# *Whistleblowing Policy*

Cuki cofresco

*Edition N. 3: 26.03.2026*

# Index

# 1 OBJECTIVE

Cuki Cofresco S.r.l. (hereinafter, the "**Company")** acts in compliance with the ethical principles of honesty, integrity, transparency and with national and international regulations and best practices relevant to its business in all the jurisdictions that it operates in.

In this context, the Company promotes the adoption of instruments aimed at reporting offences and irregularities ("**Reports**") that certain categories of individuals – internal or external to the Company – who have a legal relationship with it ("**Reporting Parties**") have become aware of.

The purpose of this Policy is to encourage Whistleblowing, to illustrate the protections that the Company guarantees to Whistleblowers, to reported persons and to the other categories referred to in paragraph 2 below, and to describe the procedures for making and managing Whistleblowing reports.

The Reporting system implemented by the Company and described in this Policy has the following main features:

1. it is accessible by anyone wishing to file a Report;
2. it guarantees the highest levels of confidentiality regarding the information disclosed and the identity of the Whistleblower and of the person who is the subject of the Report;
3. offers Whistleblowers a choice of the following alternative reporting methods: (i) web platform, which resides outside the Company's IT system as it is hosted on an independent server; (ii) recorded voice messaging system accessible by landline or mobile phone; and (iii) face-to-face meetings;
4. enables interaction between the Company and the Reporting Parties;
5. is managed by beLab S.p.A. – a company wholly owned by BonelliErede and specialised in services of (and digital solutions for) compliance management – an autonomous, dedicated entity comprising personnel specifically trained to manage the Reporting channel ("**System Manager**"); and
6. it complies with the requirements of Legislative Decree No. 24 of 10 March 2023 and subsequent amendments and integrations implementing EU Directive No. 2019/1937 on the protection of persons who report breaches of European Union law.

The content of this Policy is disseminated to all employees and third parties who have a legal relationship with the Company through publication on the Company's website and the Policy Management Application (available for the employees) and is the subject of dedicated training sessions.

## 2 WHISTLEBLOWER CATEGORIES

The following categories of Whistleblowers may file Reports and benefit from the protections under Legislative Decree 24/2023:

a) employees;

b) self-employed workers and collaborators (incl. volunteers and trainees);

c) workers and collaborators of suppliers;

d) freelancers and consultants;

e) directors and members of supervisory bodies; and

f) shareholders.

Additionally, the protections afforded to the categories of Whistleblowers listed above also apply if the Report occurs:

a) when the legal relationship has not yet begun, if information on violations has been acquired during the selection process or other pre-contractual stages;

b) during the probationary period; or

c) after the legal relationship terminates, if the information breach was acquired during the relationship.

Finally, these protections also extend to the following individuals:

a) facilitators;

b) persons in the same work environment as the Whistleblower who are linked to him/her by a stable emotional or family relationship up to the fourth degree;

c) work colleagues of the Whistleblower who work in the same professional environment as the Whistleblower and who have a regular and current relationship with the Whistleblower; and

d) entities owned by the reporting person, or that the reporting person works for, as well as entities working in the same work environment as the reporting person.

## 3 OBJECT OF THE REPORTS

The list of offences or irregularities that could be subject to a Report is non-exhaustive and a Report can concern committed or attempted actions or omissions that:

- are criminally significant or amount to civil or administrative offences or accounting violations;
- involve legal representatives, directors, managers and/or employees of the Company or – in any case – anyone acting on behalf of the Company (e.g., consultants and suppliers);

- are carried out in violation of the 231 Model or other company policies or procedures covered by penalties;
- are likely to cause financial or reputational damage to the Company;
- could give rise to potential conflicts of interest;
- are likely to cause damage to the health or safety of employees, or damage to the environment;
- could amount to a violation of the rules set out to, among other things, protect the following sectors:
  - public procurement;
  - financial services, products and markets and prevention of money laundering and terrorist financing;
  - product safety and compliance;
  - environmental protection;
  - food and feed safety and animal health and welfare;
  - public health;
  - consumer protection;
  - protection of privacy and protection of personal data and security of networks and information systems;
  - EU restrictive measures; or
- violate, in general, national or European legislation.

In any case, the Whistleblower must have reasonable grounds to believe that the information on the reported violations was true at the time of the Report. If, on the contrary, the Reports prove to be manifestly unfounded or defamatory, this would amount to a violation of this Policy, with the possible application of disciplinary measures and recognition of liability on the part of the Whistleblower.

