# INTERNAL REPORTING SYSTEM POLICY

## INTERNAL INFORMATION SYSTEM ("SII")

JULY 2025

TABLE OF CONTENTS

# 1. INTRODUCTION

SERVEIS I ADMINISTRACIONS MASERGRUP S.L.U. (hereinafter "**MASERGRUP**") in accordance with the provisions of both the *Whistleblowing Directive* (EU) 2019/1937 and the Spanish law that transposes it, Law 2/2023, of 20 February, regulating the protection of persons who report regulatory breaches and the fight against corruption (hereinafter, **the** "**Whistleblower Protection Law**"), has implemented an Internal Information System so that any member of MASERGRUP or any third party outside the company who knows of or suspects a regulatory breach can report it internally, either identified or anonymously.

The IIO may also be used to forward to MASERGRUP any queries regarding the scope, compliance and interpretation of the regulations applicable to the company.

MASERGRUP recognises as its own all the principles set out in both the *Whistleblowing Directive* and the Whistleblower Protection Act and, in order to emphasise this commitment, approves this *Internal Information System Policy*, the provisions of which are complementary to those set out in the *Protocol for the management, investigation and response to communications received through the Internal Information System (*"**GIR Protocol**").

## 1.1. OBJECT

The purpose of this Policy is to establish the general principles of MASERGRUP's Internal Information System ("SII" or "**Integrity Channel**"), the rights of whistleblowers, and the procedure governing how they can bring to the attention of the SII Manager any facts relating to the matters referred to in section 2.1 below on the material scope of application.

# 2. SCOPE OF APPLICATION

## 2.1. SCOPE OF APPLICATION

This policy, in accordance with Article 2 of the *Whistleblower Protection Act*, protects individuals who report, through any of the communication channels included in the SII implemented at MASERGRUP, any:

1. Actions or omissions that may constitute **infringements of European Union law**, provided that:

    a. They fall within the scope of the acts of the European Union listed in the annex to *Directive (EU) 2019/1937 of the European Parliament and of the Council* of 23 October 2019 on the protection of persons who report on breaches of Union law, regardless of how they are classified under national law.

    *b.* They affect the financial interests of the European Union as set out in Article 325 of *the Treaty on the Functioning of the European Union (TFEU).*

    c. Have an impact on the internal market, as referred to in Article 26(2) *TFEU,* including infringements of European Union rules on competition and State aid, as well as infringements relating to the internal market in connection with acts that infringe the rules on corporate taxation or practices whose purpose is to obtain a tax advantage that distorts the object or purpose of the legislation applicable to corporate taxation.

2. Actions or omissions that may constitute **a serious or very serious criminal or administrative offence**. In any case, all serious or very serious criminal or administrative offences that involve financial loss to the Public Treasury and Social Security shall be understood to be included.

3. Actions or omissions that may constitute a **breach of the** company's **internal regulations**, including the principles and values that guide the conduct of all its members, among them compliance with current legislation.

4. Any contingency that may pose a **risk to the reputation** of MASERGRUP.

## 2.2. PERSONAL SCOPE OF APPLICATION

This policy applies to all MASERGRUP executives, members and collaborators, regardless of their functions, as well as to third parties, regardless of whether they have already terminated their professional relationship with the company, and who communicate through MASERGRUP's SII on any of the issues indicated in section 2.1. (*"Material scope of* application") .

# 3. INTERNAL INFORMATION SYSTEM ("SII")

## 3.1. INTERNAL INFORMATION CHANNEL

In accordance with Article 8 of the *Whistleblowing* Directive and Articles 6 and 7 of the *Whistleblower Protection Act*, MASERGRUP has set up an Internal Information System ("SII"), also known as the Integrity Channel:

| INTERNAL INFORMATION SYSTEM ("IIS") | |
|---|---|
| **PURPOSE** | › **To report** inappropriate and irregular conduct |
| **AVAILABLE** | › Corporate website<br>› **canalintegridad@masergrup.com** |
| **RESPONSIBLE FOR THE SII** | **Mr. Xavier Grau Beltran**<br>*Compliance Officer* |

Likewise, at the request of the reporting party, a **face-to-face meeting** may be held with the SII Manager to explain or provide further details regarding the facts reported. In this regard, if a report of non-compliance is received and the reporting party fails to file a report, the SII Manager shall be responsible for filing said report through the platform enabled for this purpose. In such a case, verbal communications shall be duly documented in accordance with the provisions of section 8 of this Policy.

