REGULATION SCOPE

To regulate the process of receiving, analyzing, and managing reports, sent or transmitted by anyone (including independent collaborators, freelancers, volunteers, shareholders, and directors). even anonymously. It applies to all companies (production sites and otherwise), which guarantee its correct and constant application, as well as maximum dissemination within them, in compliance with the confidentiality obligations and the prerogatives of autonomy and independence of each of the PSC companies.

REFERENCE DOCUMENTS

Model of Organization, Management and Control ex D.Lgs 231/01 (MOG) of PSC

D. Lgs 24/2023 Implementation of the Directive UE) 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 and concerning the protection of persons reporting breaches of national legal provisions.

D.lgs. 231/01ì Regulation of the administrative liability of legal persons, companies, and associations even without legal personality, pursuant to article 11 of the law of 29 September 2000, n. 300.

Guidelines on the protection of persons reporting breaches of Union law and concerning the protection of persons reporting breaches of national legal provisions. Procedures for the submission and management of external reports.
ANAC - Resolution n°311 of 12 July 2023

Versione	Data	Descrizione
r00	01/07/2023	First edition
r01	04/12/2024	Use of specified platform for reporting, paragraph. 4.1

SUMMARY

1 INTRODUCTION AND DEFINITIONS

Whistleblowing" (or **"report")** means, the oral or written communication of information on breaches; by persons working in the private or public sector who acquired information on breaches in a work-related context.

Legislative Decree 24/23 defines the conducts that must be reported; this legislation covers violations of national or European Union legislative provisions that harm the public interest or the integrity of the Public Administration or a private entity, including administrative, accounting, civil or criminal offences. In continuity with the past, those illicit conducts relevant pursuant to Legislative Decree 8 June 2001, n. 231 must also be reported, as well as violations of organizational and management models.

However, r**eports regarding individual employment relationships and those regarding national security and defense are excluded from the decree**.

Public interest: the reports must be made in the public interest or in the interest of the integrity of the public administration or private entity. The reasons why the person reported, denounced, or disclosed publicly are irrelevant to their protection.

Organizational and Management Model 231 (MOG): Legislative Decree 231/01 document that describes a series of company procedures aimed at ensuring the prevention of the commission of crimes, for which the company could be held liable.

Supervisory Body (ODV): provided for by Legislative Decree 231/01, it is the entity responsible for monitoring and regularly verifying the effectiveness of the Organizational Model MOG.

2 WHO CAN MAKE A WHISTLEBLOWING

Whistleblowing procedures encourage reporting by anyone who acquires, in the context of their work, information about illegal activities committed by the organization or on behalf of the organization.
The purpose of the procedure is to facilitate the communication of information relating to violations found during work activities. The spectrum of potential whistleblowers can be very broad. The procedure is intended to protect these individuals when they report illegal conduct relating to the organization.

This Regulation shall apply to reporting persons who acquired information on breaches in a work-related context including, at least, the following:

- persons having the status of worker,
- persons having self-employed status,
- shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees;
- any persons working under the supervision and direction of contractors, subcontractors and suppliers.
- persons where they report or publicly disclose information on breaches acquired in a work-based relationship which has since ended.
- persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

4.1 Reporting through internal reporting channels

For reporting violations, the company provides a platform to make reports in written form, pursuant to this procedure.

The *encrypted IT platform* is provided by Transparency International Italia and Whistleblowing Solutions belonging to the Whistleblowing IT project.

The link to the web platform is available on the company website *https://www.pscomponents.eu.*

The platform uses GlobaLeaks, the main open-source software for whistleblowing. This tool guarantees, from a technological point of view, the confidentiality of the reporting person, of the subjects mentioned in the report and of the content of the same.

A *questionnaire* is uploaded to the platform that guides the reporting person through the reporting process by open and closed questions, some of which are mandatory. It is possible to attach documents to the report, as well.
All information uploaded and stored on the platform are encrypted and can be read only by personnel purposely authorized. At the end of the report, the reporting person receives a unique 16-digit code, with which he/she can access the his/her own report and even communicate with the receiving party, exchanging messages and sending new information/details.

