WHISTLEBLOWING PROCEDURE

ARCO S.R.L.

1. FOREWORD

Legislative Decree No. 24, of 10 March 2023, regulates the protection of persons who report breaches of national or European Union regulations of which they have become aware in a work-related context (so-called *Whistleblowing*).
The purpose of this document is to illustrate the procedure for reporting and handling reports of suspected misconduct or alleged breaches.

2. WHICH SITUATIONS CAN BE REPORTED

Behaviour, acts or omissions detrimental to the public interest or the integrity of the company, of which the whistleblower has become aware in a work-related context, may be reported, and especially:

a) administrative, accounting, civil, or criminal offences;
b) unlawful conduct relevant pursuant to Legislative Decree 231/2001, or violations of the organisation and management models provided for therein;
c) infringement of European legislation on public procurement, services, products and financial markets and prevention of money laundering and terrorist financing, product safety and compliance, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety and animal health and welfare, public health, consumer protection, privacy and personal data protection, and network and information system security;
d) breaches of competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;
e) acts or conduct that defeat the object or the purpose of the provisions of the European Union acts in the areas mentioned above.

Information on breaches that have not yet taken place, but which the reporter believes may constitute a violation on the basis of concrete and objective elements, may also be reported.

On the other hand, not subject to protection, and therefore unenforceable, is information:

a) concerning situations of a personal nature involving claims or grievances relating to relations with colleagues;
b) having insulting tones or containing personal offences or moral judgements and aimed at offending or harming the personal and/or professional honour and/or decorum of the person or persons to whom the reported facts refer;
c) based on mere suspicions or rumours concerning personal facts not constituting an offence;
d) relating to information already in the public domain;
e) for purely defamatory or slanderous purposes;
f) of a discriminatory nature, in that they refer to sexual, religious or political orientation or to the racial or ethnic origin of the reported person;
g) concerning requests to exercise personal data protection rights vis-à-vis the company (so-called privacy rights), pursuant to EU Regulation 2016/679 and Legislative Decree No. 196/2003.

Any reports that are manifestly unfounded, or made with the sole purpose of harming the reported person, and any other improper or instrumental use of the reporting mechanism are prohibited, will not be taken into consideration and may be liable to sanctions and/or action before the Judicial Authorities. In the event of slanderous or defamatory reports, the person making the report in bad faith may be held criminally liable and disciplinary proceedings may be instituted against him/her.

3. WHO CAN FILE A REPORT

The persons who may file a report of breaches known within a working relationship or collaboration with Arco S.r.l. are the following:

a) employees of Arco S.r.l., including workers whose employment relationship is governed by Legislative Decree No. 81/2015, or by Article 54 bis of Legislative Decree No. 50/2017;
b) self-employed workers who carry out their work at Arco S.r.l.;
c) workers or collaborators working for public sector or private sector entities that provide goods or services or carry out works for third parties;
d) self-employed professionals and consultants who work for Arco S.r.l.;
e) volunteers and paid and unpaid trainees working at the company;
f) persons with administrative, management, control, supervisory or representative functions;
g) Facilitators;
h) persons in the same work environment as the reporting person who are linked to him/her in a stable emotional or family relationship up to the fourth degree;
i) the reporting person's work colleagues.

Protection applies to all persons listed above if the Report, charge or public disclosure occurs in the following cases:

a) when the employment or collaboration relationship is in place;
b) when the legal relationship has not yet begun, if information on breaches has been acquired during the selection process or at other pre-contractual stages;
c) during the probationary period;
d) after the termination of the legal relationship if the information on violations was acquired in the course of that relationship.

4. PROTECTION OF THE REPORTING PERSON

The identity of the whistleblower and any other information from which that identity may be directly or indirectly inferred may not be disclosed to anyone beyond those entrusted with receiving and following up on reports. This is also in order to avoid exposing the whistleblower to retaliation that might be taken as a result of the report.

The identity of the whistleblower may be disclosed in the event of the whistleblower's explicit consent, or of written communication of the reasons for such disclosure in proceedings initiated following internal or external reports, where such disclosure is also indispensable for the reported person's defence. In this case, the whistleblower shall be given prior written notice of the reasons for the disclosure of the confidential data. In any case, the person in charge of handling reports is bound to keep confidential the identity of the reporting person, the facilitator, the reported person or in any case the persons mentioned in the Report, as well as the content of the Report and of the relevant documentation.

5. PROHIBITION OF RETALIATION

The Whistleblower may not be sanctioned, demoted, dismissed, transferred, or subject to any other organisational measure having a direct or indirect negative effect on working conditions, as a result of his/her reporting. In particular, the following are considered retaliation:

a) suspension, lay-off, dismissal or equivalent measures;
b) demotion or withholding of promotion;
c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;
d) withholding of training or any restriction of access to it;
e) negative performance assessment or employment reference;
f) adoption of disciplinary measures or other penalty, including a financial penalty;
g) coercion, intimidation, harassment, or ostracism;
h) discrimination or, in any case, unfavourable treatment;
i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
j) failure to renew, or early termination of, a temporary employment contract;
k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
m) early termination or cancellation of the contract for the supply of goods or services;
n) cancellation of a licence or permit;
o) the request to undergo psychiatric or medical assessments.

