

WHISTLEBLOWING POLICY

Document name	Whistleblowing Policy
Document identifier	Quiris_ Whistleblowing_2023.01
Number of pages	13

Drafted by	HR Quiris
Reviewed by	Legal Quiris IT Quiris
Approved by	Umberto Risso
Version	1.0
Version date	13/07/2023
Publication date	See Intranet

Policy Owner	Umberto Risso
--------------	---------------

Summary

1. Introduction.....	3
2. Purpose of the Policy and its intended recipients.....	4
3. The report/whistleblowing.....	5
4. Reporting channels.....	5
5. Report content.....	6
6. Protection and liability of the Whistleblower.....	7
7. Protection of the Reported person.....	7
8. Method of transmitting the report via the “Portal”	8
9. Reporting management.....	9
10. External reporting.....	11
10.1. Conditions for external reporting.....	11
10.2. External reporting channels.....	11
11.....	Public disclosure
.....	12
12. Periodic report.....	12
13.....	Record keeping and protection of Privacy
.....	13
14. Updating the Policy.....	13

1. Introduction

Italian Law No. 179 “Provisions for the protection of the authors of reports of crimes or breaches of which they have become aware during public or private employment” came into force on 29 December 2017 (published in the Official Gazette, General Series No. 291 of 14 December 2017). The structure of the provision distinguishes the public sector (Art. 1) from the private sector (Art. 2), and the provision on the obligation of official, business, professional, scientific and industrial secrecy (Art. 3) was added.

As far as the private sector is concerned, Article 2 of Italian Law No. 179/17 was introduced on Italian Decree No. 231 and included a new provision in Article 6 (“Persons in top management positions and organisational models of the organisation”), which also classified the measures related to the submission and management of reports within the organisational model pursuant to Italian Legislative Decree No. 231/01 .

Subsequently, Italian Legislative Decree No. 24 of 2023 was published in the Official Gazette on 10 March 2023, implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the “protection of persons who report breaches of Union law” that affect the public interest or the integrity of the public administration or private entity, of which they have become aware in a public or private context (hereinafter the “Directive”).

In summary, the new regulations set out:

- a. the obligation for all private organisations with more than 50 employees to establish internal reporting channels;
- b. the possibility, not only for employees but also for the other persons referred to in Article 4 of the Directive, to report breaches of Union law in several areas, including:
(i) public procurement; (ii) financial services, products and markets and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) environmental protection; etc.);

- c. the activation of reporting channels that are “designed, implemented and operated in a secure manner to ensure the confidentiality of the whistleblower's identity and the protection of any third parties named in the report, and that prevents access by unauthorised personnel”; and that include “notice of receipt of the report to the whistleblower within seven days of receipt”;
- d. the need to appoint impartial persons to receive and handle reports;
- e. the obligation to give final feedback to the whistleblower within 90 days;
- f. the obligation to take the necessary measures to prohibit any form of retaliation against persons who report breaches;
- g. the possibility for the parties concerned to resort, in certain cases, to “external” reporting to ANAC and to “disclosure” of the report;
- h. the need to provide the parties concerned with clear information on the reporting channel, procedures and prerequisites for making “internal” and “external” reports (the information must be displayed and made easily visible in workplaces and accessible to persons who, although not attending workplaces, have legal relations with the organisation in one of the forms set out in the decree).

Quiris sapa provides whistleblowers with a portal for reporting - the "Whistleblowing Portal" - which, by means of computerised procedures, is able to guarantee the confidentiality of the whistleblower's identity when handling reports.

2. Purpose of the Policy and its intended recipients

The purpose of this Whistleblowing Policy (hereinafter the "Policy") is to regulate the process of receiving, analysing and processing “internal” reports, from whomever they are sent and transmitted, including anonymously.

This Whistleblowing Policy applies to Quiris sapa. In particular, the intended recipients (hereinafter also simply “recipients”) of this procedure are:

- a. the top management and members of the corporate bodies of Quiris sapa;
- b. the employees of Quiris sapa;

- c. the partners, customers, suppliers, consultants, collaborators and, more generally, anyone with interests in Quiris sapa.

The “whistleblower” (pursuant to Article 2(1)(g) of Italian Legislative Decree no. 24/23 - “Whistleblower”) who has knowledge of facts that are potentially the subject of a report is invited to make the report promptly using the methods described below, refraining from undertaking any autonomous analysis and/or investigation.

3. The report/whistleblowing

“Whistleblowing” means any report of unlawful conduct or breaches of the Code of Ethics, of the 231 Organisational Model and of the internal procedures adopted by Quiris sapa or of the external discipline, in any case applicable to the Company as indicated above, based on precise and consistent facts of which the recipients have become aware because of their jobs and submitted to protect the integrity of the Company.

Reports must be made in good faith and must be substantiated with precise information so as to be easily verifiable.

As a general rule, Quiris sapa urges its employees to resolve any labour disputes, where possible, through dialogue, even informal, with their colleagues and/or their direct supervisor.

