

SIGMA INTERNAL INFORMATION SYSTEM**RULES AND OPERATING PROTOCOL OF THE INTERNAL INFORMATION
CHANNEL OF SIGMA.AI, S.L.U.****1. INTRODUCTION.**

As an essential part of the so-called Internal Information System, the Internal Information Channel is embedded within it as the preferred means of reporting the acts or omissions provided for in Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption. It is a communication channel through which reports can be submitted regarding risks or suspicions of irregular conduct and regulatory breaches. In this way, the responsible body will investigate them and, where appropriate, adopt the relevant preventive, corrective or disciplinary measures.

In this regard, and in order to improve the communication and management of SIGMA.AI, S.L.U. (hereinafter SIGMA.AI), as well as to support and protect those who report irregularities, the SIGMA.AI Internal Information Channel has been created. It is made available to all persons working at SIGMA.AI and to third parties related to the company, and through it any professional negligence and any unlawful and/or irregular conduct contrary to ethics occurring in the workplace may be reported.

The SIGMA.AI Internal Information Channel follows the guidelines set out both in 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 (*Whistleblowing Directive*), and in Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, which transposes said Directive and whose articles 5 and 7 establish the general provisions on the implementation of the internal Information System and Channel.

The ultimate goal is to foster a culture of transparency, trust, integrity and accountability. In short, to ensure that SIGMA.AI carries out its activity in an ethical environment that respects the external and internal regulations in force.

2. SCOPE OF APPLICATION.

These Rules and Protocol apply to SIGMA.AI, S.L.U.

The SIGMA Management Committee is responsible for approving this policy and for designing the mechanisms for the proper handling of activities related to the management of reports.

The Internal Information Channel may be used by the following persons, hereinafter referred to as “reporting persons”:

- a) Persons who are employees of SIGMA.AI.
- b) External staff such as self-employed workers, as well as any person working for or under the supervision and direction of contractors, subcontractors and suppliers.
- c) Partners or shareholders and persons belonging to the administrative, management or supervisory body of SIGMA.AI, including non-executive members;
- d) Reporting persons who report or publicly disclose information on breaches obtained in the context of an employment or statutory relationship that has already ended, volunteers, interns, trainees, as well as those whose employment relationship has not yet begun, where the information on breaches was obtained during the recruitment process or pre-contractual negotiations.

The reporting person protection measures provided for in the Law shall also apply, where appropriate, to:

- The legal representatives of employees in the exercise of their functions of advising and supporting the reporting person.
- Natural persons who, within the organisation in which the reporting person provides services, assist them in the process.
- Natural persons who are related to the reporting person and who may suffer retaliation, such as co-workers or relatives of the reporting person.
- Legal entities for which the reporting person works, with which they maintain any other type of relationship in a work context, or in which they hold a significant interest as established by the Law.

3. CHANNEL MANAGEMENT.

The purpose of implementing the Internal Information Channel, which is integrated into and forms part of the Internal Information System, is to provide adequate protection against retaliation that may be suffered by natural persons who report any of the acts or omissions referred to in section 4 of these Rules. Likewise, it is enabled for reporting alleged irregularities or disclosing information on acts contrary to the law or to internal regulations of which one becomes aware.

The Channel is designed, established and managed securely, so as to guarantee the confidentiality of the identity of the reporting person and of any third party mentioned in the report, and of the actions carried out in its management and processing, as well as data protection, preventing access by unauthorised personnel.

The directors appoint the Management Committee as the party responsible for the Internal Information System, which in turn delegates the powers to manage the System to the director of the Legal Department.

Once a report of an alleged breach is received, it will be assessed, applying confidentiality to the data provided, and its grounds will be analysed and thoroughly reviewed.

Upon receipt of a report, the person responsible will determine whether it should be processed. If the information is unfounded, the facts lack credibility or do not constitute a breach, it will not be admitted for processing, and the reasons for this decision will be stated.

The investigation of the reported facts will at all times respect impartiality towards all parties involved, such as the business unit or department, the reporting person and the person concerned by the report.

As with any investigation, the process will conclude, whether or not any irregularity has been detected, with a conclusion that may or may not establish the need to take action in response to the report.

4. BREACHES THAT MAY BE REPORTED.

On the basis of the SIGMA Group Code of Ethics and the regulations described in the Introduction, the irregularities that may be reported through the Internal Information Channel include, by way of example but not limited to, the following:

I.- IN GENERAL.

a) Any acts or omissions that may constitute breaches of European Union law under the terms and conditions established in Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption.

b) Acts or omissions that may constitute a criminal offence or a serious or very serious administrative offence. In any case, this includes all criminal offences or serious or very serious administrative offences involving financial loss to the Public Treasury and to Social Security.