Notwithstanding the above, any formal communication from a judicial body or public administration shall be considered a valid means of becoming aware of a breach.

The SII may be used by any person, whether a member of MASERGRUP or a third party outside the company, in particular suppliers and business partners, regardless of whether they have already terminated their professional relationship with.

Communications may be made either **identified** or **anonymously** and will be treated and considered in the same way, and whistleblowers acting in good faith will be protected against any reprisals they may receive because of their communication.

## 3.2. CONFLICTS OF INTEREST AND INCOMPATIBILITIES

In the event of incompatibility or conflict of interest, i.e. if the person affected by the communication is the Head of the SII, the informant may address the communication to **Mr Oscar Canals Morata**. The same shall apply if the Head of the SII is unable to deal with a specific matter and is removed from all processes relating to it.

## 3.3. EXTERNAL CHANNEL FOR INFORMATION AND PUBLIC DISCLOSURE

Without prejudice to the fact that the SII is the preferred channel for reporting actions and omissions that constitute infringements of European Union rights, or serious or very serious criminal or administrative offences, any natural person may directly contact the external information channel created in Spain by the Independent Whistleblower Protection Authority ("**A.I.I**.") – and the competent regional authority, if applicable.

Likewise, the public disclosure or making available to the public of information on actions or omissions constituting a breach of European Union rights, or a serious or very serious criminal or administrative offence, shall also imply the protection of the Whistleblower, provided that they have first reported the matter through internal or external channels, or directly through external channels, without appropriate measures having been taken within the established time limit, and provided that the requirements set out in the following sections are also met.

## 3.4. CONTENT OF COMMUNICATIONS

Communications made through the SII shall contain, as far as possible, the following information:

(i) Name and surname(s) of the person(s) to whom the facts and/or conduct reported are attributed.

(ii) Date of the facts and as much information as possible about them.

(iii) Any documents or other means of proof available to you that may prove the reality of the facts and/or conduct that are the subject of the communication.

(iv) Address, email address or secure location where you wish to receive notifications.

## 3.5. INVESTIGATION PROCEDURE

In accordance with Article 9 of the *Whistleblower Protection Act*, the investigation process that will be followed after receiving a report of a breach will be that set out in the *GIR* Whistleblowing *Protocol* approved by MASERGRUP.

## 4. WHISTLEBLOWER PROTECTION MEASURES

In compliance with Article 6 of the *Whistleblowing* Directive and Article 35 of the *Whistleblower Protection Act*, **whistleblowers shall enjoy all the protection rights** provided for in this policy and in the GIR Protocol, provided that:

(i) They have reasonable grounds to believe that the information they report to MASERGRUP regarding regulatory breaches is accurate at the time of reporting and that the information falls within the scope of this policy.

(ii) They have made the communication through the SII authorised for this purpose by MASERGRUP, as detailed in section 3 "*SII*".

On the contrary, persons who report the following **shall not enjoy the protection** provided for in this Policy:

(i) Information contained in reports that have been **rejected** for any of the reasons set out in Article 18.2 a) of Law 2/2023, namely:

a) When the facts reported lack any credibility.
b) When the facts reported do not constitute an offence under the legal system included in the scope of application of this law or, if they do, do not affect the general interest.
c) When the communication is manifestly unfounded or, in the opinion of the Independent Whistleblower Protection Authority, there are reasonable grounds to believe that it has been obtained unlawfully. In the latter case, provided that access could constitute a crime that is not prosecutable ex officio, in addition to inadmissibility, the case will be dismissed or a detailed report of the facts deemed to constitute a crime will be forwarded to the Public Prosecutor's Office.
d) When the communication does not contain new and significant information on infringements that were the subject of a previous communication for which the corresponding proceedings have been concluded, unless there are new factual or legal circumstances that justify further action. In such cases, the SII Manager shall notify the decision, stating the reasons therefor.

(ii) Information related to complaints about interpersonal conflicts or that only affect the informant, and the persons referred to in the communication or disclosure.

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

(iv) Information relating to actions or omissions not covered by the scope of this Policy.

