INFORMATION MANAGEMENT AND CASE PROCESSING PROCEDURE

CONTENTS

1. BACKGROUND

With the entry into force of Law 2/2023, of February 20, regulating the protection of persons reporting regulatory violations and the fight against corruption, EUROSOL, S.A.T., hereinafter also referred to as "the Entity," is obliged to implement an Internal Information System (SII) in accordance with the requirements set forth in the law. The SII is added to the existing Criminal Risk Prevention Plan (PPRP), implemented to prevent criminal risks that may be committed by the Entity as a legal person, pursuant to the requirements of Article 31 bis of the Penal Code.

To integrate both systems, an Integrated Policy for the Internal Information System and Criminal Compliance Management System has been approved. One of its general principles is the existence of an effective and reliable internal information channel applicable to both the PPRP and the SII, enabling the receipt of relevant communications for both systems according to their respective subjective and material scopes.

Thus, a single internal channel has been established—the SII Channel. This procedure aims to define the scope and regulate the process for managing information and processing cases, from the receipt, processing, and investigation of the communication to the adoption of a decision.

The drafting of this procedure complies with the legal requirements arising from Law 2/2023, which are mandatory; the references described for the external information channel in the aforementioned regulation, which ensures procedural guarantees; and the provisions of ISO Standard 19600, which expressly mentions internal information channels as tools for reporting misconduct in Clauses 9.1.3 ("The organization shall establish, implement, evaluate, and maintain procedures to seek and receive feedback from various sources—including employees, through reporting channels…") and 10.1.2 ("An effective compliance management system should include a mechanism for employees and other persons to report actual or suspected misconduct or violations of the organization's compliance obligations, confidentially and without fear of retaliation").

2. OBJECTIVE

The purpose of this document is to establish and regulate the procedure for managing information and processing cases, aimed at receiving, retaining, and processing communications regarding any regulatory non-compliance applicable to the material scope of the SII and the PPRP, as described in Section 4, Internal Channel Configuration, of this document.

This procedure is implemented independently of other communication channels maintained by EUROSOL, such as those related to quality, environmental issues, social responsibility, complaint boxes, claims or suggestions, or any other means.

3. SCOPE

This procedure applies to the EUROSOL body responsible for the SII and PPRP, as well as those who have assumed the responsibilities for managing internal information channels, including the reception, processing, and investigation of the various communications received.

Nonetheless, this procedure includes provisions regarding the configuration and use of the internal information channel regulated herein, which will be made available to informants in a clear and accessible manner at the designated location.

3. INTERNAL CHANNEL CONFIGURATION

4.1 Description of the Internal Channel

An internal information channel is established through which information will be transmitted from the informant to the Compliance Body. The main characteristics that this internal information channel must meet are:

* Early warning system: Enable the early detection of irregularities so that the Compliance Body can promptly obtain any significant information regarding the possible commission of crimes, violations, or the existence of risk situations.

* Promote an ethical culture: Contribute to the development of ethical values and good corporate practices within the Entity.

* Confidentiality: Prevent sensitive information from becoming public and damaging EUROSOL's reputation, without prejudice to the possibility of accessing external information channels or even public disclosure within the scope of the SII.

* Increase trust: Strengthen the trust of employees, related third parties, and stakeholders in the company's compliance level, thereby encouraging its preferential use over external channels.

* Exclusive processing: Ensure that communications are handled solely by the Compliance Body and, where applicable, advisory bodies created or authorized for this purpose.

* Protection and confidentiality: Guarantee the protection and confidentiality of non-anonymous informants.

* Evidence generation and secure records: Generate evidence and ensure the registration of communications and procedures to promote and, if necessary, demonstrate the correct operation of the SII and PPRP.

* Data protection compliance: Comply with data protection regulations, particularly Regulation (EU) 2016/679, of April 27, 2016 (General Data Protection Regulation), and Organic Law 3/2018, of December 5, on Personal Data Protection and the Guarantee of Digital Rights.

4.2 Authorized Persons

The following individuals are authorized to submit communications through the channel if they have obtained information within a professional or employment context, pertaining to the material scope defined in Section 4.4, Subject Matter of Communications:

1. Employees and self-employed workers.
2. Shareholders, members of the Board of Directors, directors, or supervisors, including non-executive members.
3. Volunteers, interns, or trainees, whether paid or unpaid.
4. Individuals who have terminated their employment relationship.
5. Candidates in selection processes or pre-contractual negotiations, who have obtained information during these processes.
6. Any person working for or under the supervision and direction of contractors, subcontractors, and suppliers.

Additionally, EUROSOL users and clients may also use this channel, although they will be outside the scope of the protection provided under Law 2/2023.