In addition to these, retaliation may include, for example, the demand for results that cannot be achieved in the manner and within the time specified; a specifically negative performance assessment; an unjustified withdrawal of appointments; an unjustified failure to grant appointments with the simultaneous granting to another person; the repeated rejection of requests (e.g. holidays, leave); the unjustified suspension of patents, licences, etc.

Retaliation is null and void, and individuals who have been dismissed because of the report are entitled to be reinstated in their jobs.

6. PROTECTION OF THE REPORTED PERSON

If a whistleblower files forbidden reports, and in particular reports that are false, defamatory, slanderous, with the sole purpose of harming the person reported, the protection measures described in Section 5 shall not apply in his/her favour.

When the criminal liability of the whistleblower for the offences of defamation or slander, or his/her civil liability for the same offence in cases of wilful misconduct or gross negligence, is established, including by a judgement of first instance, the company reserves the right to impose appropriate disciplinary sanctions on the whistleblower.

A reported person who is informed of a report against him or her and who considers the report to be unfounded, mendacious, slanderous or defamatory, may submit a specific request to the person in charge of handling reports to find out the identity of the reporting person, with a view to instituting civil and/or criminal proceedings against him or her to protect his or her interests.

7. POSSIBLE WAYS TO FILE A REPORT

Those who wish to file a report may do so in the following ways:

a) using the internal reporting channel;
b) via the external channel managed by ANAC (National Anti-Corruption Authority);

c) by public disclosure through the press or electronic media, or by means of dissemination capable of reaching a large number of people.

The reporting person may always refer directly to the Judicial Authority by lodging a complaint concerning the relevant facts or conduct of which he/she has become aware.

7.1 INTERNAL REPORTING CHANNEL

7.1.1 REPORTING MODALITIES

In order to file a Report, the company makes available to all the authorised parties referred to in point 3 above a specific IT platform called "Wallbrakers" accessible at the link https://arcosrl.wallbreakers.it/#/
"Wallbrakers" is a web application accessible from any device, which allows the submission of a report after entering information in the appropriate fields. At the end of the procedure the reporting person will receive a unique access code allowing him/her to access his report, follow its processing, communicate securely with the organiser and receive feedback on the report.

Anonymous Reports are also taken into account, when they are adequately substantiated and filed with a wealth of details, i.e. they are such as to bring out facts and situations relating them to specific contexts (e.g.: documentary evidence, indication of names or particular qualifications, mention of specific offices, proceedings or particular events, etc.).

The Report must be detailed and as complete and thorough as possible. The reporting person is required to provide all available and useful elements to enable the subjects in charge to carry out the necessary and appropriate checks and investigations to assess the validity of the facts reported, such as:

a) a clear and complete description of the reported facts;
b) the circumstances of time and place in which the reported breach was committed;
c) personal details or other elements allowing the identification of the person(s) who has/have carried out the reported facts (e.g. job title, place of employment where he/she carries out the activity);
d) any documents supporting the Report;
e) an indication of any other persons who may report on the facts that are the subject of the Report;
f) any other information that may provide useful feedback on the existence of the reported facts.

For a Report to be substantiated, the requirements set out in the preceding paragraph do not necessarily have to be fulfilled at the same time, in view of the fact that the Reporting person may not be in full possession of all the information requested.

Through the IT channel, the Reporting person will be guided through each stage of the reporting process and will be asked, in order to better substantiate the report, to fill in a series of fields that must be completed in accordance with the requirements.

It is imperative that the elements in the report are known directly to the Reporting person and not reported or referred to by others.

As an alternative to the reporting method described above, this can also be done verbally by contacting the following telephone number +39 0173 045808

7.1.2 REPORTING MANAGEMENT

The management of the internal reporting channel is entrusted to a specially appointed person, who is therefore

the recipient of Reports.

The person in charge of handling reports performs the following activities:

a) issues the Reporting person an acknowledgement of receipt of the Report within seven days of its receipt;
b) carries out a preliminary analysis of its contents;
c) dismisses the Report if he/she considers it to be inadmissible on the grounds of the provisions of the Decree, especially when:
   - manifestly unfounded due to the absence of factual elements referable to the typified violations;
   - only documentation is produced, in the absence of the Report of unlawful conduct.
   In which case, the person in charge pursuant to the provisions of the Decree must provide the reporting person with a written statement of the reasons for closing the procedure;
d) where the case is not dismissed, he/she takes charge of the management of the Report.