In addition, the **rejection** of a communication made through the SII shall be communicated to the whistleblower within **five working days**, unless the communication was anonymous or the whistleblower had waived the right to receive communications from the Independent Whistleblower Protection Authority.

## 4.1. PROHIBITION OF RETALIATION

In compliance with Article 19 of the *Whistleblowing* Directive and Article 36 of the *Whistleblower Protection Act*, MASERGRUP will take the necessary measures to prohibit all possible forms of retaliation against persons reporting infringements, including threats of retaliation and attempts at retaliation, against persons who submit a report.

Retaliation is understood to mean any act or omission that is prohibited by law or that, directly or indirectly, involves unfavourable treatment that places the persons suffering it at a particular disadvantage in relation to others in the workplace or professional context, solely because of their status as whistleblowers or because they have made a public disclosure. For the purposes of this Policy, and by way of example, **retaliation** shall include**,** among other things, the following forms of action:

(i) Suspension of the employment contract, dismissal or termination of the employment relationship or statutory , including non-renewal or early termination of a temporary employment contract once the probationary period has been completed.

(ii) Early termination or cancellation of contracts for goods or services.

(iii) Imposition of any disciplinary measure, demotion or refusal of promotion and any other substantial change in working conditions.

(iv) Failure to convert a temporary employment contract into a permanent contract, where the worker had legitimate expectations that they would be offered permanent employment.

(v) Damages, including reputational damage, or economic losses, coercion, intimidation, harassment or ostracism.

(vi) Negative evaluation or references regarding work or professional performance.

(vii) Inclusion on blacklists or dissemination of information within a sector that hinders or prevents access to employment or the contracting of works or services.

(viii) Refusal or cancellation of a licence or permit.

(ix) Denial of training.

(x) or unfavourable or unfair treatment.

The measures set out in points (i) to (iv) shall not be considered retaliation when carried out in the regular exercise of management powers under labour legislation or regulations governing the status of public employees, due to circumstances, facts or proven infringements unrelated to the submission of the communication.

Likewise, it is hereby stated that any person who considers that their rights have been infringed as a result of their communication or disclosure, once the period of two (2) years has elapsed, may request the protection of the competent authority, which, in exceptional and justified cases, may **extend the period of protection**, after hearing the persons or bodies that may be affected (the refusal of such an extension of the period of protection must be justified).

Similarly, any acts intended to prevent or hinder the submission of communications and disclosures, as well as those that constitute retaliation or cause discrimination following the submission of those protected under the Whistleblower Protection Act, shall be null and void and shall give rise, where appropriate, to disciplinary or liability measures, which may include the corresponding compensation for damages to the injured party.

The prohibition of retaliation shall also apply to persons related to the whistleblower who may suffer retaliation in a work context, such as their colleagues or family members. Similarly, protection shall be extended to persons who have assisted the whistleblower in the reporting process.

## 4.2. MEASURES TO SUPPORT WHISTLEBLOWERS

MASERGRUP, recognising the purposes of Article 20 of the Whistleblowing Directive and Article 37 of Law 2/2023, shall ensure that all its members have access, as appropriate, to the following support measures:

(i) **Comprehensive and independent information and advice** on the procedures and remedies available to them in relation to regulatory compliance, protection against retaliation, and their rights as affected persons.

(ii) **Effective assistance**, essentially from the SII Manager, in the event of retaliation.

(iii) **Legal assistance** in any judicial or administrative proceedings that may arise because of their communications.

(iv) **Financial assistance** and support measures in their capacity as whistleblowers, including psychological support in the context of any legal proceedings.

All the above is in addition to any assistance to which the whistleblower may be entitled under *Law 1/1996 of 10 January on free legal aid* for representation and defence in legal proceedings arising from the submission of a report or public disclosure.

## 4.3. MEASURES TO PROTECT AGAINST REPRISALS

In compliance with Article 38 of the *Whistleblower Protection Act*, MASERGRUP shall take the necessary measures to ensure that whistleblowers are protected against retaliation.