4.3 Persons Who May Be Affected

The following individuals may be affected by communications made through this channel:

* EUROSOL staff.
* Senior executives, middle management, and members of the Board of Directors.

4.4 Subject Matter of Communications

Communications may address any action or omission that may constitute a serious or very serious criminal or administrative offense under Spanish law.

Likewise, any action or omission that may constitute a violation of European Union law may be reported, regardless of how such actions are classified under Spanish transposing legislation, provided that they:

1. 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 October 23, 2019, on the protection of persons reporting breaches of Union law.
2. Affect the financial interests of the European Union.
3. Impact the internal market, understood as the space without internal borders where the free movement of goods, persons, services, and capital is guaranteed in accordance with EU regulations.

Additionally, this channel may be used to report any action considered contrary to the Entity's internal regulations, particularly any conduct that could represent a potential breach of the PPRP or the Code of Ethics.
It is important to note that communications whose content falls outside the scope established by Law 2/2023 will be excluded from the protection granted by this law.

4.5 Communication Requirements

Communications may be confidential or anonymous. In the latter case, submitting anonymous information will constitute an explicit waiver of receiving follow-up communications or tracking unless a contact method is provided.

To be accepted and processed, communications must include the following information:

* A concise account of the facts underlying the communication.
* The person or persons against whom the communication is directed, if applicable.
* Documents or evidence related to the reported facts.

4.6 Location of the Channel

The channel is accessible via EUROSOL's website: https://www.eurosol.es/, where a prominent link to the SII will be displayed on the homepage. This link will provide a brief explanation of the channel's purpose and the principles governing the management procedure.

A form will be available for submitting communications, including fields for entering necessary information and uploading documents or images.

In the same location, clear and accessible information will be provided about the existence of external information channels, specifically the channel managed by the Andalusian Anti-Fraud Office as the Independent Authority for Whistleblower Protection (AAI) in Andalusia, accessible via their website: https://antifraudeandalucia.es/.

4.7 Channel Responsible Party

The EUROSOL Compliance Body is responsible for receiving communications submitted through the SII Channel, in accordance with its appointment and the agreement by which it assumes the functions and responsibilities of the SII Responsible Party.

Additionally, EUROSOL may authorize a third party to manage the SII and handle all received information.

5. PRINCIPLES AND GUARANTEES OF THE PROCEDURE

The information management and case processing procedure recognizes the following principles and guarantees:

* Prohibition of retaliation: Any form of retaliation against informants is expressly prohibited, as well as retaliation against the following individuals:
- Legal representatives of workers performing advisory and support functions for the informant.
- Individuals within the organization who assist the informant during the process.
- Individuals related to the informant, such as colleagues or family members.
- Legal entities for which the informant works or maintains any other professional relationship or in which they hold a significant stake.

* Confidentiality and anonymity: Guarantee the confidentiality or, where applicable, anonymity of the informant, as well as the confidentiality of persons affected by the communication. This confidentiality will be maintained even if the information is communicated through other internal channels or directly to non-responsible members of the Entity.
* Continuous communication: Allow the informant to maintain communication with the Compliance Body and provide additional information, provided they have not waived tracking.
* Data protection compliance: Respect and comply with regulations regarding the processing of personal data.
* Timely resolution: The Compliance Body must issue a resolution within a maximum period of three months from the receipt of the communication, except in cases of complexity.
* Legality, typicity, and proportionality: Measures adopted throughout the procedure must be proportionate, necessary, and appropriate, considering the principles that justify them and the objectives pursued.
* Equality and non-discrimination: Respect the right to equality and non-discrimination.
* Labor compliance: Ensure that the procedure and its resolution are aligned with labor regulations and the applicable collective agreement.

The following rights are explicitly recognized for persons affected by communications:

a) Right to presumption of innocence, honor, defense, and hearing of affected persons.
b) Right to confidentiality during the processing of the procedure.
c) Right to notification of the communication, as well as information about the person or persons investigating the facts.
d) Right to submit allegations and maintain their right to defense at all times.
e) Right to propose evidence suitable for determining the facts.
f) Right to intervene in the procedure personally or through a duly authorized representative.
g) Right to dignity and respect for personal and family privacy during the process.

6. INFORMATION RECEIPT

Communications will be forwarded to the Compliance Body and/or the external manager, where applicable, who must:

1. Immediately acknowledge receipt to the informant, indicating that the procedure will follow the established process and that they will be informed of subsequent steps. This acknowledgment must be issued within seven calendar days of receipt unless it compromises the confidentiality of the communication.
In cases of anonymous communication, no acknowledgment will be issued, as the informant has waived the continuation of communication.

