# INTERNAL MANAGEMENT PROCEDURE OF THE WHISTLEBLOWER CHANNEL OF ROLTIA INTRALOGISTICS S.L.

**DATE 17-01-2025**

## Index

## 1. INTRODUCTION

**ROLTIA INTRALOGISTICS S.L.** has implemented an Ethical Code or whistleblowing policy that establishes the ethical principles and actions with which it commits to its business activity, and defines the behavioral framework to be followed by the Members of the Organization in the performance of their professional duties.

In the intention to provide an adequate response to any doubt, discrepancy, or irregularity in the compliance with this Code, as well as to collaborate in the monitoring of compliance with the set of applicable norms to our entity and its Members, this Whistleblower or Ethical Channel is activated as a communication and knowledge channel, through the procedure regulated in this document.

The Ethical Channel is, therefore, a confidential and transparent communication means so that both the Members of our entity and other interested parties have an appropriate channel to report any behaviors that may involve irregularities or any act contrary to legality or the behavioral norms of the Ethical Code and other applicable internal rules, whether committed by other Members of the Organization or by representatives or employees of companies collaborating with our entity in its various activities.

Its purpose is to establish the necessary mechanisms to communicate and manage early any issue related to the scope, compliance, or interpretation of the regulations applicable to the Organization, and especially those behaviors from which a crime may derive, potentially leading to **criminal liability for the legal entity**.

The purpose of this document is to develop the procedure for this communication channel.

## 2. DEFINITIONS:

The following are the definitions of the terms that are frequently used in this document:

- **Communication**: a statement in which any Member of the Organization, Business Partner, or Third Party records an issue regarding the scope, interpretation, or compliance with the applicable regulations of the Organization. Depending on its content, a communication may contain either an inquiry or a report
- **Inquiry**: a communication in which any Member of the Organization, Business Partner, or Third-Party requests clarification, a response, or guidance regarding the scope, interpretation, or compliance with the applicable regulations of the Organization.
- **Report**: a communication related to a potential breach of the applicable regulations directed to the Responsible Person for the internal information system.
- **Accused**: An individual or legal entity to whom a potential violation is attributed, and who is subject to investigation by the person responsible for the internal information

system of **ROLTIA INTRALOGISTICS S.L.**

- **Whistleblower**: an individual or legal entity with access to the Ethical Channel who makes a report.
- **Non-compliance**: Behavior, whether active or omissive, that constitutes a violation of the applicable regulations of **ROLTIA INTRALOGISTICS S.L.** Non-compliance can vary in severity, ranging from mere formal breaches of a requirement included in an internal rule to the commission of actions that may constitute a criminal offense potentially attributable to the Organization.
- **Members of the Organization**: The members of the governing body, directors, employees, temporary workers, or those under collaboration agreements, and volunteers of the Organization, as well as others under the hierarchical subordination of any of the aforementioned individuals.
- **Responsible for the Internal Information System**: A single-person or collegiate body, with autonomous powers of initiative and control, entrusted with responsibilities including overseeing the proper functioning of the Organization's Compliance Management System in general.
- **Business Partners**: Any legal or natural person, excluding the Members of the Organization, with whom the Organization has or plans to establish some type of business relationship. By way of example, but not limited to, this includes intermediaries such as agents or brokers, external advisors, suppliers, and clients.
- **Parties affected by this document**: All Members of the Organization as well as Business Partners or Third Parties who have a business relationship with **ROLTIA INTRALOGISTICS S.L.**
- **Third Party**: A natural or legal person or entity independent of the Organization.

## 3. SCOPE OF APPLICATION

This whistleblower channel is established so that various stakeholders, such as Senior Management, Employees, partners, shareholders, members of the organization's governing body, suppliers, representatives of society in general, and anyone working for or under the supervision and direction of contractors, subcontractors, and suppliers, etc., with whom the Organization interacts in a labor or professional context, can communicate their doubts, suggestions, possible irregular behaviors, or any non-compliance with the rules outlined in the Code of Conduct, Anti-Corruption Policy, or any other internal or external regulations.

It is a confidential and even anonymous channel through which any irregular behavior taking place within the Organization can be reported:

The Ethical or Whistleblower Channel must be clearly visible on our entity's website and easily accessible to the members of our entity and/or, if not, in a visible location at the physical premises where the company operates.

