WHISTLEBLOWING INFORMATIVE REPORT _CENTRALFIN SRL

The Legislative Decree No. 24 of March 10, 2023 (hereinafter referred to as the "Whistleblowing Decree"), implements EU Directive 2019/1937 and came into force from Marc 30,2023.

The term "Whistleblowing" refers to the spontaneous disclosure by an individual, called "whistleblower," of a wrongdoing or irregularity committed within the entity, which he or she witnessed in the course of his or her duties.

The whistleblower is often an employee, but can also be a third party (a supplier).

This legislation, applicable with respect to Centralfin srl group (AFC srl, CSA Spa, Central Shipping Agency Spa, Portital srl, Intermedri srl), **governs the protection of persons who report violations** of national or European Union regulatory provisions that harm the public interest or the integrity of the public administration or private entity, of which they have become aware in a public or private employment context.

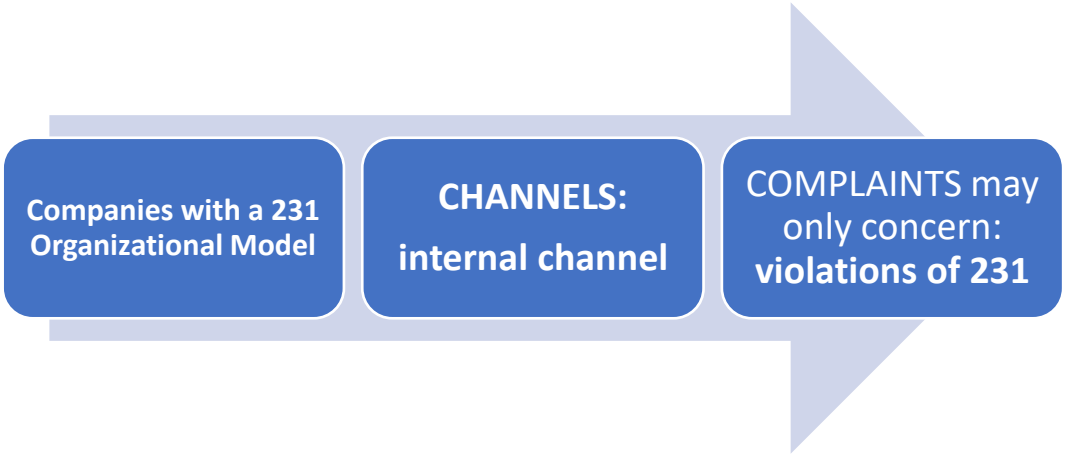
Pursuant to Article 5 of the Decree, workers have the right to be informed as to what violations can be reported and what methods and procedures need to be followed in order to report such violations of which they have become aware. This notice, therefore, serves that specific purpose.

WHO CAN REPORT VIOLATION

All individuals who **have an employment relationship** in any capacity with **the single company**, for instance:

- **employees**
- **trainees;**
- **collaborators**;
- **consultans** who perform self-employment activities in favor of the company;
- **Candidates** who, although they have not yet established an employment relationship with the company, have undertaken with it a selection process aimed at starting the same.

WHICH VIOLATIONS MAY BE REPORTED AND CHANNELS TO USE.



Only violations of which the reporting person has definite knowledge or of which the reporting person has a reasonable suspicion because it is based on definite and concrete facts may be reported.

The report must be accurate as well as complete, and the following essential elements must be clear, including for the purpose of screening for admissibility:

1. **identifying data of the reporter**, as well as an address to which updates can be communicated,

2. **the circumstances of time and place** in which the event occurred and its **detailed description** (manner, place and date);

3. the **generalities or other elements** that enable the identification of the person to whom the reported facts can be attributed.

In addition:

- the reason for the report;

- the nature and content of the violation;

- The names of the persons involved as well as any witnesses or persons informed of the facts;

In contrast, the following are not reportable violations:

- - disputes, claims or demands relating to an interest of a personal nature of the person making the report;
- - disputes, claims or requests that relate exclusively to the employment relationship of the person making the report and to relations between him/her and his/her hierarchical superiors;
- - complaints, claims or requests that are general in nature or otherwise not specifically related to any of the violations listed above;
- - reports relating to classified information (thus covered by secrecy by the Italian state or internationally), covered by forensic or medical secrecy or covered by the principle of secrecy of the deliberations of judicial bodies.

