PROCEDURE FOR REPORTING OFFENCES AND IRREGULARITIES WHISTLEBLOWING PURSUANT TO LEGISLATIVE DECREE NO. 24/2023

INDEX

1. Purpose
2. Normative references
3. Operating modes

1. PURPOSE

This procedure governs procedures for reporting:

- unlawful conduct (so-called Whistleblowing) relevant under Legislative Decree 231/2001;
- other violations of national or European Union regulations
- retaliation found as a result of the reports submitted.

Reports may be made by employees or external parties (e.g. suppliers, professionals, business partners) who must be informed of the contents of this document.

The provisions of this document do not apply to disputes, claims or demands of a personal nature or relating to one's employment relationship.

2. REGULATORY REFERENCES

- Legislative Decree no. 231/2001 - art. 6; Law no. 179/2017 - art. 2; Legislative Decree 24/2023 implementing Directive (EU) 2019/1937; Regulation (EU) 2016/679; Legislative Decree 196/2003.
- ANAC Guidelines as per Resolution No. 311/2023 on the protection of persons who report breaches of Union law and the protection of persons who report breaches of national laws. Procedures for the submission and management of external reports.

3. OPERATIONAL MODALITIES

Reporting Channels

The following reporting channels are available: Internal within the

- company organisation;
- External (ANAC - National Anticorruption Authority);
- Public dissemination (bringing information about violations into the public domain through the press, electronic media or media capable of reaching a large number of people);
- Complaint to the judicial authority.

The communication channels set up to facilitate the submission of internal written or oral reports are as follows:

- **Postal service** by letter addressed to:

PC COMPONENTS EUROPE SRL
Via Orazio Raimondi,47
00143 Rome
Reserved for attention of the SB

The envelopes containing the reports will be opened exclusively by the company's Supervisory Board, which will handle them with the utmost confidentiality in compliance with current privacy provisions.

- **Verbal communication by requesting a direct meeting with the Supervisory Board.**

At the request of the whistleblower, to be made by sending a relevant request through the postal service channel, a meeting with corporate Supervisory Board may be arranged or arranged, within a reasonable time, for direct oral communication.

If the reports do not fall within the scope of the Supervisory Board's operations because they do not relate to the predicate offences referred to in Legislative Decree No. 231/01, the Supervisory Board shall forward them to the relevant corporate function, which shall handle them in the same manner and with the same safeguards as set out in this procedure.

As a priority, whistleblowers must use the internal channel and, only under certain conditions, will it be possible to make an external report, a public disclosure or a complaint.
Whistleblowers may use the external channel (ANAC) directly when:

- The internal reporting channel is not active or, even if activated, does not comply with legal requirements;
- the reporting person has already made an internal report that was not followed up;
- the reporting person has reasonable grounds to believe , if he or she were to make an internal report, the report would not be effectively followed up or that the report might lead to a risk of retaliation;
- the person issuing the alert has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

Whistleblowers may directly make a public disclosure and/or a complaint to the competent judicial or accounting authority when:

- the reporting person has previously made an internal and external report or has directly made an external report that has remained unreported within the prescribed time limits on the measures envisaged or taken to follow up the reports;
- the person issuing the alert has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- the reporting person 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 violation.

Within the reporting channels indicated, the possibility of anonymous reports is foreseen, which, in this case, will be equated and treated as ordinary communications. In the case of anonymous reports through the internal channel, they shall be handled, as ordinary reports, with all the precautions and investigations aimed at preventing any cases of defamation or slander (offences punishable under Article 16(3) of Legislative Decree 24/2023), having been made in bad faith.
In any , the whistleblower or anonymous complainant, subsequently identified, who has disclosed that he or she has suffered retaliation, may benefit from the protection that Legislative Decree 24/2023 guarantees retaliatory measures

Content of reporting with the internal channel

The Whistleblower, regardless of the way in which the internal report is submitted, should preferably provide the following information, in order to enable the relevant assessment:

- company name of the company concerned by the alert:
- details of the person making the report, indicating the position or function held within the company or other relevant third parties (suppliers, business partners, etc.);
- a clear and complete description of the facts being reported;
- if known, the circumstances of time and place in which the acts were committed;
- if known, the particulars or other elements (such as the job title and the department in which the activity carried out) that make it possible to identify the person who has carried out the reported facts;
- an indication of any other persons who may report on the facts being reported;
- an indication of any documents that may confirm these facts (attaching copies where possible);
- any other information that may provide useful feedback on the existence of the reported facts.