It is not possible to manage other reports sent in other ways. If these are sent any way, the receiving entity, where possible, will invite the reporting party to submit the same report in the institutional manner, i.e. via the IT platform.

The whistleblower also has the faculty of requesting a "direct meeting" with the *Whistleblowing Team.*

The entity responsible for receiving and managing reports is the W*histleblowing Team,* which is composed by internal PSC individuals (identified by the HR department of holding companies) and the Supervisory Body (ODV), duly appointed with respect to specific tasks.

When the W*histleblowing Team* receives the reports, it engages a dialog with the reporting person, in order to clarify and investigate on the matters described in the received whistleblow. The reciprocal communication goes on during all the investigation phases.

The W*histleblowing Team* receives the report immediately after the reporting person receives the receipt code and must:

- *Within 7 days*, confirm to the reporting person that the report has been taken into account and invite the same to monitor his/her report on the platform to answer to possible questions on clarification or demand further information.
- *Within 3 months* from the day the report has been sent, the W*histleblowing Team* provides the reporting person with feedback regarding the investigation activities carried out to verify the matter. The feedback provided within 3 months may not coincide with the outcome of the investigation activities: in this case, the recipient invites the reporting person to keep monitoring the platform until the final outcome of the same is known.

The W*histleblowing Team* analyses and classifies the issued Reports, assuring to process only those ones in compliance with the scope described above (paragraph 3: What can be reported); in the event that the submitted Reports are not adequately detailed, the team may also request further detailed information from the Reporting Party.

As first the W*histleblowing Team* carries out a preliminary check of the reports (also involving the ODV for correctly addressing the right whistleblowings to the proper agency) to assess whether there were the grounds for starting the Analysis process or for proposing its archiving (for generic reports or those with lacking information elements).

In order to acquire information, the W*histleblowing Team* carries out in-depth analyses, including meeting and listening to the Reporting Person, the reported party and also other persons mentioned in the Report (as informed of the facts), as well as requesting the aforementioned persons to produce information reports and/or documents.

At the end of the analysis, the W*histleblowing Team* prepares a report that contains the carried-out activities, the relevant outcomes, a judgment of whether (or not) the reported facts are reasonably well-founded, and any indications (suggestions) to the management regarding the necessary corrective actions to be taken.

All the documentation collected for the analysis and the corrective actions taken relating to the reports are archived by the W*histleblowing Team* and the ODV (each according to its competence).

4.2 Reporting through external reporting channels

In addition to what has already been described regarding the internal procedure, the law allows the whistleblower to also make external reports to the *National Anti-Corruption Authority (ANAC*). The whistleblower can report externally to his or her company in some cases:

- if he or she has already made a report that has not been followed up,
- if he or she has reasonable grounds to believe that an internal report will not be followed up or that this may lead to a risk of retaliation against him or her
- if he or she has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

The methods of reporting to the National Anti-Corruption Authority are available on the dedicated page on the ANAC website anticorruzione.it/-/whistleblowing.

There are also additional conditions under which a whistleblower can make a *public disclosure*: the lack of response to a previously made report (internal or external), an imminent or obvious danger to the public interest, reasonable grounds that an internal report will not be processed or that evidence of the same may be destroyed or hidden.

5 CONFIDENTIALITY AND ANONYMITY

The provisions introduced by Legislative Decree 24/2023 significantly strengthen the protection of the confidentiality of the whistleblower, providing various guarantees against any retaliatory acts.

- The identity of the whistleblower cannot be revealed to persons other than those competent to receive or follow up on the reports;
- The protection concerns not only the name of the whistleblower but also all the elements of the report from which the identification of the whistleblower can be derived, even indirectly;
- The report is exempt from access to administrative documents and from the generalized right of civic access;
- The protection of confidentiality is extended to the identity of the persons involved and of the persons mentioned in the report until the conclusion of the proceedings initiated on the basis of the report, in compliance with the same guarantees provided for the reporting person.