In handling the Report of sub (d) above, the person in charge:

a) maintains the discourse with the Reporting person and may request further additions from the latter, if necessary. On this matter, the "Wallbrakers" platform allows direct communication between the Reporting person and the person in charge of handling the reports, thus enabling the latter to supplement the information needed to complete the investigation. This is done by accessing the platform using the credentials received when submitting the report. The unique access code also allows you to check the status of the alert;
b) follows up on the Reports received;
c) provides feedback on the Report within three months from the date of the acknowledgement of receipt or, in the absence of such notice, within three months from the expiry of the seven-day period from the submission of the Report.

7.1.3 METHODS OF CARRYING OUT THE INVESTIGATION

The investigation is the set of activities aimed at verifying the content of the internal Reports received and at acquiring elements useful for the subsequent assessment phase, guaranteeing the utmost confidentiality on the identity of the reporting person and on the subject of the Report.

During the investigation phase, in order to assess an internal Report, the person in charge of handling reports may carry out the appropriate internal investigations, either directly or by appointing a person inside or outside the company, subject to the obligation of confidentiality.

It is everyone's duty to cooperate with the investigating party in the conduct of the investigation. Of each

investigation, the appointed person prepares a final report containing at least:

- the established facts;
- the evidence gathered;
- the causes and shortcomings that allowed the reported situation to occur.

If, following the investigation carried out, the Report is found to be well-founded, the person in charge of handling reports will take the due and most appropriate mitigating and/or corrective action.
If, on the other hand, he/she finds that the internal Report is unfounded, he/she will proceed to close the procedure and notify the reporting person.

7.1.4 STORING MODALITIES

In order to ensure the traceability, confidentiality, preservation and retrievability of data throughout the process, documents are stored and archived both in digital format, via the platform, through password protected network folders, and in paper format, in a specially secured cabinet, accessible only to specially authorised and trained persons.

The data are kept for as long as necessary for the processing of the specific internal Reporting, and in any case no longer than five years from the date of the communication of the final outcome of the internal Reporting procedure.

7.2 EXTERNAL REPORTING CHANNEL MANAGED BY ANAC

If one of the following conditions is met:

a) an internal report was made through the channel made available by Arco S.r.l., which, however, was not followed up. Reference is made to cases where the internal channel has been used but the person entrusted with the management of the channel has not undertaken, within the deadlines provided for by law, any activity concerning the admissibility of the report, the verification of the existence of the facts reported or the communication of the outcome of the internal analyses carried out. It should therefore be clarified that by "taking action", the rule does not mean that the reporting person's expectations, in terms of the outcome of the report, must necessarily be fulfilled;
b) the reporting person, on the basis of concrete circumstances and information that can actually be acquired and, therefore, not on mere inferences, has reasonable grounds to believe that, if he/she were to make an internal report through the channel made available, it would not be effectively followed up or that it could give rise to the risk of a retaliatory conduct;
c) the reporting person has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest. This refers, for instance, to cases where the breach clearly requires urgent intervention by a Public Authority to safeguard a public interest such as health, safety or environmental protection;

the reporting person may make a report using the external reporting channel set up for this purpose by ANAC.

The external reporting channel, similarly to the internal channel, guarantees, also by means of encryption tools, the confidentiality of the identity of the reporting person, the person concerned and the person mentioned in the report, as well as the content of the report and the related documentation.

7.3 PUBLIC DISCLOSURE

In addition to the modalities described above, an external Report may be made that consists in a public disclosure, through which information on breaches is made public through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people. Public disclosure of breaches may take place if one of the following conditions is met at the time of disclosure:

a) an internal Report, to which the person in charge of handling such reports has not provided feedback on the measures envisaged or taken to follow up on the Report within the prescribed time limit (three months from the date of the acknowledgement of receipt or, in the absence of such notice, within three months from the expiry of the seven-day period from the submission of the Report), was followed up by an external Report to ANAC, which, in turn, did not reply to the reporting person within a reasonable period of time (three months or, if there are justified and substantiated reasons, six months

from the date of the acknowledgement of receipt of the external Report or, in the absence of such notice, from the expiry of seven days from its receipt);

b) the person has already filed an external Report directly to ANAC, which, however, has not provided feedback to the reporting person on the measures envisaged or taken to follow up on the Report within the aforementioned reasonable time limits;

c) the person directly makes a public disclosure because, on the basis of reasonable and well-founded grounds, in the light of the circumstances of the case, he or she believes that the breach may constitute an imminent or manifest danger to the public interest or may entail a risk of retaliation or may not be effectively followed up because, for example, he or she fears that evidence may be concealed or destroyed or that the person who has received the Report may be colluding with or involved in the breach.

This is without prejudice to the possibility of approaching the competent judicial and accounting Authorities directly to file a report of unlawful conduct of which they have become aware in their work environment.