## 4. MANAGEMENT OF THE ETHICAL OR WHISTLEBLOWER CHANNEL

The ethical or whistleblower channel is hosted on an external web platform that meets the highest standards of confidentiality and information security, and it also allows for the anonymity of reports and/or inquiries.

The management of the Ethical or Whistleblower Channel is entrusted to an external company with which the appropriate service provision contract has been formalized, ensuring compliance with confidentiality and information security standards for the data received through the whistleblower channel. This entity is responsible for the following tasks:

a. Reception, verification, and handling of communications received.
b. Management and maintenance of the case files and generated records.
c. Review and monitoring of the operation of the Ethical or Whistleblower Channel.
d. Periodic updates of the Procedure.
e. Keeping a register of the information received and the internal investigations initiated as a result.

## 5. PRINCIPLES GOVERNING THE ETHICAL CHANNEL

I. **Obligation to Report**: Members of our organization, as well as other interested parties, who have reasonable and rational indications of the commission of an irregularity or any act contrary to the law or the internal rules voluntarily adopted by the Organization, must report it to the person responsible for the internal information system.

   In the case of individuals with a labor relationship with the Organization, a commercial relationship, or those providing a service, this obligation is considered an essential part of good faith in fulfilling the contract. Therefore, all employees are required to inform the person responsible for the internal information system of any data or indication that a violation of applicable regulations may have occurred or may occur

II. **Guarantee of Confidentiality**: The identity of the person reporting a violation through the Ethical Channel will be treated as confidential information and may even remain anonymous. Therefore, it will not be disclosed to those involved in a verification process.
The data of the individuals making the report may only be disclosed to administrative or judicial authorities, to the extent that they require it as a result of the procedure derived from the report, and to those involved in any subsequent investigation or legal proceedings initiated by and as a consequence of the report. The disclosure of such data will be made in accordance with the legislation on the protection of personal data.
III. **Promotion of the Ethical Channel**: Our organization will promote the dissemination of the existence of this whistleblower channel to improve the functioning of its services, and therefore encourages and promotes its use.
IV. **Protection of the Whistleblower**: Reporting, whether done by individuals outside or within the Organization, is a practice that the Organization encourages and appreciates for the better performance of its business activities. Therefore, no negative consequences will arise for the whistleblower.
V. **False Reports:** A false report is understood as: (1) one that is not based on facts or indications from which an abnormal event or irregular behavior could reasonably be inferred; (2) one made when the author is aware of the falsity of the facts and/or deliberately distorts them. In the event that an investigation confirms that a report has been made in bad faith based on false or distorted information, the employment relationship with the whistleblower will be checked to determine if the Director or HR responsible should be informed so that they can take any disciplinary actions deemed appropriate.

## 6. RECEIPT OF COMMUNICATIONS

Communications to the Ethical Channel or reports can be sent through various channels:

a. **Email**: administracion@roltia.com
b. **Web**: www.eurotransis.com
c. **Phone**: 957529009
d. **Postal Address**: CARRETERA CASTRO DEL RIO Nº 26. APART. 196, 14940, CABRA (CORDOBA)

Attention: SILVIA HURTADO CASADO

## 7. WHISTLEBLOWING MANAGEMENT SYSTEM

It includes the computer tools provided by ROLTIA INTRALOGISTICS S.L. to register and file the communications received and the documentation generated during their processing.

ROLTIA INTRALOGISTICS S.L.'s Whistleblowing Management System has the necessary technical and organizational security measures to ensure the highest possible level of confidentiality. Information containing sensitive personal data will be handled with appropriate security measures in accordance with the provisions of Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights, and Regulation EU 2016/679 of the European Parliament and the Council of April 27, 2016, on the protection of natural persons (hereinafter, GDPR).

The person responsible for the Internal Information System will maintain an updated list of individuals with access to the information contained in the Whistleblowing mailbox, specifying the actions they are authorized to take, if deemed appropriate. Access to the data contained in the whistleblowing processing documents will be strictly limited to personnel carrying out compliance functions, internal audits of the Organization, and, if necessary, external audits.