Important: Where an employee believes that he or she **has suffered violations of his or her personal interest,** or within **the scope of his or her employment relationship,** or even **in managing relations with his or her supervisor, he or she will always and in all cases be required to use the ordinary remedies and protections,** i.e., confrontation with his or her employer, the HR department, and possibly the assistance of labor unions or recourse to legal assistance**.**

HOW TO REPORT

There are 3 channels for making the report:

1. reporting through the **internal channel**,
2. reporting through an **external channel**,

1	ANAC
2	Legal Authority

3. **Public disclosure**

The channel to be favored is the INTERNAL channel.

INTERNAL CHANNEL

The Reporting Channel is managed by an **independent and certified external company**, which has established a channel for written reports for this purpose, which will then be sent to the internal functions in charge.

1	***Landing page***	Dedicated web page
2	***PO BOX***	Audit People S.r.l – Società Benefit

		PO BOX n. 301 c/o **centro Mail Boxes Etc. 0197** Address (**via Cenisio 37 - 20154 Milano)**: IMPORTANT: specify the corporate name of your organization
3	***Toll-free number***	800 985 231 with voice messaging (valid for Italy only)

It is critical that **EthicPoint** experts be contacted **before any action is taken** so they can provide all the necessary information

MANAGEMENT OF THE REPORT

EthicPoint takes charge of the report, which is forwarded to the internal functions in charge, issuing the reporting person with an **acknowledgement of receipt of the report within 7 days** from the date of receipt and giving evidence to the internal WhistleB. team.
The internal functions shall diligently follow up the reports received, through constant discussion with the EthicPoint, **providing feedback within 3 months** from the date of the notice of receipt of the report or, in the absence of such notice, within 3 months from the expiration of the 7-day period from the submission of the report. Acknowledgement is provided to the reporter through the e-mail address:
centralfin@ethicpoint.eu
centralshippingagency@ethicpoint.eu
csa@ethicpoint.eu
finanzaecontrollo@ethicpoint.eu
portital@ethicpoint.eu
intermedri@ethicpoint.eu
or **through the references that the reporter will eventually forward in the opted reporting mode.**
All information will be handled in accordance with the whistleblower protection provisions.
If indispensable, internal functions request clarifications from the reporter or any other parties involved in the report, with the necessary precautions taken.
They shall also verify, in cooperation with EthicPoint, the substantiation of the circumstances represented in the report through any activity deemed appropriate, including the acquisition of documentation and the hearing of any other individuals who may report on the facts reported, while respecting the principles of impartiality, confidentiality and protection of the identity of the reporter.

Verification of the merits of anonymous report

The Company's verification of the merits of the report is similar for both confidential and anonymous reports. However, the following guidance will be taken into account for **anonymous reporting**:

- the need for greater depth in verifying the elements that exclude direct filing.
- contact of the whistleblower if technically possible.

In the event that the report is found to be **inadmissible**, the individuals in charge of handling the report **may proceed to file it**, while still ensuring the traceability of the supporting reasons.

Storage of the report for UNFOUNDEDNESS.

The Company, on the basis of an assessment of the facts that are the subject of the report, may decide, in the case of obvious and **manifest groundlessness, to dismiss the report, giving feedback to the reporter**.

The Company orders the direct filing of reports in cases of:

- manifest lack of interest in the integrity of the Company;

- manifest groundlessness due to the absence of factual elements suitable to justify investigations**;**

- manifest lack of legal prerequisites for the application of the sanction**;**

- manifestly emulative purpose;

- ascertained generic content of the report or such as not to allow understanding of the facts, or report accompanied by inappropriate or irrelevant documentation;

- production of documentation but **without the reporting** of **illegal conduct or irregularities;**

- lack of data that constitute **essential elements of the Report.**

Procedure for handling substantiated reports.

In case there is **evidence that the fact is not manifestly unfounded**, the internal functions in charge, having started the internal investigation of the reported facts and conduct, shall inform:

1	Board of directors
2	Board of auditors (where applicable)

PRESERVATION/STORAGE.