Additionally, Reports must not concern personal grievances of the Whistleblower or claims/complaints that are covered by the rules of the employment relationship or relations with hierarchical superiors or colleagues, or product complaints by customers.

## 4 CONTENT OF THE REPORTS

The Whistleblowers must provide all the useful elements to enable the competent functions to carry out the necessary checks and verifications to assess the grounds of the facts reported.

To this end, the Report must contain the following elements:

a) a clear and complete description of the facts that form the subject of the Report;

b) the circumstances of time and place in which they were committed;

c) an indication of any other persons who could report on the facts that form the subject of the Report;

d) the enclosure of all documents that confirm the accuracy of such facts; and

e) all other information that could serve as useful evidence of the existence of the facts reported.

The requirement of the accuracy of the facts or situations reported remains in place to protect the reported person.

## 5 GENERAL PRINCIPLES

The Reporting system is based on the following fundamental principles:

- **Protection of the identity of Whistleblowers and confidentiality of information**: the Company guarantees the confidentiality of the identity of Whistleblowers and the confidentiality of the information in the reports at every stage of the management process, to the extent that anonymity and confidentiality are enforceable under the law. More specifically, confidentiality is waived – subject to the Whistleblower's express consent – in cases where: (i) within the framework of disciplinary proceedings, the charge is fully or partially based on the Whistleblowing and knowledge of the Whistleblower's identity is indispensable for the defence of the person accused; and (ii) disclosure of the Whistleblower's identity and the information from which this identity could be inferred, directly or indirectly, is also indispensable for the defence of the person involved. In both above cases, the Whistleblower is notified in writing of the reasons for the disclosure of the confidential data. Also, all Reports are exempt from the right of access provided for, and to the extent applicable to the private sector, by Arts. 22 et seq. of Law 241/1990 and Arts. 5 et seq. of Legislative Decree 33/2013. The measures to protect the confidentiality of the Whistleblower are aimed at, among other things, ensuring that he/she is subject to no form of retaliation.
- **Prohibition of retaliatory or discriminatory acts against Whistleblowers**: the Company prohibits all forms of active or omissive retaliation and discrimination even if only attempted or threatened and that is carried out on account of the Whistleblowing and causes or could cause the Whistleblower direct or indirect unjust damage. This protection is guaranteed if the Report (even if subsequently assessed as unfounded) was filed in good faith because the Whistleblower had reasonable grounds to believe that the information on the reported breaches was true when the Report was filed and that it fell within the objective scope of § 3.

  Discriminatory measures include unjustified disciplinary actions, harassment in the workplace and all other forms of retaliation that could lead to intolerable working conditions for the Whistleblower[1].

Retaliatory or discriminatory action taken against the Whistleblower can lead to disciplinary proceedings against those responsible and appropriate disciplinary measures in accordance with applicable national labor laws.

A Whistleblower who believes he/she has suffered retaliation/discrimination for having filed a Report must file a new Report concerning the retaliation/discrimination suffered. In these cases, the Company ensures that all related investigations are carried out promptly.

- **Duty of independence and professionalism in the management of reports**: all persons involved, in any capacity whatsoever, in managing reports must perform their duties independently and ensure accurate and efficient management of all reports. More specifically, the body in charge of handling reports is autonomous, dedicated and composed of staff specifically trained for this activity.
- **Protection of whistleblowers**: the Company protects whistleblowers regarding both the confidentiality of the Reports concerning them and of any investigations carried out, and the protection of them from all retaliatory and/or defamatory actions.
- **Protecting the integrity of Reports**: the web platform guarantees that no Report (from the notification to the decision-making stage) can be deleted and/or altered.

---

[1] Examples include:

- dismissal, suspension or equivalent measures;
- downgrading or non-promotion;
- change of duties, change of workplace, reduction of salary or change of working hours;
- suspension of training or any restriction on access to it;
- negative feedback notes or references;
- adoption of disciplinary measures or any other penalty, including a fine;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- failure to convert a fixed-term employment contract into a permanent employment contract where the employee had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, in particular on social media, or economic or financial loss, including loss of economic opportunities and loss of income;
- inclusion in improper lists based on a formal or informal sectoral or industry agreement, which could result in the person being unable to find employment in the same sector in future;
- early termination or cancellation of a contract for the supply of goods or services;
- cancellation of a licence or permit; or
- a request to undergo psychiatric or medical examinations.