The main protection measures provided for by both regulatory bodies are set out below and made known to all potential whistleblowers. Although these measures have yet to be transposed into applicable law, MASERGRUP adheres to them and is committed to facilitating their effective implementation:

(i) Persons who report information on actions or omissions covered by the Whistleblower Protection Act (in short, regulatory breaches) or who make a public disclosure in accordance with it shall not be considered to have infringed any restriction on the disclosure of information, and they shall not incur any liability whatsoever in relation to such communication or public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure of such information was necessary to reveal an action or omission under the Draft Bill, all without prejudice to the provisions of Article 2.3 of Law 2/2023.

The provisions of this section shall extend to the communication of information by representatives of workers, even if they are subject to legal obligations of secrecy or non-disclosure of confidential information. All of the above is without prejudice to the specific protection rules applicable under labour legislation.

(ii) Informants shall not be liable for the acquisition or access to information that is communicated or disclosed publicly, provided that such acquisition or access does not constitute a criminal offence.

(iii) Any other possible liability of whistleblowers arising from acts or omissions that are not related to the communication or public disclosure or that are not necessary to disclose a breach under this law shall be enforceable in accordance with applicable regulations.

(iv) In labour proceedings before a court concerning harm suffered by whistleblowers, once the latter has reasonably demonstrated that they have communicated or made a public disclosure in accordance with Law 2/2023 and that they have suffered harm, it shall be presumed that the harm was caused in retaliation for reporting or making a public disclosure. In such cases, it shall be for the person who took the prejudicial measure to prove that the measure was based on duly justified grounds unrelated to the communication or public disclosure.

(v) In civil or labour proceedings, including those relating to defamation, copyright infringement, breach of confidentiality, breach of data protection rules, disclosure of trade secrets, or claims for compensation based on labour or statutory law, communicators shall not incur any liability as a result of communications or public disclosures protected by this policy.

Such persons shall be entitled to claim as a defence that they made a communication or public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure was necessary to reveal a breach of the provisions of Law 2/2023.

# 5. PROTECTION MEASURES FOR PERSONS CONCERNED BY THE COMMUNICATION

MASERGRUP shall ensure that the persons concerned by the communication (i.e. the alleged *offenders*) are heard in the internal company investigation, where they shall be presumed innocent and shall have the right to access their file to present their version of the facts and provide any evidence, they deem relevant.

Likewise, the identity of the person concerned by the report of an infringement will be protected and treated as confidential, as will the facts reported, in the same way as the identity of the person making the report, always within the limits and exceptions necessary to ensure the proper conduct of the investigation or any communication to the competent authorities.

In this regard, MASERGRUP acknowledges Article 39 of the *Whistleblower Protection Act*, to which it adheres: "*During the processing of the file, the persons affected by the communication 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 this law, as well as the same protection established for whistleblowers, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure*."

## 6. SANCTIONS

In accordance with Article 63 of *the Whistleblower Protection Act*, MASERGRUP, in compliance with the relevant labour legislation and regulations, essentially the Workers' Statute and the applicable collective agreements, shall establish effective, proportionate and dissuasive sanctions applicable to members of the company who:

(i) Prevent or attempt to prevent the reporting of breaches or the raising of doubts regarding *Corporate Compliance.*

(ii) Take retaliatory measures against whistleblowers.

(iii) Promote abusive procedures against whistleblowers.

(iv) Breach their duty to maintain confidentiality regarding the identity of the whistleblower or the persons involved in the communication.

Finally, in accordance with Article 24 of the *Whistleblowing* Directive, MASERGRUP will ensure that the rights and remedies available to all members of the company and third parties in the context of communications regarding regulatory breaches are not limited in any way, and reaffirms that no one may waive their rights of communication by means of any agreement, policy, form of employment or working condition, including any arbitration clauses.

# 7. CONFIDENTIALITY AND PROCESSING OF PERSONAL DATA

## 7.1. CONFIDENTIALITY

In compliance with Article 33 of the *Whistleblower Protection Act*, MASERGRUP undertakes to ensure that the identity of the person making the communication through the SII enabled for this purpose is not disclosed, unless they give their express consent.

The duty of confidentiality means that, except for members specifically authorised to receive, follow up or resolve the communications received, no one may know the identity of the communicator or any other information that can be directly or indirectly deduced from their identity. To guarantee such confidentiality, MASERGRUP has implemented appropriate technical and organisational measures to preserve the identity and ensure the confidentiality of the data corresponding to the persons investigated on the basis of the information provided, in particular the identity of the person making the communication, if they have been identified.

