



INTERNAL REPORTING SYSTEM

INTEGRITY CHANNEL POLICY

CONTENTS

1.	INTRODUCTION	3
2.	PURPOSE AND NATURE OF THIS POLICY	3
3.	PERSONAL SCOPE - WHO CAN REPORT	3
4.	MATERIAL SCOPE - WHAT CAN BE REPORTED	4
5.	AVAILABLE CHANNELS	5
6.	GUARANTEES OF CONFIDENTIALITY AND PROTECTION OF IDENTITY	5
7.	SYSTEM MANAGER (RSII)	6
8.	PROTECTION AGAINST RETALIATION	6
9.	PROCEDURE FOR MANAGING REPORTS RECEIVED	7
10.	DISCIPLINARY MEASURES	9
11.	PERSONAL DATA PROTECTION	10
12.	DISSEMINATION AND ACCESSIBILITY	11
13.	ENTRY INTO FORCE, VALIDITY AND REVIEW	11

VERSION CONTROL

Version	Date	Drafted by	Approval date
1.0	31/07/2025	Compliance Officer	31/07/2025
2.0	31/07/2026	Compliance Dept.	05/08/2026

1. INTRODUCTION

Noel Alimentaria, S.A.U. (hereinafter, "the Entity") has a regulatory compliance system structured around the Code of Ethics, the Compliance Policy and the various corporate Policies that implement the Code of Ethics.

Within the framework of this system, and in compliance with **Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption**, the Entity has implemented an **Internal Reporting System (SII)**, which it will call the **Integrity Channel**, and approves this Policy.

In this way, the SII is integrated into the Entity's organisation and management model (criminal compliance programme) and constitutes the channel provided for in **Article 31 bis 5.4 of the Spanish Criminal Code** for reporting potential risks and breaches to the supervisory body.

The Entity states its firm commitment to a culture of integrity, transparency and zero tolerance of any irregular conduct, as well as to the protection of those who report potential infringements in good faith, guaranteeing them protection against retaliation.

2. PURPOSE AND NATURE OF THIS POLICY

The purpose of this Policy is to:

- / Express senior management's commitment to the SII as a tool for the **prevention and detection** of irregularities, not merely as a formal mailbox.
- / Inform all persons within its personal scope of the **existence of the channels** (internal and external) available for reporting.
- / Establish the **guarantees of confidentiality** and the **protection against retaliation** for those who report.
- / Regulate the **procedure for managing the reports received**.

3. PERSONAL SCOPE - WHO CAN REPORT

In accordance with Article 3 of Law 2/2023, any natural person who has obtained information on infringements in a work or professional context with the Entity may report through the SII, regardless of whether the relationship has ended or has not yet begun. In particular:

- / Current employees and staff.
- / Persons whose employment or statutory relationship has ended (former employees).

- / Candidates in selection processes, where the information was obtained during the process.
- / Trainees, interns and volunteers (paid or unpaid).
- / Self-employed persons, consultants and professionals with a contractual relationship with the Entity.
- / Contractors, subcontractors, suppliers and their staff.
- / Shareholders, partners and members of the administrative, management or supervisory body.
- / Persons connected with the above who could suffer retaliation (legal representatives, colleagues, related legal entities), in accordance with Article 3.4 of Law 2/2023.

4. MATERIAL SCOPE - WHAT CAN BE REPORTED

In accordance with **Article 2 of Law 2/2023**, the following actions or omissions may be reported:

- a)** Those that may constitute infringements of **European Union law** falling within the scope of Article 2.1.a of Law 2/2023.
- b)** Those that may constitute a **serious or very serious criminal or administrative offence**. In any case, those involving financial loss to the Tax Authority or the Social Security system.
- c)** Those affecting the **financial interests of the European Union**.