## 6 THE REPORTING SYSTEM

The Whistleblowing system comprises the following internal channels:

1. web platform accessible at the following link;
2. registered telephone line/voice messaging system accessible at the following phone number: **+39 02 87377216**; and
3. direct meeting, upon request to the Human Resources Function Coordinator.

The Company recommends that Whistleblowing reports should be filed through the web platform because it is specifically designed to guarantee the Whistleblower's ease of use, confidentiality and privacy.

In order to protect the Whistleblower's privacy without exposing the Company to possible violations of the GDPR, it is not possible to use IT devices, telephone equipment and/or company networks to file Reports (either through the web platform or through a recorded telephone line/voice messaging system).

The Company recommends using the web platform unless it cannot be accessed for technical reasons, as:

a. the use of alternative channels cannot guarantee the same level of protection for Whistleblowers and efficiency in the handling of reports; or

b. in case of anonymous Reporting, the use of the web platform is the only way to ask for clarification from the Whistleblower while preserving his/her anonymity.

If the Whistleblower uses the recorded telephone line/voice messaging system or requests a direct meeting with the Human Resources Function, the System Manager or the person taking part in the direct meeting has the right, subject to the Whistleblower's consent, to document the Whistleblowing (as the case may be through a verbatim transcript or recording of the conversation, or a detailed report or minutes).

The Whistleblower is given the opportunity to verify, rectify and approve the transcript, record or minutes of the meeting.

Transcripts, reports and minutes relating to Reports received through internal channels other than the web platform are then entered into the web platform by the System Administrator.

For the next steps in the process of handling oral reports, the following paragraphs apply.

In any case, anyone who receives a Report through channels other than those provided for by the Reporting system, or in case the Report reaches a person who is not competent to handle it, they must promptly – and within 7 days from receiving the Report – forward it to the System Administrator, who will enter it into the web platform and simultaneously notify the Whistleblower of its transmission.

### 6.1 AUTHENTICATION IN THE PLATFORM AND SENDING OF REPORTS

The Whistleblower accesses the web platform through the dedicated link on the corporate website.

The web platform will request authentication from the Whistleblower, whose identification data will be stored in a separate database that the Company will not have access to, in order to guarantee confidentiality of the Whistleblower's identity and the impossibility of tracing it when processing the Report. The access credentials to this separate *database* will be provided exclusively to a person external to the Company, who must certify the existence of all statutory requirements for accessing the Whistleblower identification data.

The web platform also allows anonymous Reporting. Both methods of reporting through the web platform guarantee confidentiality, privacy and protection for the reporter.

Once authenticated, the Whistleblower: (i) reports the breach; (ii) fills in the required fields; (iii) enters a precise description of the facts and persons involved; and (iv) attaches all supporting documentation.

The web platform facilitates interaction with the Whistleblower and any requests for clarification from him/her, while ensuring maximum protection and confidentiality and protection from retaliatory and/or defamatory reports.

Upon receiving the Report, the web platform returns an initial notice confirming receipt and acceptance of the Report and sends the Whistleblower a unique identification code linked to the Report and through which he/she can check any updates on the Report by accessing the web platform. This unique identification code prevents any identification of the reporter, whose identity remains confidential. Each reporter is responsible for safeguarding it and preventing its release to or access by any other parties.

Once the Report has been uploaded and the unique identification code has been received:

a. the Whistleblower may check the progress of the Report at any time by accessing the web platform;
b. the System Manager may continue to communicate confidentially with the Whistleblower through the web platform and request further details if the Report is not sufficiently substantiated.

In light of the above, the Whistleblower should periodically access the web platform to check for any clarification requests on the Report submitted.

## 6.2 TAKING CHARGE

Once the Report has been received, the web platform sends an acknowledgement of receipt of a new Report to the System Manager 's mailbox, indicating the nature of the Report but without providing any detailed information on its content.

Upon receipt, the System Manager makes a preliminary assessment and classifies the Report based on its nature.

At this stage, the System Manager must immediately archive Reports that are clearly unfounded, instrumental or outside the scope of application of this Policy.

All the potential conflicts of interest that may concern any person who is an active part of the Reporting System must be handled adequately.

*Conflicts of Interest concerning the System Manager*
If, while handling the Report, any potential conflict of interest concerning the System Manager arises, the System Manager must not proceed with handling the Report (even in the preliminary assessment and classification phase) and must therefore inform the Reporting Committee. In this case, the preliminary assessment and classification will be conducted by the Reporting Committee.