## 8. PROCESS OF HANDLING RECEIVED COMMUNICATIONS

The handling of received communications must be carried out following these phases:

1. Receipt of the communication.
2. Preliminary analysis of its content.
3. Admission for processing.
4. Registration.
5. Acknowledgment of receipt.
6. Transfer or delegation.
7. Instruction or verification of the facts.
8. Resolution and proposed action.
9. Communication of the resolution to the affected parties.
10. Closing of the file and preparation of reports for the governing bodies.

### 8.1 Receipt of the communication.

Communications to the Whistleblowing Channel can be received through the various means of access to the Channel outlined in section 6 of this procedure.

Once the communication is received, the person responsible for the internal management of the whistleblowing channel will forward it to the Internal Information System Manager, who will act based on its content as follows:

- If the content of the communication is a query, the Internal Information System Manager will respond to the questions raised as soon as possible, through the same channel the query was communicated.
- If the content of the communication suggests the possibility of a breach having occurred or potentially occurring, the communication will be treated as a whistleblowing report and subjected to a preliminary analysis to determine its acceptance, registration, or rejection.

### 8.2 Preliminary analysis of its content.

Any communication referring to a possible breach (i.e., a whistleblowing report) must undergo a preliminary analysis by the Internal Information System Manager to decide on its possible acceptance, registration, or rejection.

The Internal Information System Manager will document the reasons for admitting and registering or rejecting a communication related to a possible breach, through a form, which may contain, depending on the case, the following information:

- Descriptive name of the whistleblowing report, including its unique reference number and the date of receipt.
- Summary of the data provided in the report, distinguishing between objective and subjective data.
- Analysis of the information and documentation sent with the report.
- Evaluation of the content of the report and the reliability of the informant. The anonymity of the informant will, in principle, be considered an indication of lower credibility of the reported facts.
- Decision on the admission of the report for processing, including, if deemed appropriate, the actions to be taken.
- Exceptional measures adopted, if the Internal Information System Manager deems them necessary or appropriate for urgent reasons.
- Appointment of the responsible investigator, if the Internal Information System Manager considers it appropriate to delegate this function.

In this preliminary analysis, it will be evaluated whether to refer any information that is outside the scope of this Channel or requires a different and specific procedure to other relevant entities, if applicable.

If it is a communication that concerns the actions of Partners of our entity,

it will proceed to verify the matter in collaboration with the area that maintains communication with the Partner and, if necessary, it will be forwarded to the person responsible for the Internal Information System performing similar tasks in that entity.

In the case of communications highlighting a malfunction in any Department or Area of the Organization or a breach of commitments with clients, the established channels for handling such complaints or claims will be used, with the informant being notified of the transfer.

It will also be decided whether it is appropriate to merge the instruction with other similar procedures already in progress.

### 8.3 Admission for processing.

The reports must contain the following for their acceptance for processing:

- The facts or behaviors they affect, and their impact on the Organization, the informant, colleagues, Business Partners, or Third Parties.
- The supporting evidence or documentation available (documents, witnesses, etc.).

The lack of identification of the informant will not be a sufficient reason to dismiss the processing of a report.

If the communication is anonymous, the responsible person for the internal information system, in accordance with due diligence, will assess whether to carry out an investigation of the facts or dismiss it without further processing. For this, they must evaluate the apparent veracity of the report and the data or indications provided. In any case, they must document their decision in writing.

No report will be processed in which, clearly, the action it concerns does not constitute behavior that could imply the commission of an irregularity or an act contrary to legality or the behavioral norms included in the Code of Ethics.

### 8.4 Registration.

The complaints admitted for processing will be registered in a logbook with a unique

reference number so that they can be easily located, completing a standardized registration format.

### 8.5 Acknowledgment of receipt.

Once the preliminary analysis of the complaint has been carried out, if the informant is correctly identified, the person responsible for the internal information system will proceed with the acknowledgment of receipt, providing information in any of the following ways: Regardless of the categorization of the communication by the Responsible for the Internal Information System, an acknowledgment of receipt will be sent to the informant within a maximum of 7 calendar days from the reception.

If the complaint is considered irrelevant, unfounded, or not related to the objectives of this Procedure, an informational notification will be sent to the informant.

The informant must also be informed about the transfer to other channels enabled for processing commercial complaints or complaints of any other kind.