By way of **example and without limitation**, actions or omissions relating to the following areas may be reported:

- | | |
|---|---|
| / Public procurement | / Influence peddling |
| / Financial services, products and markets | / Conflicts of interest |
| / Money laundering or terrorist financing | / Occupational health and safety (prevention of occupational risks) |
| / Product safety and compliance | / Child labour |
| / Transport safety | / Forced labour or human trafficking |
| / Environmental protection | / Workplace harassment |
| / Radiation protection and nuclear safety | / Sexual harassment |
| / Food and feed safety, animal health and animal welfare | / Gender-based harassment or violence |
| / Public health | / Harassment of or violence against LGBTI people |
| / Consumer protection | / Discrimination |
| / Protection of privacy and personal data, and security of networks and information systems | / Moral integrity or Human Rights |
| / Financial interests of the Union and the internal market | / Industrial or intellectual property |
| / Public or private corruption | / Free competition |
| / Bribery | / Subsidies, Tax Authority or Social Security |

5. AVAILABLE CHANNELS

5.1. Internal channel

The Entity makes available to persons within the personal scope an internal reporting channel, established as the **preferred channel**, accessible through the following means:

- / **Platform/application:** [<https://www.noelalimentaria.com/whistle-blowing/>]. Also accessible from the “NoelOne” intranet.
- / **Postal address:** Polígon Industrial Pla de Begudà, s/n; 17857 – Sant Joan les Fonts (Girona), Spain.
- / **In person:** at the reporting person's request, through a meeting with the RSII within a maximum of seven days.

5.2. External channels

Reporting through the internal channel is not a prerequisite for using the external channels. The reporting person may contact directly:

- / The **Independent Authority for the Protection of Whistleblowers, A.A.I. (AIPI)**, or the equivalent regional authority or body (**Anti-Fraud Office of Catalonia**).
- / The competent **institutions, bodies, offices or agencies of the European Union**, where applicable.

6. GUARANTEES OF CONFIDENTIALITY AND PROTECTION OF IDENTITY

1. The Entity guarantees the **confidentiality of the reporting person's identity** and of any third party mentioned in the report, as well as of any information from which their identity could be deduced.
2. Access to the reporting person's identity is **restricted to the RSII** and, where applicable, to the staff strictly necessary for its management, who are bound by a duty of secrecy.
3. The Entity accepts **anonymous** reports.
4. The reporting person's identity may only be disclosed to the **judicial authority**, the **Public Prosecutor's Office** or the **competent administrative authority** in the context of an investigation, and the reporting person will be informed beforehand unless doing so could jeopardise the investigation.
5. The person concerned is guaranteed the following rights: **to be informed of the facts attributed to them and to be heard**, at a time and in a manner that does not jeopardise the investigation; **to the presumption of innocence, honour and defence**; to access the file, excluding the identity of the reporting person and of third parties; and to the rectification of inaccurate data.

7. SYSTEM MANAGER (RSII)

The RSII is the company's Compliance Committee, a collegiate body currently made up of five members. In accordance with Article 8.2 of the Whistleblower Protection Law, this collegiate body has delegated to its Chair the powers to manage the Reporting Channel and to process investigation files.

The RSII:

- / Performs its duties with **full independence and autonomy**, without receiving instructions of any kind in doing so.
- / Is the **ultimate guarantor** of the System's operation and the only person authorised to manage reports.
- / Is available for **enquiries** at: compliance.penal@noel.es

If the RSII has an incompatibility or conflict of interest with the facts or persons that are the subject of the report, it will abstain from taking part in managing and processing the report and will therefore have no access to information arising from the actions taken in its management. In such cases, the RSII will be replaced by another person appointed from within the Compliance Committee.

8. PROTECTION AGAINST RETALIATION

The Entity **expressly prohibits any retaliation** against anyone who reports in good faith through the SII, provided that the following conditions are met:

- a) they have reasonable grounds to believe that the information was true at the time of reporting or disclosure, even if they do not provide conclusive evidence, and that the information falls within the scope of this Policy;
- b) the report or disclosure was made in accordance with the requirements set out in this Policy.

By way of example and without limitation, the following forms of retaliation are prohibited (Article 36.1 Law 2/2023):

- / Suspension of contract, dismissal, termination of the relationship or removal from office.
- / Imposition of disciplinary measures.
- / Demotion or denial of promotion.
- / Change of position, duties or place of work, reduction in pay or change in working hours.
- / Denial of training.
- / Negative performance assessments or references.
- / Reputational damage, financial loss, coercion, intimidation, harassment or ostracism.
- / Discrimination or unfavourable or unfair treatment.
- / Failure to convert a temporary contract into a permanent one, where there was a legitimate expectation.

- / Failure to renew, or early termination of, a temporary contract.
- / Blacklisting or damage (including reputational damage) on social media.
- / Early termination or cancellation of contracts for goods or services, and revocation of licences or permits.