II.- IN PARTICULAR.

A. Labour Conflicts.

» Workplace harassment (mobbing).

Action aimed at producing fear or terror in a person or group of persons with respect to their workplace, affecting the dignity of workers and their right to privacy. It may occur vertically or horizontally.

» Sexual harassment.

Abuse by a person in a position of superiority over another, or between equals, in order to obtain sexual favours, violating the other person's sexual freedom.

» Discrimination.

Unequal treatment of a person or group in matters of hiring, treatment and promotion on grounds of race, religion, politics, sex, gender, age, physical or mental condition, etc.

» Abuse of authority.

Abuse of power by managers or supervisors over their employees or collaborators.

» Inappropriate conduct.

Inappropriate conduct that creates an uncomfortable and unsafe working environment.

B. Working conditions.

» Health and safety.

Situations that pose an occupational risk to employees (unhealthy conditions, safety measures, use of helmets and uniforms...).

» Remuneration.

Pay gaps, late payment of salaries, etc.

C. Damage to the environment.

Acts or omissions that have a negative impact on the environment.

D. Human Rights.

Acts or omissions that cause or may cause human rights violations within the company.

E. Privacy and information security.

Misappropriation of information and data of the company, clients, employees, shareholders or suppliers for one's own benefit or that of third parties. Breach of professional secrecy. Breach of processes that manage the confidentiality, integrity and availability of information assets.

F. Intellectual Property.

Actions that infringe brand protection, disclose trade secrets, violate copyright or hinder the fight against plagiarism; as well as infringing the intellectual property rights of other companies.

G. Malpractice.

This includes, on the one hand, giving an incorrect or incomplete description of the company's services and, once the service has been provided, giving erroneous, outdated or subjective information.

H. Disloyal conduct.**» Conflict of interest.**

Situations in which an employee's private interest (personal or financial) influences their professional decisions, such private interest conflicting with the interests of SIGMA.AI.

» Corruption.

Accepting or receiving, or promising, offering, paying, giving or authorising the delivery of gifts, invitations or other incentives to members of another company or public officials with the intention of obtaining a benefit for the company or influencing certain decisions.

» Money laundering.

Introduction into the company of money derived from illegal activities or serious crimes.

» Anti-competitive practices.

Actions that restrict competition in the market: cartels, monopolies, abuse of a dominant position, unfair practices, etc.

» Collaboration with companies engaging in unfair practices.

Collaborating or carrying out transactions with companies linked to money laundering, corruption, anti-competitive practices or terrorist financing.

I. Financial reporting.

Irregularities in the accounts, unauthorised use of funds or resources, waste, etc.

J. Asset fraud.**» External fraud.**

Action by which a third party or person outside the company deliberately acts against the company's interests to deprive it of property, assets or money through deception or other unfair means.

» Internal fraud.

Action by which an employee deliberately acts against the company's interests to deprive it of property, assets or money through deception or other unfair means.

K. Favourable treatment.

Granting privileges, concessions or benefits to a third party outside the company or to an employee.

L. Breach of the law or internal regulations.**» Breach of the law.**

Breach of national, European or international regulations or legislation.

» Breach of regulations.

Breach of SIGMA Group corporate regulations or of the Code of Ethics.

5. NON-REPORTABLE FACTS.

Non-reportable facts are all those not included in section 4 above, or other matters that do not involve irregular or unlawful acts or omissions.

6. REPORTING INFORMATION ON BREACHES.

The persons defined in section 2 may inform SIGMA.AI, through the Internal Information Channel, of the commission of any acts or omissions falling within the scope of these rules (section 4).

At the request of the reporting person, a report may also be submitted at an in-person meeting, within a maximum period of seven days.

When submitting the information, the reporting person may indicate an address, email or safe place for the purpose of receiving notifications, and may also expressly waive receiving any communication on actions carried out by SIGMA.AI as a result of the information.

7. REQUIREMENTS FOR REPORTED INFORMATION.

The information reported must meet the following minimum requirements:

1. If not anonymous, it must include the first name and surname of the reporting person and contact details (email and/or telephone).
2. Identification of the person responsible for the irregularity: name and surname, position held in the company, whether several departments or persons are involved, etc.
3. Conduct or irregularity reported: description of the circumstances of the irregularity, answering questions such as what it consists of, when it occurred, etc.

Where possible, documents or evidence of the reported facts should be attached, especially if the report is anonymous.

