WHISTLEBLOWING PROCEDURE

Report management procedure model

INTRODUCTION

Whistleblowing, or reporting of an alleged offence, is a corruption prevention system introduced by law 6 November 2012, n. 190 "Provisions for the prevention and repression of corruption and illegality in the Public Administration".
For private organizations with between 50 and 249 employees, the obligations are in force from 17 December 2023.

WHO CAN REPORT THROUGH THE INTERNAL REPORTING SYSTEMS?

Whistleblowing procedures encourage reporting anyone who acquires, in the context of work, information on offenses 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. For this purpose, the spectrum of potential reporting persons is very broad. The procedure is aimed at protecting these subjects when they report illegal conduct relating to the Company.

The following categories of subjects can make a report through the procedure:

- Employees
- Collaborators
- Suppliers, subcontractors and employees and collaborators of the same
- Freelancers, consultants, self-employed workers
- Volunteers and interns, paid or unpaid
- Shareholders or persons with administrative, management, supervisory, control or representation functions
- Former employees, former collaborators or people who no longer hold one of the positions indicated above
- Subjects in the selection or probationary phase or whose legal relationship with the organization has not yet begun.

The procedure also protects the identity of the facilitators, the natural persons who assist a reporting person in the reporting process, operating within the same working context.

WHAT TYPE OF OFFENSE CAN BE CONSIDERED IN THE REPORTING PROCEDURES?

Within this procedure, illicit facts of which one has become aware in the context of one's work activity can be reported. Qualified suspicions of crimes or other violations of legal provisions or potential risks of their commission may also be reported.
The reporting person is not required to fully demonstrate the commission of an offence, but the reports must be as detailed as possible, in order to allow the recipients to ascertain the facts communicated. At the same time, reporting entities are not invited to carry out investigative activities that could expose them individually.
The reports may concern criminal, civil, administrative or accounting offences, as well as violations of community regulations.

Reports of a personal nature, for example relating to your employment contract, which are regulated by other Company procedures, do not fall within the scope of this procedure.

WHO RECEIVES AND MANAGES THE REPORTS?

The Supervisory Body (ODV) is the entity responsible for receiving and managing reports of offences.
The ODV receives the reports and dialogues with the reporting person to clarify and explore what has been received. The dialogue with the reporting person also continues during the investigation phases.
The ODV carries out verification activities on the information reported, also requesting specific information from other offices and functions within the organisation.
The ODV provides periodic feedback to the reporting person and, at the end of the assessment activity, communicates the outcome of the assessment activities. The communication of the outcome does not include references to personal data relating to the individual reported.
Among the possible outcomes that can be communicated to the reporting person are:
o Correction of internal processes
o Initiation of disciplinary proceedings
o Transfer of the results of the assessment activities to the Public Prosecutor's Office (and/or the Court of Auditors in the event of damage to the public treasury)
o Archiving due to lack of evidence
The report that is mistakenly sent to the hierarchical superior may not be treated as a whistleblowing report, as the latter does not have the same confidentiality obligations as the receiving party.

REPORTING CHANNEL

The Company makes available to reporting persons, as the sole channel, the IT platform accessible at https://whistleblowing.mvcgroup.com.

In particular, it is possible to make reports in oral and written form.

As regards reports in written form, the Company provides an encrypted IT platform, provided by IT Strategy Srl. 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 thereof.

A questionnaire is uploaded to the platform which guides the reporting person in the reporting process through open and closed questions, some of which are mandatory. You can also attach documents to your report.

As regards oral reports, the Company provides an encrypted IT platform, provided by IT Strategy Srl. 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 thereof.

The platform allows you to record the reporting message using a specific recording button. The message must last at least 10 seconds and the voice will be distorted to anonymize it. Before sending the message, the reporting party must ensure that the message is understandable by listening to what was recorded using the appropriate Play button made available by the platform itself.

At the end of the report, the reporting person receives a unique 16-digit code, with which he or she can access the report and communicate bidirectionally with the receiving party, exchange messages and send new information. All the information contained on the platform is encrypted and can only be read by individuals authorized to receive the report.

It is not possible to manage other reports received in written form. If these are sent, the receiving party, where possible, will invite the reporting person to submit the report again via the IT platform.

REPORT MANAGEMENT TIMELINES

At the end of the reporting process, the platform displays a receipt code confirming that the report has been delivered and taken care of by the receiving party.

Within 7 days, the receiving party confirms to the reporting person that they have taken charge of the report and invites the reporting party to monitor their report on the platform to respond to possible requests for clarification or further information.

Within 3 months from the day of the report, the receiving party communicates to the reporting person feedback regarding the assessment activities carried out to verify the information communicated in the report.

The feedback provided within 3 months may coincide with the outcome of the assessment activities. If these are not concluded, the recipient invites the reporting person to keep the platform monitored until the final outcome is known.

CONFIDENTIALITY AND ANONYMITY

The receiving party is required to process the reports while preserving their confidentiality. Information relating to the identity of the reporting subject, the reported subject and any other person mentioned in the report is treated according to the principles of confidentiality. Likewise, all information contained in the report is also treated confidentially.

The identity of the reporting person cannot be revealed without his or her consent. Knowledge of the reports and the related assessment documents are also excluded from the right to administrative access by the interested parties.

The only reason for possible disclosure of the identity of the reporting person may occur in the event that the assessment documents are forwarded to an ordinary or accounting prosecutor's office and knowledge of the same is necessary for the purposes of the right of defense during judicial or accounting proceedings at the relevant bodies.

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

MANAGEMENT OF PERSONAL DATA

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

The reports contain personal data and can be processed and maintained only for the time necessary for their processing: this time includes the analysis, assessment activities and communication of the results, as well as any additional time for possible additional comments.

In no case will the reports be kept longer than 5 years following the communication of the outcome of the investigation activities to the reporting person.

As regards access to personal data, these are known only to the receiving party.
During the assessment activities, the receiving party can share information previously anonymized and minimized with respect to the specific activities of the latter's competence with other functions of the Company.

SAFEGUARDS AND PROTECTIONS

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

In addition to protecting the confidentiality of the identity of the reporting person and of the subjects mentioned in the report, as well as of its content, there are other forms of protection guaranteed through this procedure.
In fact, protection is guaranteed to the reporting person against any form of retaliation or discrimination that they may suffer following and as a result of a report. Retaliation means any threatened or actual action or omission, direct or indirect, connected to or resulting from reports of actual or suspected wrongdoing, which causes or may cause physical or psychological harm, damage to a person's reputation, or economic loss.

Possible discrimination includes:

- dismissal, suspension or equivalent measures;
- demotion or failure to promote;
- the change of functions, the change of place of work, the reduction of salary, the modification of working hours;
- the suspension of training or any restriction of access to it; o notes of merit or negative references;
- disciplinary measures or other sanctions, including pecuniary;
- coercion, intimidation, harassment or ostracism;
- discrimination or unfavorable treatment;
- the failure to convert a fixed-term employment contract into a permanent 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 person's reputation, economic or financial prejudice, including the loss of economic opportunities and income;
- improper listing on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector in the future;
- the early termination or cancellation of the contract for the supply of goods or services; the cancellation of a license or permit; the request to undergo psychiatric or medical tests.

SANCTIONS

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

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

Abuses of the reporting system are also punishable, with possible sanctions for anyone who slanders or defames another person through the procedure.

The Company may take disciplinary action against those responsible for this conduct.