The identity of the whistleblower cannot be revealed, except with the express consent of the whistleblower himself, to persons other than those competent to receive or follow up on the reports, expressly authorized to process such data.

However, the right to *confidentiality* is not absolute: possible disclosure of the identity of the reporting person may occur in the event that the investigation documents are forwarded to an ordinary or accounting prosecutor's office and therefore knowledge of the same is necessary for the purposes of the right of defense during any ordinary or accounting judicial proceedings at the Court of Auditors.

Confidentiality is guaranteed through technological tools, such as the encrypted platform for reports and a confidential protocol, and within organizational processes aimed at minimizing the circulation of information.

Moreover, it is also possible to send *anonymous reports*. The receiving party can decide whether or not to process them. In any case, the reports are treated according to the same principles of confidentiality. However, in the case of anonymous reports, the receiving party does not have knowledge of the identity of the reporting person and could inadvertently expose it during the investigation activities.

6 SAFEGUARDS AND PROTECTIONS

The person referred to in the report as responsible for the suspected breach benefits from identity protection measures similar to those of the reporting person and other persons mentioned in the report.

In addition to the protection of the confidentiality of the identity of the reporting person and of the persons mentioned in the report, as well as of the content of the report, there are other forms of protection guaranteed through this procedure.

The reporting person is guaranteed protection against any form of retaliation or discrimination that he or she may suffer following and because of a report. Retaliation means any threatened or actual action, direct or indirect, connected to or resulting from reports of actual or suspected breaches, which causes or may cause physical or psychological harm, damage to the reputation of the person, economic loss.
Possible discrimination includes:

- dismissal, suspension, or equivalent measures;
- demotion or failure to promote;
- change of duties, change of place of work, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- negative marks or references;
- disciplinary measures or other sanctions, including financial ones;
- coercion, intimidation, harassment, or ostracism;
- discrimination or unfavourable treatment;
- failure to convert a fixed-term employment contract into an indefinite one, where the worker had a legitimate expectation of such conversion;
- failure to renew or early termination of a fixed-term contract;
- damage, including to the reputation of the person, economic or financial prejudice, including loss of economic opportunities and income;
- inclusion in improper lists on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in the sector in the future;
- early termination or cancellation of a contract for the supply of goods or services; cancellation of a licence or permit; the request to undergo psychiatric or medical examinations.

7 PERSONAL DATA MANAGEMENT

The reports received, the investigation activities and the communications between the reporting person and the receiving person are documented and stored in accordance with the provisions on confidentiality and data protection.

The reports, since they contain personal data, can be processed and kept only for the time necessary to their processing: this time includes the analysis, the investigation activities and that for communicating the results, in addition to any necessary time for possible comments.
In no case will the reports be stored for more than 5 years following the communication of the outcome of the investigation activities to the reporting person.

Regarding access to personal data, these are known only by the *Whistleblowing team*.
It is mandatory that, if for investigative reasons, other parties must also be made aware of the content of the report and its attachments, the identity of the persons involved (reporter, facilitator, reported and other persons mentioned in the report), and all data from the disclosure of which the identities of the persons involved can be indirectly or directly deduced, will be subject to obscuring.

If such data are really necessary for the investigation conducted by external parties (possibly involved by the Whistleblowing team), it will be necessary to extend the duties of confidentiality and privacy to external parties through specific contractual clauses, to be included in the agreements stipulated with the external party.

8 SANCTIONS

Legislative Decree no. 24/2023 provides for administrative sanctions, which can be imposed by the National Anti-Corruption Authority in the event of violation of the rules on whistleblowing.

The sanctions specifically concern any retaliation against the reporting parties, violations of the confidentiality obligation, boycotting an attempted report, failure to take charge of a report or insufficient investigative activity initiated following the same.

PRIMA SOLE COMPONENTS spa
Chief Executive Officer