8. PRINCIPLES, GUARANTEES AND PROTECTION OF THE REPORTING PERSON.

The procedure shall be governed by the following principles and guarantees, which must be observed at all times:

- Guarantee of confidentiality and protection of the privacy of the persons involved, guaranteeing in all cases the preservation of the identity and personal circumstances of the parties. Compliance with the provisions on personal data protection as provided for in the Law.
- Priority and timely and proper processing.
- Thorough investigation of the facts and their resolution.
- Guarantee of action by adopting the necessary measures.

- Protection against retaliation.

Immediate referral of the information to the Public Prosecutor's Office where the facts may indicate the commission of a criminal offence.

The identity of the reporting person may only be disclosed to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation.

For their part, the reporting person has a duty to act in good faith and to report at least on the basis of reasoned suspicions. Otherwise, disciplinary or sanctioning measures may be taken against the reporting person.

Persons who report or disclose the following are expressly excluded from the protection provided for in Law 2/2023:

- a) Information contained in reports that have been rejected by any internal information channel or for any of the reasons provided for in article 18.2.a) of the aforementioned Law.
- b) Information related to complaints about interpersonal conflicts or that affects only the reporting person and the persons to whom the report or disclosure refers.
- c) Information that is already fully available to the public or that constitutes mere rumours.
- d) Information referring to acts or omissions not included in section 4 of these Rules.

9. PROTECTION AND RIGHTS OF THE PERSON CONCERNED.

During the processing of the file, the persons concerned by the report of breaches shall have the right to the presumption of innocence, the right of defence and the right of access to the file under the terms regulated in these Rules, as well as the same protection established for reporting persons, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

In particular, the person concerned shall have:

» **Right to be informed**, at the time and in the manner deemed appropriate to guarantee the successful outcome of the investigation, that they are involved in an investigation process as a result of a report submitted against them or their conduct.

» **Right of access to the recorded data**, except the identity of the reporting person and of other persons affected by the file, and right to rectify personal data that is inaccurate or incomplete.

» **Presumption of Innocence**. They may provide the documentation and information they consider necessary to prove their innocence.

» **Right to be informed of the resolution**, dismissal or closure of the complaint, where applicable.

» **Right of the person concerned to be informed** of the acts or omissions attributed to them, and to be heard at any time. Such communication shall take place at the time and in the manner deemed appropriate to guarantee the successful outcome of the investigation.

10. PHASES OF THE PROCEDURE FOR PROCESSING AND INVESTIGATING A REPORT SUBMITTED THROUGH THE CHANNEL.

I. REPORTING PHASE

A link will be enabled on the website for submitting reports, which will be managed by the person responsible for the Channel or by specifically designated third parties. Reports may be submitted anonymously or not, as the channel allows both options.

If the report is not made anonymously, the following details shall be included:

- a. Name of the reporting person and national ID number (or similar).
- b. Company to which they belong.
- c. Contact details: telephone, email, etc.
- d. Content of the information, which must describe specifically and precisely the facts, the area affected, the date or period in which they occurred and the possible persons responsible. The reporting person may also attach any evidence available to them.

If the report is submitted anonymously, the reporting person must choose that option in the channel and must not provide their name, ID number or contact details.

The security and integrity of the Channel and the correct recording of the reports received will be guaranteed.

II. ANALYSIS PHASE

a) Receipt and Admission of reports.

Once the information has been submitted, it will be recorded in the Information Management System and assigned an identification code. The Information Management System will be held in a secure database with access restricted exclusively to duly authorised personnel, in which all reports received will be recorded, with the following data:

- a) Date of receipt.
- b) Identification code.
- c) Actions taken.
- d) Measures adopted.
- e) Closing date.

Acknowledgement of receipt will be sent within no more than five working days of receipt of the information, unless the reporting person has expressly waived receiving communications relating to the investigation or SIGMA AI reasonably considers that acknowledging receipt would compromise the protection of the reporting person's identity.

If the report is anonymous, follow-up will be carried out through the link generated for this purpose. The person must take note of the number generated when registering the information as anonymous, which will be used for all procedures and for follow-up purposes; it is therefore their responsibility to keep the number and log in to check the status of their report.

The following are causes or grounds for rejecting a report:

- a) Where the content of the information does not entail a breach of the principles and values defined in the Code of Ethics.
- b) Where the facts reported do not constitute a breach of the legal system falling within the scope of the Law.
- c) Where the report is manifestly unfounded, the facts lack all credibility or there are reasonable indications that it was obtained through the commission of a crime.
- d) Description of the facts in a generic, imprecise or vague manner. Before rejecting a report on this ground, the person responsible for the channel will inform the reporting person of its deficiencies and grant them a period of 5 working days to clarify, specify or properly define the facts referred to. If such deficiencies are not remedied within that period, the report will be rejected. If it is anonymous and does not provide sufficient information to verify the reported facts, it will also be rejected.
- e) Where the report does not contain new and significant information on breaches compared to a previous report for which the corresponding procedures have concluded, unless there are new factual or legal circumstances that justify different follow-up.