Reports must be made in a spirit of responsibility, be in the interests of common good, and fall within the types of non-compliance for which the system has been implemented.

4. Reporting channels

The Whistleblower must, without delay, report any breach, or reasonable suspicion of a breach, of the Policy.

Reports must be submitted through the following channels:

- a. via the dedicated reporting portal accessible at the following address (<https://quirisholding.integrityline.com>)
- b. ordinary mail addressed to Organismo di Vigilanza di Quiris sapa - Via Gabriele D'Annunzio 2/75, 16121 Genova.

However, for purely practical reasons, use of the portal as a reporting tool is preferred

Access to the Whistleblowing Portal is subject to the “no-log” policy in order to prevent identification of whistleblowers who wish to remain anonymous: this means that the company's IT systems are not able to identify the portal access point (IP address), even if access is from a computer connected to the company network.

Reports transmitted via the Whistleblowing Portal are received by the Supervisory Board (hereinafter also SB) of the company concerned.

Reports may also be made orally to the persons outlined above. Internal reports in oral form may be made via telephone lines or voice messaging systems or, at the request of the whistleblower, through a face-to-face meeting organised within a reasonable period of time.

To this end, Quiris sapa has established that oral reports may be made through a telephone contact with one of the members of the SB, who can be reached at the following number through the Quiris sapa switchboard tel. 010 90411.

Anyone who receives a report outside the aforementioned channels must transmit it through those channels without delay.

5. Report content

Reports should be as detailed as possible in order to allow for due verification. By way of example, a report should contain the following elements:

- a. the particulars of the whistleblower, indicating the organisational unit to which he/she belongs and/or the activity carried out for the Company;
- b. a clear and complete description of the events being reported and the time and place at which the events took place;
- c. elements making it possible to identify the person who perpetrated the reported events;

- d. any other persons who may report on the events being reported;
- e. any documents that may confirm the accuracy of the reported events.

Reports may not involve grievances of a personal nature or claims/complaints falling within the discipline of the employment relationship or relations with hierarchical superiors or colleagues, in which case reference should be made to the various communication channels made available by the Company.

Substantiated anonymous reports (containing all the objective elements needed for subsequent verification) will be considered for further investigation.

Any reports received by the SB and deemed irrelevant shall be filed without further investigation, without prejudice to the feedback to the whistleblower, which must be provided within the time limits laid down in Italian Legislative Decree 24/23.

6. Protection and liability of the Whistleblower

There may be no retaliation or discrimination, direct or indirect, against a person who has made a report in good faith. In addition, there may be sanctions for those who violate the whistleblower protection measures, as well as sanctions for the whistleblower in the event of reports made with malice or gross negligence or that prove to be false, unfounded, defamatory or in any case made for the sole purpose of harming the Company, the reported person or other persons involved in the report. The Company reserves the right, in any case, to take the appropriate steps, including in the courts.

7. Protection of the Reported person

The report is not sufficient to initiate any disciplinary proceedings against the reported person. If, following concrete findings concerning the report, it is decided to proceed with the investigation, the reported person may be contacted and given the opportunity to provide any necessary clarification.

8. Method of transmitting the report via the “Portal”

After accessing the Portal, the whistleblower will be guided through filling in a questionnaire consisting of open and/or closed questions that will allow him or her to provide the elements characterising the report (facts, company concerned, department concerned, etc.).

Invia una segnalazione

Qual è il tuo sospetto? *Obbligatorio

Lavori nell'organizzazione? Scegli un'opzione

In quale azienda ha avuto luogo l'incidente?

Indicare il nome del dipartimento interessato:

Chi è coinvolto nell'incidente?

The Portal collects the identity of the whistleblower, who may, however, choose to remain anonymous.

Informazioni di contatto

Nome

Numero di telefono

E-mail

In any case, the whistleblower may provide his or her personal details at a later stage, again through the Portal.

When sending the report, the Portal will issue the whistleblower with a unique identification code (ticket), consisting of a sequence of 3 letters and numbers separated by a hyphen.

This code is known only to the whistleblower and cannot be recovered in any way in case of loss. The ticket will be used by the whistleblower to access his or her report through the Portal in order to: monitor its progress; enter additional elements to substantiate the report; provide his or her personal details; answer any follow-up questions. In fact, the Portal makes it possible to establish a virtual dialogue between the whistleblower and the recipient, ensuring anonymity if requested by the whistleblower.


Abbiamo ricevuto la tua segnalazione. Inizieremo a trattare il tuo caso il più presto possibile.

Una volta che la tua segnalazione è stata trattata, puoi trovare la risposta nella Inbox - casella postale. Sarai informato via email. Nel caso di una registrazione che non richieda un'approvazione, ti contatteremo solo in caso di domande.

Importante:

Se stai utilizzando una modalità di navigazione privata, ti suggeriamo di accedere all'interno della Inbox sicura (Casella postale) e prendere nota del numero della segnalazione e della Password. Questo ti consentirà di effettuare il login in un secondo momento.