If the informant chooses to file an anonymous complaint without providing any contact email, upon completing the communication process, they will receive an acknowledgment of receipt in a pop-up window, in which a reference number will be assigned so that they can obtain information about it in future communications.

Please be aware that if the informant does not provide a contact email (which does not necessarily have to be identifiable), they will not be able to receive communications from our entity about the status of the processing or other communications. However, rest assured that we will respond within the legally established timeframe, and they will be able to track any updates on their complaint by accessing the website link dabocanaldenuncia.com/ROLTIA using the same username and password with which they submitted the complaint and including the reference number.

When the complaint is considered relevant but its content is insufficient, incomplete, or lacks the necessary detail to initiate the case investigation, a notification will be sent to the informant acknowledging the communication and requesting the additional information needed.

When the report is deemed relevant, and the information or documentation provided is sufficient to initiate the corresponding investigation, a notification will be sent to inform the whistleblower about the commencement of the investigation.

ROLTIA INTRALOGISTICS S.L. must ensure the confidentiality of the whistleblower at all times and protect them from retaliation for making a good-faith report. Therefore, the identity of the whistleblower or any circumstances that may make them identifiable will be excluded from the information provided to the accused in the exercise of their right to access.

The deadline to acknowledge receipt of reports to the whistleblower must not exceed seven calendar days.

However, when there is a significant risk that such communication could jeopardize the effective investigation of the facts reported or the collection and analysis of the necessary evidence, the person responsible for the internal information system may include a written justification in the case file to bypass this communication.

### 8.6 Transfer or delegation.

The responsible person for the internal information system may delegate all or part of the investigation phases or request the support of specialists from the relevant areas or subsidiary companies to assist in the investigation of the reports, if applicable.

These investigators must maintain confidentiality and professional secrecy in their involvement and, in all cases, respect the principles outlined in this procedure.

If a report received through the Ethical Channel falls within the scope of the confidential advisory services regarding sexual harassment, the responsible person for the internal information system will promptly forward it to the mentioned Confidential Advisory for processing. The Confidential Advisory will inform the Responsible Person for the Internal Information System of the closure of its procedures so that they can be included in reports to the governing bodies.

If at any point during the process it becomes known that judicial or administrative actions exist for the same facts, the responsible person for the internal information system may decide to suspend the actions of the Ethical Channel and resume them if there are relevant aspects not yet decided in those actions.

### 8.7 Instruction or verification of the facts.

The person responsible for the internal information system must inform the accused of the content of the complaint that affects them, giving them the opportunity to present and prove their position regarding the content.

The instruction will be carried out by the person responsible for the internal information system or the person or persons appointed by them, depending on the type of complaint and the checks that may be necessary. During the instruction, the following actions may be carried out:

**8.7.1.** Request for clarification/additional information: in cases where it is necessary, the person who made the communication will be asked to clarify or supplement it, providing any documents and/or data they may have to support the existence of the irregular action or behavior.
**8.7.2.** Verification of the truthfulness and accuracy of the communication in relation to the described behavior, respecting the rights of the affected individuals. All Members of the Organization are required to collaborate in good faith during the verification process. Testimonies and statements from the affected parties will be treated with strict confidentiality. Notes or reports may be requested from relevant Departments or Areas.
**8.7.3.** Interview with the accused: respecting their rights, they will be informed of the content of the communication so that they can present their version of the events and provide any evidence they may have. Private interviews will also be held with anyone who may be involved. In all cases, a written record of these interviews will be made, which must be signed by those involved at the end of the meetings.
**8.7.4.** Depending on the nature of the investigated facts, interviews may be conducted with the presence of a witness (supervisor, team member, or another person deemed appropriate). In this case, the witness must also sign the meeting minutes.
**8.7.5.** Expert reports from internal or external professionals.
**8.7.6.** Access to documents related to the reported event, including corporate emails of the accused, in accordance with the established rules.
**8.7.7.** Other actions deemed necessary during the processing.

From all the sessions of the investigation and the interviews conducted during the investigation process, the responsible for the internal information system or, where

applicable, the instructor, must keep a written record.

In the case of formal meetings, at the end of each meeting, a summary note will be signed with the agreement, if possible, of all attendees.