In all cases of rejection, the reporting person will be informed in writing, at the contact address they provided, of the reasoned decision to reject. The status will also be changed to “communication”, allowing either the reporting person to accept or not respond to the rejection, in which case it will be closed; or the reporting person not to accept it and submit representations through the channel.

In order to facilitate the analysis of the reports received, the following aspects are established to be taken into account when assessing their importance:

- Number of persons or Departments affected.
- Amount associated with the report.
- Impact on business continuity.
- Damage to the image and reputation of the Organisation.
- Breach of legislation.
- Possible criminal liability arising from the reported fact.

Once this preliminary analysis has been carried out, within a period not exceeding ten working days from the date the information was entered in the register, the following action will be taken:

- Reject the report in the cases outlined in the preceding sections. The rejection will be communicated to the reporting person within the following five working days, unless the report was anonymous or the reporting person has waived receiving communications.
- Admit the report for processing. Admission will be communicated to the reporting person within the following five working days, unless the report was anonymous or the reporting person has waived receiving communications.
- Immediately refer the information to the Public Prosecutor's Office where the facts may indicate the commission of a criminal offence, or to the European Public Prosecutor's Office where the facts affect the financial interests of the European Union.

b) Opening of the file.

If, after analysing the facts contained in the Report, the person responsible for the Channel considers that there are reasonable indications of non-compliance, they will order the opening of a file and the start of the corresponding internal investigation.

III. INVESTIGATION AND INQUIRY PHASE.

a) Internal investigation of the Report.

The person responsible for the Channel or the third parties specifically designated to collaborate in the investigation may gather the information and documentation they consider appropriate in order to determine the certainty or credibility of the reported facts or indications.

A maximum period of three months from the admission of the report is established for carrying out the investigation. This period may be extended by a further period of equal duration where the facts under investigation are complex or require special technical, accounting or IT knowledge, as well as in cases where several reports are joined.

b) Information and hearing.

The inquiry will include all actions aimed at verifying the credibility of the reported facts. It will be ensured that the person concerned by the report is made aware of it, as well as of a brief account of the reported facts. In addition, they will be informed of their right to submit written representations and of the processing of their personal data. Under no circumstances will the identity of the reporting person be disclosed to the persons concerned, nor will they be given access to the report. During the inquiry, the person under investigation will be notified of the report with a brief account of the facts.

The hearing procedure will guarantee the right of the reporting person and of the person concerned to present their arguments, representations and evidence in writing.

IV. RESOLUTION PHASE.

Once all actions have been completed, a report will be issued containing at least:

- o A statement of the reported facts together with the identification code of the report and the date of registration.
- o The classification of the report in order to determine whether or not it has priority in its processing.
- o The actions carried out in order to verify the credibility of the facts.
- o The conclusions reached in the inquiry and the assessment of the proceedings and of the indications supporting them.

Once the report has been issued, one of the following decisions will be adopted:

- a) Closure of the file, which will be notified to the reporting person and, where applicable, to the person concerned. In these cases, the reporting person will be entitled to the protection provided for in the Law and in these Rules.
- b) Declaration of the existence of the breach and proposal of measures to be adopted and, where applicable, the establishment of additional guarantees, such as indicating to which persons or Department heads it is proposed to communicate the content of the resolution.
- c) Referral to the Public Prosecutor's Office if, despite no initial indications that the facts could constitute a criminal offence, this results from the course of the inquiry. If the offence affects the financial interests of the European Union, it will be referred to the European Public Prosecutor's Office.

The period for completing the proceedings and responding to the reporting person, where applicable, may not exceed three months from the entry of the information in the register. Whatever the decision, it will be communicated to the reporting person, unless they have waived this or the report is anonymous.

V.- RETENTION, CUSTODY AND FILING OF INFORMATION.

The person responsible for the Channel will keep an up-to-date record of all reports received, as well as, where applicable, of the internal investigations carried out and the measures adopted, for the periods legally permitted in each case under the applicable regulations.

The information and data will be stored and retained in accordance with the applicable legal requirements and SIGMA's data protection policy, as well as its personal data retention and storage policies.

Possible requests from courts and tribunals as well as from public administrations will be taken into account, under the terms established in the applicable legislation and

for the limitation period of any resulting actions, which is also set out in SIGMA's data protection policies.

Personal data relating to information that does not fall within the scope of the Channel, is not necessary for the investigation and/or is not the subject of investigation will be deleted without delay, except where it is made available to Public Administrations or Judicial Bodies, should it be necessary to address possible liabilities during the corresponding limitation periods.