harm was caused as a reprisal for reporting or making a public disclosure. In such cases, it will be up to the individual that has taken the harmful action to prove that this measure was based on duly justified grounds, not linked to the report or public disclosure.

In legal proceedings, including those relating to defamation, copyright infringement, breach of professional secrecy, breach of the data protection rules, disclosure of business secrets or compensation claims based on employment or statutory law, the individuals referred to within the scope of this policy will not be held liable in any way as a result of the reports or public disclosures protected by it. These individuals will have the right to present an argument in their defence and the context of the aforementioned legal proceedings, having reported or made a public disclosure, provided that they had reasonable grounds to believe that the report or public disclosure was necessary to reveal a breach under this policy.

These protection measures apply to whistleblowers who report potential breaches included in this policy, except for those relating to breaches or reasonable suspicions of relevant breaches of the internal regulations of the entities and basic principles conveyed by the Code of Ethics that do not amount to a breach of European Union Law, serious or very serious administrative offences or criminal offences.

5.3 Support measures and competent authority

Individuals who report potential breaches included in this policy, except for those relating to breaches or reasonable suspicions of relevant breaches of the internal regulations of the entities and basic principles conveyed by the Code of Ethics that do not amount to a breach of European Union Law, serious or very serious administrative offences or criminal offences, shall have the right to the support and protection measures provided by the Law for the protection of persons that report regulatory breaches in the fight against corruption.

The aforementioned support measures will be provided by the Independent Whistleblower Protection Authority, when the breaches are committed within the scope of the private sector and state public sector and, where applicable, by the competent bodies of the autonomous communities, regarding breaches in the scope of the autonomous and local public sector of the territory of the relevant autonomous community, in addition to breaches in the private sector, where the breach reported is confined to the

territorial scope of the corresponding autonomous community. The above must be understood without prejudice to the specific measures of support and assistance that may be put in place by the public and private sector entities.

5.4 Measures for the protection of persons affected

While the case is being processed, the individuals affected by the report will have the right to be presumed innocent and the right to defence.

Furthermore, except in the case of reports relating to breaches or reasonable suspicions of relevant breaches of the internal regulations of the entities and basic principles conveyed by the Code of Ethics, which do not also amount to a breach of European Union Law, serious or very serious administrative offences or criminal offences, the individuals affected by the report will also have the right to access the case under the terms regulated by Law 2/2023, in addition to the same protection established for whistle-blowers, keeping their identity secret and guaranteeing confidentiality of the facts and details of the procedure.

6. Protection of personal data

This policy has been produced under the provisions of Title VI on the protection of personal data and the other provisions of Law 2/023, of 20 February, regulating the protection of persons who report breaches of the law and the fight against corruption, and with the general data protection regulation, 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 guarantee of digital rights.

The data protection policy incorporated into the Reporting Channel will contain and report on the legal regime and legality of the processing of personal data that is carried out. Additionally, it will provide information regarding the preservation period of data in relation to this processing, in addition to the necessary communication of data that must be carried out to comply with the applicable legislation. Furthermore, information will be provided about data protection rights and the channels available to exercise those rights, in addition to the right to preserve the identity of the whistleblower and persons affected. All of the above is in accordance with Law 2/2023 of 20 February, regulating the protection of persons who report breaches of the law and the fight against corruption.