2. Open a case file for each communication, identified sequentially for internal control purposes by a unique identification code corresponding to its order of receipt. The files must contain the following information:

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

7. ADMISSION PROCESS

Once the information is registered, the Compliance Body must verify whether the reported facts or conduct fall within the scope defined in Section 4, Internal Channel Configuration.
Following this preliminary analysis, within a period not exceeding 15 business days from the acknowledgment of receipt, the Compliance Body will decide to:

1. Reject the communication for any of the following reasons:
- The reported facts lack veracity or are mere rumors.
- The facts do not fall within the objective scope of the channel.
- The facts are unfounded or show evidence that the information was obtained through the commission of a crime. In this last case, the matter must also be forwarded to the Public Prosecutor's Office.
- The communication does not provide new information compared to a previous communication for which the corresponding procedure has been concluded.

- The information concerns interpersonal conflicts.
- The information is fully available to the public.

If the matter pertains to another internal channel, it will be forwarded to the responsible party for appropriate handling. If it does not fall under such channels but affects one of EUROSOL's departments, it will be referred to Management.

2. Accept the communication for processing: Proceed as outlined in Section 8, Instruction.
3. Immediately refer the information to the Public Prosecutor's Office if the facts may constitute a crime.

In all cases, the informant must be informed of the decision unless it is an anonymous communication, in which case the informant has expressly waived receiving any updates on the procedure.

8. INSTRUCTION

The instruction phase will encompass all actions carried out by the Processing Officer aimed at verifying the accuracy of the reported facts. The Processing Officer may request additional information from the informant, except in cases where the informant has expressly waived further communication as a result of submitting an anonymous report. In such cases, the informant will neither be informed about the status of the procedure nor receive further updates.

8.1. Processing Officer

The Processing Officer will be the Compliance Body, designated for this purpose in accordance with the appointment of the SII Responsible Party.

Additionally, the management of the SII may be outsourced, in which case processing may be delegated to an external third party, without prejudice to the fact that decisions must be made by the Compliance Body.

8.2. Investigation of Reported Facts

The Processing Officer must conduct the investigation confidentially, ensuring appropriate discretion regarding both the reported facts and the identity of the informant and the affected party.

Throughout the investigation, the right to defense and the presumption of innocence of the affected party must be respected at all times.

The Processing Officer may undertake any necessary activities and procedures for the investigation, such as interviewing involved persons or third parties who may have relevant information, commissioning expert opinions or reports, seeking support from the legal department or any other department of the Entity, among others. In any case, Management must facilitate the Processing Officer's tasks by providing the necessary resources to carry out their functions. If necessary, external advisors or specialists may be hired to support the investigation and analysis of relevant matters.

8.3. Notification to the Affected Party for Allegations and Exercise of the Right to Defense

The Processing Officer will inform the affected party of the facts disclosed, allowing them to present any allegations they deem appropriate for their defense and propose and submit supporting evidence.

Without prejudice to the right to submit written allegations, whenever possible and subject to prior recording, an interview will be offered to the affected party to present their version of the facts and provide the evidence they consider suitable and pertinent.

Under no circumstances will the identity of the informant be disclosed to the affected parties, nor will they be given access to the informant's communication. They will only be informed of the communication with a brief summary of the facts and granted access to the file after the identifying information has been removed.

8.4. Evidence Gathering

Upon receiving the allegations and proposed evidence, an evidentiary period will be opened, during which the evidence admitted by the Processing Officer will be examined. Copies of documentary evidence and reports will be retained in the file, while audiovisual or written records of interviews and interrogations will be documented and signed by the declarant and the Processing Officer.

9. CONCLUSION OF PROCEEDINGS

The Processing Officer, once the evidence has been examined, must prepare a final investigation report, which will be submitted to the Compliance Body. This report will include the following information:

* A presentation of the facts reported, along with the identification code of the communication and the date of registration.
* The classification of the communication within the material scope of the channel.
* The actions carried out to verify the veracity of the facts.
* The conclusions reached during the investigation and the assessment of the evidence and indications supporting them.

Based on the final report, the Compliance Body will make one of the following decisions:

1. Case closure: In cases where no infringement is substantiated. The closure will be notified to the informant, provided they did not submit the communication anonymously, and to the affected persons.
2. Referral to the Public Prosecutor's Office: If there are indications that the facts may constitute a crime.
3. Transfer to the Human Resources Manager: If disciplinary measures are deemed necessary. If the final report indicates a breach related to the PPRP, the adoption of disciplinary measures will adhere to the disciplinary regime of the PPRP.
4. Transfer to the Legal Department: If legal measures related to the facts reported in the communication are warranted.
5. Transfer to the competent body: For the adoption of necessary internal control measures.

10. NOTIFICATION OF THE RESOLUTION

Once the conclusion of the proceedings has been made by the relevant body, the informant (unless they have chosen to remain anonymous) and the affected persons will be notified of the investigation results and the resolution by any reliable means.