However, there shall be an exception to this duty of confidentiality of identity when disclosure of the identity is a necessary and proportionate obligation imposed by European Union or Spanish law, in the context of an investigation carried out by national authorities or in the context of legal proceedings, and, in particular, when disclosure is intended to safeguard the right of defence of the person concerned. In this regard, the identity of the person making the communication 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.

If the identity is to be disclosed for the above reason, MASERGRUP shall inform the whistleblower in advance, unless such information could compromise the investigation or legal proceedings. In the same vein, when the competent authority informs the whistleblower that their identity has been disclosed, it shall also explain the reasons for the disclosure.

In any case, MASERGRUP shall ensure that the competent authorities receiving information on infringements that include trade secrets do not use or disclose them for purposes other than those necessary for the proper follow-up of the proceedings.

## 7.2. PROCESSING OF PERSONAL DATA

In accordance with Article 34 of the *Whistleblower Protection Act*, MASERGRUP guarantees that the processing of personal data carried out in application of this Policy and the Protocol for the management, investigation and resolution of reports of non-compliance, including the exchange or transmission of personal data with the competent authorities, will be carried out in accordance with Organic Law 3/2018, of 5 December, on Personal Data

Protection and Guarantee of Digital Rights, Regulation (EU) 2016/679 ([1]) and Directive (EU) 2016/680 ([2]).

Likewise, personal data that is not clearly relevant to the processing of a specific complaint will not be collected, and if it is collected by accident, it will be deleted without undue delay.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

# 8. RECORD OF COMMUNICATIONS

In compliance with Article 26 of the Whistleblower Protection Act, MASERGRUP will keep a record of all communications and queries it may receive through the SII, compiled in the so-called "register", always complying with the established confidentiality requirements, and for the time strictly necessary and proportionate to comply with the legal and regulatory requirements of the European Union.

## 8.1. VERBAL COMMUNICATIONS

If the means used by the employee is internal communication through a face-to-face meeting with their superiors, managers or the person responsible for the Internal Information System, MASERGRUP reserves the right to **document the verbal communication**, using one of the following methods, specified in section 4 of *the GIR Protocol* ("Receipt and Registration of Verbal Communications"):

(i) By recording the conversation in a durable and accessible format, or

(ii) Through a complete and accurate transcript of the conversation made by the person and the person responsible for handling the verbal communication. The employee will also be given the opportunity to check, rectify and accept the transcript of the meeting by signing it.

In any case, the company shall ensure that the meeting is kept in a complete and accurate record, in a durable and accessible format.

Only at the reasoned request of the competent judicial authority, by means of an order, and always within the framework of legal proceedings and under the supervision of that authority, may the contents of the register be accessed in whole or in part.

The data contained in this record book shall be kept only for as long as necessary and, in any case, shall not be kept for a period exceeding ten (10) years.

## 9. CHANNEL FOR QUESTIONS AND/OR SUGGESTIONS

Remember that if you have any **questions and/or suggestions** regarding the interpretation and/or application of the content of this Policy, regarding the company's *Corporate Compliance* System, or any other matter related to regulatory compliance, you should immediately contact the *Compliance Officer* by sending an email to the following address provided for this purpose:

**compliance@masergrup.com**

However, the **reporting** or communication of inappropriate, irregular, or un y conduct that may violate the content of this Policy must be reported through the **SII** or **the Integrity Channel** set up for this purpose, as provided for in section 3 of this Policy.

| COMMUNICATION CHANNELS | |
|---|---|
| QUESTIONS AND SUGGESTIONS FROM *CORPORATE COMPLIANCE* | **Consultation Channel**<br>compliance@masergrup.com |
| REPORT INAPPROPRIATE AND IRREGULAR CONDUCT | **SII or Integrity Channel** (*section 3*)<br>Corporate website<br>canalintegridad@masergrup.com |

## APPENDIX I. APPROVAL AND AMENDMENTS

| APPROVAL AND AMENDMENTS | |
|---|---|
| **VERSION NUMBER** | 3 |
| **APPROVED BY** | Sole Administrator |
| **RESPONSIBLE** | SII Manager |
| **DATE OF FIRST APPROVAL** | September |
| **DATE OF FIRST AMENDMENT** | April 2025 |
| **DATE OF SECOND AMENDMENT** | July 2025 |