*Conflicts of Interest concerning the Reporting Committee*
In the event of a conflict of interests that involves a member of the Reporting Committee, he/she must refrain from all activity relating to managing the Report.
Where, instead the whole Reporting Committee is involved in the conflict of interests, the Report will be handled by:

(i) The Supervisory Body ("**S.B.**") for Reports that are relevant under Legislative Decree 231/2001;
(ii) As a residual measure, to the management body.

The Company's Reporting Committee comprises the Human Resources Function Coordinator, the CFO and the Compliance Function.

## 6.3 INITIAL ASSESSMENT AND PRELIMINARY INVESTIGATION

The System Manager verifies, for Reports that have not been immediately discarded, whether they are accompanied by sufficient elements to assess their validity.

If the Report is not obviously unfounded, instrumental or outside the scope of this Policy but is insufficiently detailed, the System Manager must prepare the appropriate requests for additions/clarifications to the Whistleblower.

Once this initial assessment has been carried out and enough further clarification has been provided, the System Manager must decide whether to:

i. archive Reports that, following the preliminary assessment, are believed to be unfounded and/or inadequately documented, despite clarification obtained; or

ii. file Reports that, following the initial assessment, are reasonably well-founded and supported by sufficient elements to proceed with the preliminary investigation phase and: (i) classify the Report based on its nature by using the categories listed on the platform; (ii) carry out the preliminary assessment; and (iii) inform the Reporting Committee of the need to proceed with the preliminary investigation phase. If the Report falls within the scope of the 231 Decree 2001, it must also be managed in accordance with the 231 Model adopted by the Company.

If the Whistleblowing Committee proceeds with the investigation, it must prepare – together with the functions that may be involved – a specific "investigation plan". In the event that the Reports fall within the scope of Decree 231/2001, the Supervisory Body must be involved in order to be able to supervise the functioning and application of the 231 Model.

The investigation plan specifies:

- how the investigation is to be carried out (requests for additions/clarification to the Whistleblower, performance of the checks considered necessary, etc.);
- the internal or external Company functions in charge of conducting the investigation;
- all functions that could be affected by the violation based on the subject matter dealt with;
- any other persons who could provide additional information on the facts reported and whose hearing must be conducted in compliance with the principles of impartiality, confidentiality and protection of the identity of the Whistleblower; and
- the timeframe that the investigation should be carried out under.

The investigation phase is completed within 60 days from receiving the Report – except in cases where Reports concerning particularly complex situations require a longer assessment period – in compliance with the principles of impartiality, competence and professional diligence.

If, during the investigation, disclosure of the identity of the Whistleblower becomes indispensable for the defence of the person involved, the Company must explain to the Whistleblower the reasons why the confidential data has been disclosed and request the Whistleblower's consent to disclose his/her personal data.

## 6.4 DECISION

At the end of the investigation/investigation phase, the Reporting Committee expresses its decision on the Report, identifies – with the possible involvement of other corporate functions and/or external consultants (incl. the Supervisory Body) where necessary – any disciplinary measures and possible corrective actions to be proposed, and prepares a report on the outcome of the investigations carried out.

In any case, the feedback to the Whistleblower on the outcome of the relevant Report must be provided within three months from the date of the acknowledgement of receipt of the Report, or – in the absence of such an acknowledgement – within three months from expiry of the seven-day time limit for such notice. If the investigation has not been concluded due to facts that could require – for the purposes of verification – more than three months, it is in any case necessary to provide the Whistleblower with an interim reply at the expiry of the deadline indicated.

*Disciplinary measures*

Disciplinary measures must be appropriate and proportionate to the violation ascertained, also considering the possible criminal relevance of the conduct, and must comply with all provisions of applicable national labour laws.

All disciplinary measures proposed following ascertainment of the violation must be shared with the functions concerned by the violation and with the Human Resources Function. All measures are then finally approved and adopted by the Human Resources Function and communicated to the person responsible for the violation, in compliance with all applicable national labour laws.

*Corrective measures*

The Company's Reporting Committee informs the corporate functions affected by the violation of all corrective measures suitable to remedy the consequences of the violation and to prevent the risk of violations like the one reported.