### 8.8 Resolution and proposed action.

Once the instruction process is concluded, the person responsible for the internal information system will draft a report and a conclusion or resolution. If an instructor has been involved, they will submit a signed report with their proposed resolution, which must also be ratified by the signature of the person responsible for the internal information system. The resolution document must contain, at a minimum, the following points:

**8.8.1.** Description of the reported case.
**8.8.2.** Actions taken during the file instruction, as well as any relevant documentation analyzed and that may serve as evidence to support the conclusions.
**8.8.3.** Results obtained in the investigation.
**8.8.4.** Assessment or qualification of the verified facts.
**8.8.5.** Proposal, if applicable, of corrective measures, addressed to the person with decision-making and execution authority over them.

The procedure must be completed as soon as possible, not exceeding three months from the receipt of the communication or, if no acknowledgment of receipt was sent to the informant, within three months from the expiration of the 7-day period after the communication was made, unless there are special complexities that require an extension, in which case the period may be extended for a maximum of an additional 3 months.

If the resolution concludes that a Member of the Organization has committed a violation, corrective measures will be applied, and if applicable, it will be forwarded to the Director or responsible person in the Human Resources Area for the application of the corresponding disciplinary measures or, if appropriate, to the Director of the Legal Advisory Area.

If the involvement is of a Business Partner providing goods, services, and/or supplies, the responsible person for the internal information system will forward the matter to the Department or Area that carried out the hiring or is responsible for ensuring compliance with their commitments.

Regardless of the previous measures, if the actions verified are related to an administrative or judicial proceeding, whether or not the Organization is a party, the Legal Advisory Department, if available, and the competent authorities will be immediately informed.

When the content of the report or the investigation reveals the possible existence of significant criminal liabilities that could affect the Organization, the person responsible for the internal information system must immediately inform the entity's governing body, which is responsible for making the appropriate decisions regarding the report after receiving the proper report on its content.

If it is determined that a report was filed in bad faith based on false or distorted information by an employee, this will be reported to the Director or responsible for Human Resources so that they can adopt, if appropriate, the necessary disciplinary measures.

### 8.9 Communication of the resolution to the affected parties.

The responsible person for the internal information system will notify the informant and the accused in writing about the completion of the instruction and its evaluation, indicating whether or not a breach of the applicable regulations to the Organization has occurred, particularly its Ethical Code.

### 8.10 Closing of the file and preparation of reports for the governing bodies.

In any case, a record book will be created from the received communications, their classification, and resolution, without personal data, in order to carry out the corresponding studies and reports and to promote the correction of situations where appropriate.

## 9. PROTECTION OF PERSONAL DATA

### PRIVACY CRITERIA FOR THE ETHICAL OR WHISTLEBLOWER CHANNEL

#### 1. Purpose

The purpose of this section of the Ethical Channel or Whistleblowing procedure is to inform communicants about the processing of the data that will be carried out for the management and processing of the reports submitted through it. To this end, the privacy criteria of the Ethical Channel are also defined on the corporate website.

For the proper configuration and design of the Ethical Channel, the Organization fully complies with the applicable data protection regulations; specifically, Regulation (EU) 2016/679 of the European Parliament and Council, of April 27, 2016, concerning the

protection of individuals with regard to the processing of personal data and the free movement of such data, and its implementing regulations.

Additionally, the Ethical Channel has been designed in accordance with Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights.

## 2. Processing of your personal data and legitimacy

The purpose of the Ethical Channel or whistleblowing system is to manage notifications received regarding non-compliance with the applicable regulations of ROLTIA INTRALOGISTICS S.L., committed by Members of the Organization or Business Partners, investigate the reported facts, and adopt the relevant corrective measures.

It is a confidential communication channel between Members of the Organization, Business Partners, and Third Parties linked to the Organization.

The information contained in the Channel will be deleted three months after the resolution of the case and will be canceled once the legal deadlines have passed, during which administrative or judicial procedures might arise for the legal entity. In any case, this will not occur before 10 years if the complaint is related to money laundering or terrorism financing.

Legitimacy is provided by consent, which has been granted and obtained through the Ethical Channel.

## 3. Recipients of the data

Only the person responsible for the internal information system at ROLTIA INTRALOGISTICS S.L., as well as collaborators authorized by them (unless a management request involves commercial operations where the affected departments or areas must intervene), will have access to the information submitted by the interested party.

