WHISTLEBLOWING PORTAL – Frequently Asked Questions

What is Whistleblowing?

Whistleblowing is the mechanism that protects individuals who report irregularities or situations of danger or risk within the organisation they belong to, which could potentially harm the organisation or third parties. Legislative Decree No. 24 of March 10, 2023, implementing Directive (EU) 2019/1937 on Whistleblowing, introduced unified regulations for reporting channels and the protections afforded to whistleblowers in both the public and private sectors, including the FiberCop Group.

Who can report a violation?

Anyone can submit a report, including employees, former employees, job applicants, shareholders, customers, partners, suppliers (including subcontractors), independent contractors or collaborators, freelancers, consultants, agents, intermediaries, volunteers, and interns (paid or unpaid), or anyone with a legitimate interest in the business activities of the FiberCop Group.

What can be reported?

Whistleblowing involves reporting improper or illegal conduct within the company. This may include violations of laws and regulations, the Code of Ethics, company procedures, or the system of rules and procedures in place within the company, as well as incidents of equal opportunity violations, such as discrimination or abuse. Reports may concern both FiberCop personnel and third parties (e.g., suppliers and external collaborators).

Reports do not include commercial complaints, disputes, or requests related to personal interests, for which other dedicated channels are available.

It is essential that reports are adequately detailed, containing sufficient specifics to reveal precise, consistent, and context-related circumstances and facts, as well as to identify elements useful for verifying the validity of the report (e.g., details identifying the individuals involved, the context, location, timeframe of the reported incidents, and supporting documentation).

Which channels should be used to submit a report?

The internal reporting channels provided by FiberCop are indicated on the “Whistleblowing” page available on both FiberCop’s website and the company intranet. The preferred channel is the online portal, as it ensures maximum confidentiality of the whistleblower’s identity through the use of secure protocols and encryption tools.

Reports can also be submitted via a dedicated toll-free number, by sending a letter to FiberCop’s Supervisory Body, or through a direct meeting with Internal Audit personnel.

How can I access the Reporting Portal?

The online portal is accessible via the “Whistleblowing” page on both FiberCop’s website and the company intranet. Upon submission, the whistleblower must note the date and the Unique Identification Code (an alphanumeric ticket that uniquely identifies the report) automatically generated by the portal. This code allows tracking of the report’s processing status and facilitates anonymous communication regarding the report. Supporting documentation can also be attached to the report, even after submission.

Who receives the reports?

Reports are received by FiberCop's Internal Audit Department for preliminary investigations. Within 7 days of receiving the report, the whistleblower is notified of receipt. Within 3 months of this notice (or, if no such notice is provided, within 3 months from the 7-day deadline following the report's submission), feedback is provided on the actions taken or planned, specifying whether the report falls within the scope of Legislative Decree No. 24 of March 10, 2023.

I received a report from a third party. What should I do?

Anyone receiving a report, in any form (written or oral), must forward it promptly—no later than 5 days from its receipt—through internal reporting channels, notifying the whistleblower (if known) of the transmission and ensuring complete confidentiality. The original report, including any supporting documentation, must be forwarded, along with evidence of notification to the whistleblower regarding the transmission. Copies of the original must not be retained, and any digital copies must be deleted. The recipient must refrain from conducting any independent analysis or investigation. Failure to report a received notification and breaches of confidentiality obligations constitute violations of the Whistleblowing Procedure and may result in disciplinary action for employees.

What protections are in place?

- Subject to legal obligations, the whistleblower's identity and any information that could directly or indirectly identify them cannot be disclosed without their explicit consent. Confidentiality is also guaranteed for individuals involved and/or mentioned in the report and for facilitators (i.e., those who work in the same context and assist the whistleblower in the reporting process).

- Any retaliatory acts against the whistleblower are null and void. Whistleblowers who believe they have been retaliated against due to their report can notify ANAC. Protections, including the prohibition of retaliation, extend to facilitators, colleagues, and relatives of the whistleblower, as well as legal entities connected to the whistleblower.

- Under certain conditions, liability limitations apply in cases of disclosure of information covered by confidentiality obligations, protecting copyright and personal data rights.

Are anonymous reports allowed?

Anonymous reports are permitted. In such cases, the whistleblower's identity cannot be determined. The Reporting Portal allows protected communication with the whistleblower (even if anonymous) by accessing the portal using the report's date and the Unique Identification Code generated at the time of submission.

Is there an authority ensuring the fairness of Whistleblowing systems?

ANAC (National Anti-Corruption Authority) can be contacted if the internal channel is inactive or non-compliant, if the whistleblower submitted an internal report but did not receive an acknowledgment of receipt and/or feedback on the report's outcome, or if they reasonably believe (based on concrete circumstances and verifiable information) that an internal report would not be effectively addressed or might result in retaliation, or if the violation poses an imminent or clear danger to public interest. ANAC provides an online platform accessible through its institutional website. Whistleblowers who believe they have been retaliated against due to their report can notify ANAC through the same online platform.