The functions concerned by the breach confirm the implementation of the measures identified and inform the Reporting Committee of their outcome. The Reporting Committee, in turn, informs the System Manager of the implementation of the corrective measures to follow up with the Whistleblower.

### 6.5 REPORTING

At least once a year, the System Manager draws up a report on the Reports received and handled, to be forwarded by the Reports Committee to the respective corporate management and control body, as well as to the Supervisory Body.

In any case, the System Manager, at any stage of the process of managing a Report, may inform the company's management and control body of any Report that could materially impact the Company.

### 6.6 INFORMING THE REPORTED PERSON

As part of all the phases of the Whistleblowing management process, the Whistleblowing

Committee considers how to inform the reported person of the transmission of the Report against him/her, the conduct of the relevant investigation and its outcome.

More specifically, when the Report against him/her is announced, it needs to be assessed on a case-by-case basis to verify whether the release of such information could prejudice the conduct of the investigations necessary to ascertain the facts that form the subject of the Report, or whether, on the contrary, the involvement of the Reported person is necessary for development of the investigation.

The Company guarantees, in any case, the right of the reported person to be able to defend himself/herself and to be informed (within a reasonable time) of the charges and of any disciplinary measures against him/her.

## 7 TRACEABILITY OF THE WHISTLEBLOWING MANAGEMENT PROCESS

Reports received (together with any attached documentation) are stored in the web platform’s computer archive, which prevents any form of deletion and/or alteration.

This documentation must be kept for as long as necessary to process the Report, and in any case no longer than five years from the date of communication of the final outcome of the Reporting procedure.

Once the Report has been assessed and/or filed or discarded, the System Manager proceeds with the anonymization of the personal/sensitive information contained in the Report. In any case, personal information related to Reports is processed in accordance with Regulation (EU) 2016/679 and Legislative Decrees 196/2003 and 51/2018 and therefore personal information that is manifestly not useful for processing a specific Report is not collected or, if accidentally collected, is deleted immediately.

The retention period for records and documents may be extended if legal proceedings have been initiated or initiatives taken by the employer (e.g. disciplinary measures, forwarding of records to the competent authorities etc.) that arose in whole or in part from the Report.

This is due to the fact that such records and documents generally do not contain specific references to the Reporter, without prejudice to the provisions of art. 12, par. 5, of Legislative Decree No. 24/2023.

## 8 EXTERNAL REPORTING

Given that, as explained in this Policy, the Company has set up appropriate internal reporting channels, in compliance with Legislative Decree 24/2023, Reporting is only permitted through the external channel activated by the National Anti-Corruption Authority (“**ANAC**”), if the Whistleblower has:

(i) already filed an internal Report that was not followed up;

(ii) reasonable grounds for believing that, if he/she were to file an internal Report, it would not be effectively followed up, or that the Report might give rise to the risk of retaliation; or

(iii) reasonable grounds for believing that the breach could amount to an imminent or obvious danger to the public interest.

Without the above prerequisites, the Report is not handled by ANAC and the person does not benefit from the protection under Legislative Decree 24/2023.

The external reporting channel activated by ANAC is available at the following link: https://whistleblowing.anticorruzione.it/#/

## 9 DISSEMINATION AND TRAINING

The Company ensures the dissemination of this Policy to all employees and third parties who have legal relations with it, as well as the organisation of training sessions on the subject. More specifically, the Company provides clear information on the channels, procedures and prerequisites for filing internal Reports, as well as on the channel, procedures and prerequisites for filing external Reports.

This information is:

- displayed and made easily visible in the workplace, as well as accessible to persons who, although not frequenting the workplace, have a legal relationship with the Company;
- published in a dedicated section of the corporate website; and
- published on the digital platform (where adopted by the Company) accessible to all personnel and dedicated to policy management.

Training for all employees is carried out regularly and, in any case, when the need arises and includes, as far as possible, case studies and examples aimed at avoiding the recurrence of any situations that have already arisen.

Additionally, new employees are promptly informed of the rules and procedures to protect employees in the event of whistleblowing.

## 10 REVISIONS AND UPDATES

This policy – and its subsequent modifications – is approved by resolution of the management body. Pursuant to art. 4, par. 1. of Legislative Decree of 10th March 2023, as well as the ANAC resolution n. 478 of 26th November 2025, before approving any substantial modification to this policy or to the Reporting System, the management body must preliminarily discuss them with the Trade Union Representation pursuant to art. 51 of Legislative Decree n. 81 of 15$^{th}$ June 2015.