Personal data relating to reports and related documentation are retained and maintained for the period necessary to complete the verification of the facts set forth in the report and **for a subsequent 5 years after the closure of the report**, **except for any proceedings arising from the handling of the report** (e.g., disciplinary, criminal, accounting) against the reported person or the reporter (e.g., bad faith, false or defamatory statements). In this case, they will be retained for the duration of the proceedings and until the expiration of the time limit for appealing the relevant measure. Personal data that are manifestly not useful for the processing of a specific report shall not be collected or, if accidentally collected, shall be deleted immediately.

PROTECTIVE MEASURES FOR THE REPORTING PERSON AND LIMITS

The reporting person **may not be subject to retaliation** because of the report made and as such is protected. The protection measures apply under the following conditions:

(a) at the time of reporting, the reporting person had reasonable grounds to believe that the information about the reported violations was true and fell within the scope of reportable violations;

(b) the public reporting or disclosure was made using the Internal Reporting Channel or alternatively the External Reporting Channel, if the conditions for its use are met.

Retaliation is considered to be any conduct, action or omission, even if only attempted or threatened, put in place because of the report and which causes or may cause the reporting person, directly or indirectly, unjust harm. Acts carried out for retaliatory purposes are null and void.

Important: The reporting of alleged violations that the reporter did not have probable cause to believe to be true or that could not reasonably be expected to fall within the scope of reportable violations **deprives the reporting person of the aforementioned protections and exposes him or her to actions that may be of a disciplinary nature within the employment relationship as well as civil, criminal, and administrative**.

The protection does not apply in cases where the report contains false information made with malice or gross negligence.

DUTY OF CONFIDENTIALITY

The objective of this procedure is to ensure the protection of the Whistleblower, keeping his or her identity confidential, only in the case of reports coming from identifiable and recognizable individuals.

Anonymous reports, where these are punctual, adequately substantiated, supported by appropriate documentation and made with an abundance of detail, that is, where they are able to bring out facts and situations by relating them to specific contexts, are equated with reports with an exposed reporter as well as their treatment, even if interlocution with the anonymous reporter is not possible after the report itself. Anonymous reports are also subject to this procedure, to the extent applicable.

In any case, anonymous reports should be recorded by the reporting manager and the documentation received should be retained, since-if the anonymous reporter is later identified and has suffered retaliation-the protections provided by the regulations should be ensured.

The identity of the reporting person and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the reporting person, to persons other than those responsible for receiving or following up reports and expressly authorized to process such data.

In criminal proceedings, the identity of the whistleblower is covered by secrecy as per Article 329 of the Code of Criminal Procedure

In the context of disciplinary proceedings, the identity of the reporting person may not be disclosed, where the disciplinary charge is based on investigations that are separate and additional to the report, even if consequent to the report. Where the charge is based, in whole or in part, on the report and the knowledge of the identity of the reporting person is indispensable for the defense of the accused, the report will be usable for the purposes of disciplinary proceedings only if the reporting person expressly consents to the disclosure of his or her identity.

RESPONSABILITY OF THE WHISTLEBLOWER.

This policy is without prejudice to **criminal, civil and disciplinary liability in the event of libelous or defamatory reporting,** including under the Criminal Code and Article 2043 of the Civil Code**.**

Any forms of abuse of this policy, such as reports that are manifestly opportunistic or made for the sole purpose of harming the whistleblower or others, and any other hypothesis of improper use or intentional instrumentalization of the Company subject to this procedure, as well as unfounded reports made with malice or gross negligence, are also a source of liability in disciplinary and other competent venues.

SANCTION SYSTEM

An effective whistleblowing system must provide for sanctions both against the Whistleblower, in case of abuse of the reporting tool, and against the reported persons in case of a finding of the reported wrongdoing in accordance with the provisions of the applicable legislation, including applicable collective bargaining, and

specifically Legislative Decree 24 of 2023 on the protection of persons who report violations of Union law and national regulatory provisions.

EUROPEAN PRIVACY REGULATION 679/2016

Any processing of personal data will be carried out by the company in compliance with Regulation (EU) 2016/679, Legislative Decree No. 196 of June 30, 2003, and Legislative Decree No. 51 of May 18, 2018. Personal data that are manifestly not useful for the processing of a specific report shall not be collected or, if accidentally collected, shall be deleted immediately. The processing of personal data related to the receipt and handling of reports shall be carried out by the company, as the data controller, in compliance with the principles set forth in the aforementioned legislation, providing appropriate information to the reporting persons and the persons involved as well as taking appropriate measures to protect the rights and freedoms of the data subjects.