Support measures. The Entity recognises that the reporting person will have access to the support measures provided for in **Article 37 of Law 2/2023**(information, advice, assistance and any others that apply), managed by the competent authority.

Persons who report or disclose the following are expressly **excluded from the protection provided**:

- a)** Information contained in reports that have been rejected by an internal reporting channel or for any of the reasons set out in Article 18.2.a).
- b)** Information linked to complaints about interpersonal conflicts or that only affects the reporting person and the persons referred to in the report or disclosure.
- c)** Information that is already fully available to the public or that amounts to mere rumour.
- d)** Information relating to actions or omissions not covered by Article 2.

9. PROCEDURE FOR MANAGING REPORTS RECEIVED

9.1. Report requirements

The report should contain, as far as possible:

- / Identification of the reporting person and contact details, unless the report is anonymous (contact details optional).
- / Type of infringement being reported.
- / Description of the facts: what they consist of, when they occurred and, if possible, the persons or areas involved.
- / Supporting evidence or documents, if available, and identification of possible witnesses.

9.2. Process stages and time limits

The process is structured in four stages:

Stage 1 Receipt and registration

- / The report is received through any of the enabled channels and is **registered** in Centinela, which marks the start of the time limits and its entry in the register.
- / **Acknowledgement of receipt** to the reporting person within a maximum of seven calendar days from receipt. For anonymous reports, the acknowledgement is made available through Centinela's secure link.

Stage 2 Analysis and admission decision

- / The RSII analyses the report to decide whether to **admit it for processing** (Validation status) or **reject it** with reasons (Non-validation status).
- / **Grounds for rejection:** the facts clearly fall outside the material scope of Article 2 Law 2/2023; they are manifestly unfounded; or the description is so general or imprecise that it prevents any action. (A mere lack of documentary evidence is not grounds for rejection.)
- / If the report is rejected, the reporting person is informed in writing and has 10 days to submit observations through the channel. Once the rejection is accepted, or the period ends without observations, the report is closed.
- / On admission, the adoption of urgent **precautionary measures** to protect the reporting person or the course of the investigation is considered.
- / Where the reported facts relate to a breach of the **Protocol for the prevention of and response to workplace harassment, the Protocol for the prevention of and response to harassment based on sexual orientation, gender identity, gender expression or sex characteristics, or the Protocol for the prevention of and response to sexual or sex-based harassment in the workplace, the RSII will immediately refer the matter to the Committee appointed** for this purpose so that the report is processed in accordance with the relevant Protocol.

Stage 3 Investigation

- / The RSII gathers the information and documentation needed to establish the credibility of the facts. The RSII will hear all persons concerned and any witnesses and will carry out whatever steps it considers necessary (review of documentation, obtaining information from external sources, etc.). The participation of witnesses and persons concerned will be strictly confidential. The RSII may obtain any information and documentation it considers appropriate from any area or department of the organisation in order to substantiate the investigation. All members of the organisation are required to cooperate fully and in good faith with the investigation.

Likewise, as part of the investigation, the RSII may request, on its own initiative or at the request of a party, any reports, documents, records or other relevant data, and may seek technical or legal analysis from internal or external experts where the complexity or nature of the facts so advises. All of this will always guarantee confidentiality, impartiality and the adoption of measures to protect the reporting person and the rights of the persons concerned.

Written minutes will be taken of all investigation actions and, in particular, of the explanations/statements given by the persons involved in the investigation of the report (provided their prior consent is obtained). The minutes will be duly signed by those involved to certify their content and that it accurately reflects their statement.
- / **Hearing:** the person concerned is informed and given a genuine opportunity to respond in writing before any proposed resolution, provided this does not obstruct the investigation.

- / The **presence of external legal advisers** will be permitted at hearings/statements of the parties concerned, interested parties, witnesses, etc., if the RSII considers it appropriate.
- / **Evidence management:** evidence is collected, preserved and documented to ensure its integrity. If the facts could constitute a criminal offence, the chain of custody will be preserved and the legal adviser will be consulted before any action that could affect its evidential value.
- / **Time limit:** this stage has no specific time limit in the Law, but falls within the overall maximum resolution period.