11. DATA PROTECTION

The processing of personal data derived from the use of the channels will be governed by the provisions of the following regulations:

* Title VI of Law 2/2023, of February 20.
* Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
* Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDDGG).
* Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of preventing, detecting, investigating, and prosecuting criminal offenses and executing criminal penalties.

Consequently, personal data collected within the framework of the internal information channel will present the following characteristics:

* The Data Controller is the governing body in accordance with Article 5.1 of Law 2/2023.
* Data will be lawfully processed as necessary for compliance with the legal obligation established in Law 2/2023, pursuant to Article 6.1(c) of the GDPR and Article 8 of the LOPDDGG.
* Data collected through the ethical channel will be lawfully processed under the performance of a task carried out in the public interest and with the consent of the informant for the specific purpose of processing and investigating potential non-compliance within the Criminal Compliance Management System, as per Articles 6.1(a) and (e) of the GDPR.
* Data will be processed solely for the purpose of handling communications and, where appropriate, investigating the reported facts. Personal data not necessary for the investigation will be deleted.
* Personal data categorized as special will be immediately deleted without being registered or processed.
* Personal data from communications not admitted for processing will not be incorporated into any file and will be immediately deleted. However, data may be anonymized and retained for three months to demonstrate the system's operation.
* Data may be kept in the SII for as long as necessary to decide whether to initiate an investigation into the reported facts.
* Personal data will be deleted three months after receipt if no investigation actions have been initiated. However, anonymized data may be retained beyond three months to demonstrate the system's operation.
* The data subject may exercise their rights to access, rectification, deletion, and objection by contacting the company's data protection mailbox (protecciondedatosexcarmenthyssenmalaga.org).
* The right to access information in the file will be limited to personal data pertaining to the requester, without access to the personal data of other participants or the informant.

* The right to rectification may be exercised when data is inaccurate or incomplete.
* The right to deletion cannot be exercised by any participant during the course of the investigation.
* If the person to whom the reported facts refer exercises the right to object, it will be presumed, unless proven otherwise, that there are overriding legitimate grounds for processing their personal data.

Access to personal data within the channel will be limited, according to their roles and responsibilities, to:

* The System Responsible Party and the person managing the system.
* The Human Resources Manager, only if disciplinary measures against an employee are warranted.
* The Legal Department, only if legal measures concerning the reported facts are required.
* The designated data processor, for instance, in cases of outsourcing.
* The Data Protection Officer, if applicable.

Notwithstanding the above, data processing by other persons or communication to third parties will be lawful if necessary for corrective measures or the processing of disciplinary or criminal proceedings.

Moreover, identified informants have the right to keep their identity confidential from third parties. In any case, the informant's identity may only be disclosed to judicial authorities, the Public Prosecutor's Office, or the competent administrative authority in the context of a criminal, disciplinary, or sanctioning investigation.

In light of the above, EUROSOL will ensure that all necessary technical and organizational measures are adopted to preserve the security, identity, and confidentiality of collected data to protect them from unauthorized disclosures or access.

12. VIOLATIONS OF THE CRIMINAL RISK PREVENTION MODEL

It is an imperative duty for all employees and executives of the Entity to perform their functions in compliance with the law, as well as the internal policies and regulations established in the Code of Ethics and other corporate policies that form part of the Criminal Risk Prevention Model (PPRP). They are also required to act at all times guided by the principles of ethics, integrity, legality, and transparency in all their actions.

Consequently, the commission of a criminal act, activity, or conduct contrary to the company's legal regulations entitles the company to take disciplinary measures against its executives, managers, employees, or workers, including dismissal.

Any conduct that contributes to obstructing or hindering the discovery of or failure to report criminal indications or detected illegal activities to the Compliance Body will be considered a very serious violation, likewise entitling the company to take corresponding disciplinary measures, including dismissal, if applicable.

Disciplinary measures will be adopted following the initiation of the corresponding Disciplinary Proceedings, which may be resolved with the imposition of the sanctions provided for in the Workers' Statute.

If the violation is committed by executives, representatives, agents, or mediators of the company, the corresponding disciplinary proceedings will also be conducted, and the company may act in accordance with the provisions of their respective contracts, including the termination of the relationship.

This disciplinary regime is complementary to any judicial procedure that may be initiated against the professional and/or employee and to any sanction or consequence that may arise from said procedure.

13. APPROVAL OF THE INFORMATION MANAGEMENT PROCEDURE

This Information Management and Case Processing Procedure was approved by the EUROSOL Board of Directors during its session held on June 21, 2023, and will take effect on the date of this document. It will be reviewed annually or whenever circumstances require modification.