The data will not be shared with third parties, except when legally required, in which case the information will be made available to public authorities, judges, and courts, for addressing potential responsibilities.

**4. Exercise of rights**

At all times, the data subject may exercise the rights of access, objection, rectification, and erasure in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and Council and Organic Law 3/2018, of December 5.

In certain circumstances, data subjects may request the restriction of processing of their data, in which case the Ethical Channel will retain them only for the purpose of exercising or defending claims.

When technically feasible, the data subject may request the portability of their data to another data controller.

To exercise these rights, in accordance with the current legislation, data subjects can use the email account roltia@roltia.com, attaching a copy of an identification document (ID or Passport) and expressly stating the right they wish to exercise.

The data subject may file a complaint with the Spanish Data Protection Agency, especially if they are not satisfied with the exercise of their rights. For more details, please visit the website https://www.aepd.es.

**5. Principle of proportionality and data minimization**

- The personal data collected within the framework of the Ethical Channel: Its use will be limited to what is strictly and objectively necessary for processing the reports and, if applicable, verifying the veracity of the reported facts;
- They will always be processed in accordance with the applicable data protection regulations, for legitimate and specific purposes related to the investigation that may arise as a result of the report;
- They will not be used for incompatible purposes;
- They will be adequate and not excessive in relation to the stated purposes.

**6. Limitation of data access**

Access to the data contained in these systems will be strictly limited to the bodies responsible for carrying out the compliance functions, internal audit of the entity, and,

when appropriate, external audit.

Data processing will only be allowed by personnel with management and control functions in Human Resources when disciplinary measures may need to be taken against a Member of the Organization.

Additionally, as indicated, the Organization may rely on third-party professionals, external to the organization, for the provision of certain services related to the management of the Ethical Channel.

### 7. Security and confidentiality measures

The Organization will ensure that all necessary technical and organizational measures are adopted to preserve the security of the recorded data in order to protect them from unauthorized disclosures or access

To this end, the Organization has implemented appropriate measures to ensure the confidentiality of all information and will ensure that data related to the identity of the whistleblower is not disclosed to the accused during the investigation, always respecting the fundamental rights of the individual, without prejudice to any actions that may be taken by the competent judicial authorities.

## 10. COMMITMENTS OF THE COMPLIANCE FUNCTION

The person responsible for the internal information system, as well as those acting on their behalf, and anyone involved in the management and processing phases of the Ethical Channel or in handling communications, must perform their work with the utmost diligence and confidentiality, refraining from disclosing information, data, or records to which they have access during their task, as well as from using them for personal benefit or that of a Third Party.

The person responsible for the internal information system and anyone collaborating in the management procedure of the Ethical Channel must refrain from acting if there is a conflict of interest due to the individuals affected by the communication or the subject matter being dealt with. This should be communicated to the organization's management body, and the processing will be reassigned to a qualified person where such a situation does not arise.

## 11. RELATIONSHIP WITH OTHER EXISTING PROCEDURES

This Ethical Channel should not interfere with the procedures of the Confidential Advisory

Service responsible for handling cases of harassment and/or sexual violence, which will continue to be governed by its specific regulations.

## 12. COMPLIANCE STATEMENT

Since compliance with ethical standards and rules is a commitment of the entire Organization and constitutes a strategic objective for it, all personnel are expected to be aware of and adhere to the content of this Procedure.

ROLTIA INTRALOGISTICS S.L. will take immediate action in response to any breaches of the provisions of this Procedure, in accordance with its internal regulations and within the parameters established by current legislation.

## 13. APPROVAL, ENTRY INTO FORCE, AND UPDATES

This Ethical Channel procedure has been approved by the management and administration body in its meeting on 17-01-2025.

From that moment, it is fully in force in all its terms.

This Ethical Channel procedure must be kept up to date over time. It should be reviewed regularly on an annual basis and, extraordinarily, whenever there are changes in strategic objectives or applicable legislation.

It is the responsibility of the Internal Information System Manager to assess any proposed modifications.

## CHANGE CONTROL

**Version 1.0 approved by the Administration Service**

| Version | Modification Date | Purpose of the Modification | Affected Sections |
|---|---|---|---|
| 2.0 | | | |
| 3.0 | | | |
| 4.0 | | | |