Stage 4 Resolution and communication

- / A **report of findings** is issued, including: a description of the investigation, the facts established, an assessment (whether or not there is an infringement/evidence of an offence) and, where applicable, the proposed measures.
- / **Maximum resolution period:** three months from receipt of the report, exceptionally extendable by a further three months in particularly complex cases, with reasoned notification.
- / **Communication of the outcome** (Communication status) to the reporting person and the person concerned, subject to confidentiality safeguards.
- / **Evidence of an offence:** where the facts may constitute a criminal offence, the RSII will immediately forward the information to the Public Prosecutor's Office; if they affect the financial interests of the EU, to the European Public Prosecutor's Office. In such cases, it may refer the report directly to the governing body.
- / **Disciplinary integration:** findings that involve liability are referred to the People Department for application of the disciplinary regime. Retaliation against the reporting person is considered a very serious offence for disciplinary purposes (Article 63 Law 2/2023).

10. DISCIPLINARY MEASURES

Where it is determined that the reported conduct constitutes an employment-related infringement, NOEL may adopt the appropriate measures in accordance with the applicable Collective Agreement and the Spanish Workers' Statute.

Without prejudice to compliance in all cases with the employment legislation in force at any given time, and insofar as it allows, the following criteria, among others, may be considered when assessing the seriousness of conduct for the purpose of grading the sanctions to be imposed:

- / Degree of intent;
- / Failure to heed previous warnings;
- / Repeat offending;
- / Several infringements in the same act or activity;
- / Concealment in the conduct of the offender;

- / Continuity in the conduct of the offender;
- / Remedy of the breach that gave rise to the infringement on the offender's own initiative;
- / Repair by the offender of the damage or harm caused;
- / The offender's level of responsibility within the organisation;
- / Scale of the financial loss resulting from the infringement;
- / Scale of any other harm resulting from the infringement that cannot be assessed financially;
- / Impact on other employees or third parties;
- / Cooperation with the organisation.

Notwithstanding the adoption of disciplinary measures, where the facts may constitute a criminal offence, the relevant information will be forwarded immediately to the Public Prosecutor's Office. Where the facts affect the financial interests of the European Union, it will be forwarded to the European Public Prosecutor's Office.

11. PERSONAL DATA PROTECTION

The processing of personal data arising from the SII is governed by the **GDPR (EU) 2016/679**, **Spanish Organic Law 3/2018 (LOPDGDD)** and **Article 32 of Law 2/2023**.

Data controller	Noel Alimentaria, S.A.U., tax ID A17014713, registered office at Pol. Ind. Pla de Begudà, s/n - 17857 Sant Joan les Fonts, Spain.
Purpose	management and processing of reports received through the SII.
Legal basis	compliance with a legal obligation (Article 6.1.c GDPR , in relation to Law 2/2023).
Access to data	<p>Access to the personal data contained in the Integrity Channel will be limited, within the scope of their powers and duties, exclusively to:</p> <ul style="list-style-type: none"> a) The System Manager and whoever manages it directly. b) The external adviser involved in the investigation, with whom the corresponding confidentiality agreements will be signed. c) The head of the People Department or the duly appointed competent body, only where the reported infringement relates to the Workplace and Sexual Harassment Prevention Protocol or where disciplinary measures against an employee may be appropriate. d) Any data processors that may be appointed.

Retention

Personal data relating to reports received and internal investigations will only be kept for as long as is necessary and proportionate to comply with Law 2/2023. In particular, data will be kept only for the time strictly necessary to decide whether to open an investigation and, in any case, **no longer than three months** from receipt if no action has been initiated, unless retained to evidence the operation of the System (Article 32.2 Law 2/2023). Under no circumstances may data be kept for more than ten years.

12. DISSEMINATION AND ACCESSIBILITY

This Policy will be published in a visible and easily accessible place on the corporate website and on NoelONE, avoiding locations that are hard to find.

In addition, it will be expressly communicated to:

- / Suppliers and third parties at the start of the contractual relationship.
- / The entire organisation after each significant update.

13. ENTRY INTO FORCE, VALIDITY AND REVIEW

This Policy will enter into force on the date of approval, amendment or update of this document and will remain in force until repealed.

This Policy must be reviewed periodically in order to identify possible weaknesses or areas for improvement and to update and/or improve its provisions. On an extraordinary basis, this Policy will be reviewed and, where appropriate, amended when significant legal, organisational or other circumstances arise that justify its immediate adaptation and/or update.