Il numero della tua segnalazione è : MUY7-BF4



Hai aperto una Inbox - casella postale sicura. Per accedere alla casella postale, devi utilizzare la password che hai appena digitato. Per accedere a un altro dispositivo/computer sono necessari il numero della segnalazione e la password di accesso. Queste informazioni sono disponibili nella tua Inbox -casella postale. È importante ricordare la password perché a causa dell'anonimato e della sicurezza del sistema non ci sarà possibile inviartela di nuovo qualora la dimenticassi.

9.Reporting management

Once received by the Supervisory Board, reports undergo the following investigation procedure.

Acknowledgement of receipt

The Supervisory Board will provide the whistleblower with an acknowledgement of receipt within 7 days.

Analysis

The Supervisory Body undertakes to provide feedback to the whistleblower within 90 days of the report. In particular, reports will undergo preliminary analysis in order to verify the presence of useful data and information to assess their grounds.

When carrying out the aforementioned analysis, the SB may request further information or documentation from the whistleblower by means of the chat available on the portal, and may avail itself - for specific aspects dealt with in the reports and where deemed necessary - of the support of corporate functions and external professionals.

If, at the end of the preliminary analysis, it emerges that there are no sufficiently circumstantial elements or that the facts referred to are unfounded, the report will be filed with the relevant reasons.

Where, as a result of the preliminary analysis, useful and sufficient elements emerge or can be deduced to assess the report as well-founded, the next phase of specific investigations will be initiated.

Specific investigations

The SB will:

- a. initiate specific analyses using, if deemed appropriate, the competent structures in the Company or external experts and appraisers;
- b. agree with the management in charge of the department involved in the report, the possible action plan needed to remove the control weaknesses detected;
- c. agree with the departments involved any initiatives to be taken to protect the interests of the Company (e.g. legal initiatives, suspension/deletion from the suppliers' register, etc.);
- d. request, if possible, the start of disciplinary proceedings against the whistleblower, in the case of reports in relation to which the whistleblower's bad faith and/or purely defamatory intent is established, possibly also confirmed by lack of grounds for the report;
- e. at the end of the investigation carried out, submit the results for assessment by the Human Resources Department so that appropriate action may be taken;
- f. terminate the investigation at any time if, during the investigation, it is established that the report is unfounded.

The activities described above are not necessarily carried out sequentially.

10. External reporting

10.1. Conditions for external reporting

An external report may be made by the whistleblower if, at the time of its submission, one of the following conditions is met:

- a. there is no mandatory activation of the internal reporting channel within his or her working situation, or this channel, even if mandatory, is not active or, even if activated, does not comply with Article 4;
- b. the whistleblower has already made an internal report under Article 4 and the report has not been followed up;
- c. the whistleblower has reasonable grounds to believe that, if he or she were to make an internal report, the report would not be effectively followed up or that the report might give rise to the risk of retaliation;
- d. the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

10.2. External reporting channels

The National Anti-Corruption Authority (ANAC) activates an external reporting channel that guarantees, including through the use of encryption tools, the confidentiality of the identity of the whistleblower, the person involved and the person mentioned in the report, as well as the content of the report and the related documentation. The same confidentiality is guaranteed even when the report is made through channels other than those indicated in the initial period or reaches staff other than those in charge of handling reports, to whom it is in any case transmitted without delay.

External reports are made in writing via the IT platform or orally via telephone lines or voice messaging systems or, at the request of the whistleblower, by means of a face-to-face meeting organised within a reasonable period of time.

An external report submitted to a person other than the ANAC is transmitted to the latter, within seven days from the date of its receipt, with simultaneous notification of the transmission to the whistleblower.

11. Public disclosure

The Decree states that the whistleblower may disclose information on breaches in the public domain through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people.

A whistleblower who makes a public disclosure benefits from the protection provided by the Decree if, at the time of the public disclosure, one of the following conditions is met:

- a. the whistleblower has previously made an internal and external report or has made an external report directly, under the conditions and in the manner set out in this Policy, and has not received a response to the report;
- b. the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- c. the whistleblower has reasonable grounds to believe that the external report may involve a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there is a well-founded fear that the recipient of the report may be colluding with or involved in the perpetrator of the breach.

12. Periodic report

In its half-yearly report, the SB provides a summary report of the reports received by the Board of Directors and the Board of Auditors.

This report contains the results of the analysis, including adoption (or non-adoption) of disciplinary measures.

13. Record keeping and protection of Privacy

In order to ensure the management and traceability of reports and related activities, the SB ensures that all supporting documentation for the report is archived for a period of five years from the report closure.

Any personal information and details contained in the report, relating to the whistleblower and/or other individuals involved in various capacities in the events brought to the Company's attention, will be processed in accordance with the procedures set out in the personal data processing policy, available on the intranet reserved for employees and on the website www.quirisholding.com in the section dedicated to handling Whistleblowing.

14.Updating the Policy

The policy and the Portal will be subject to periodic review by the Human Resources Department to ensure that it is constantly aligned with the applicable legislation and is in accordance with any suggestions made by the Company's SB on the basis of experience.