Confidentiality obligations

The management of internal reports is entrusted to the company's Supervisory Board.
Regardless of the internal channel used by the whistleblower, the Supervisory Body shall handle reports in compliance with the provisions of Legislative Decree 24/2023 and the ANAC guidelines force of reference; in particular, this body shall handle all reports received in compliance with the GDPR - Regulation 2016/679 and Article 2 *quaterdecies* of Legislative Decree 196/03, guaranteeing anonymity/maximum confidentiality:

- the identity of the reporter;
- of the people involved;
- of the persons nevertheless mentioned in the report;
- the content of the report and related documentation.

Whistleblowing reports may not be used beyond what is necessary to adequately follow them up.
The identity of the whistleblower and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the whistleblower, to persons other than the Supervisory Board.
In criminal proceedings, the identity of the whistleblower is covered by secrecy in the manner and within the limits set out in Article 329 of the Code of Criminal Procedure.

Within the framework of disciplinary proceedings, the identity of the reporting person may not be disclosed, where the allegation of the disciplinary charge is based on investigations that are separate from and additional to the report, even if consequent to it.
Where the charge is based, in whole or in part, on the report and knowledge of the identity of the reporting person is indispensable for the defence of the accused, the report shall be usable for the purposes of disciplinary proceedings only where the reporting person has expressly consented to the disclosure of his identity; in such a case, the person making the report shall be notified in writing by the SB of the reasons for the disclosure of the confidential data, as well as in the internal and external reporting procedures referred to in this procedure when disclosure of the identity of the person making the report and of the above-mentioned information is also indispensable for the defence of the person concerned.

Without prejudice to the provisions of the internal and external reporting procedures, the person concerned may be heard or, at his request, shall be heard, also by means of a paper procedure through the acquisition of written observations and documents. With regard to the processing of personal data, including communication between the competent authorities, please refer Article 13 of the
D. Lgs. 24/2023.

Managing internal reporting channel

Within the framework of the management of the internal reporting channel, the Supervisory Board shall perform the following activities

- notify the reporting person, within seven days of the report, that the report has been received (by the same means of communication used by the whistleblower). To this end, the Supervisory Board must check, at least once a week, whether or not any report has been received in the relevant internal channels;
- maintaining contact with the whistleblower, including any requests for additions concerning the report;
- diligently follow up on reports received (including by means of relevant investigations);
- provide acknowledgement of the report within three months of the date of the acknowledgement of receipt or, in the absence of such notice, within three months of the expiry of the seven-day period from the submission of the report;
- make available, through company organisation and the following procedure, clear information on the channel, procedures and prerequisites for making internal reports, as well as on the channel, procedures and prerequisites for making external reports. This information should be displayed/easily visible in the company workplace and in a dedicated section of the company website.

Any oral communications/reports must be documented by the Supervisory Board by means of a specific verbatim transcript (signed by the whistleblower after verification of the contents).

The management and verification of the justification of the circumstances represented in the report are entrusted to the Supervisory Board, which does so in compliance with the principles of impartiality and confidentiality, carrying out any activity deemed appropriate, including the personal hearing of the reporter and any other persons who may report on the facts reported.

If, at the outcome of the verification, the report proves to be well-founded, the Supervisory Board shall, in relation to the nature of the violation and insofar as applicable, take action:

- to file a complaint with the competent judicial authority;
- communicate the result of the assessment to the Head of the Area to which the author of the ascertained breach belongs, so that he may take the management measures falling within his competence, including, if the prerequisites are met, the exercise disciplinary action;
- to take any further measures and/or actions that may be necessary in the specific case to protect company.

Protection measures for whistleblowers

The protective measures provided for in this paragraph apply to the authors of alerts when the following conditions are met:

- at the time of the report or public disclosure, the reporting or whistleblowing person had reasonable grounds to believe that the information about the reported, publicly disclosed or reported violations was true and fell within the objective scope of this procedure (without bad faith on the part of the whistleblower);
- the reporting or public disclosure was made the basis of the following procedure;
- The person's reasons for reporting or denouncing public disclosure are irrelevant for the purposes of his or her protection.

Where the criminal liability of the reporting person for offences of defamation or slander or, in any case, for the same offences committed with the report to the judicial authority or his civil liability for the same offence, in cases of wilful misconduct or gross negligence, is established, even by a judgment of first instance, the protections provided for in this Chapter are not guaranteed and a disciplinary sanction is imposed on the reporting or whistleblowing person.
Therefore:
retaliation against whistleblowers in any form whatsoever is prohibited.
The Company will sanction any form of threat, discrimination or retaliation against whistleblowers and any further breach this procedure and/or related legal requirements.

Retaliation" against the whistleblower shall mean any conduct, act or omission, even if only attempted or threatened, occurring by reason of the whistleblowing, reporting to the judicial or accounting authorities, or public disclosure, and which causes or may cause, directly or indirectly, unjustified harm to the whistleblower or to the person making the report.

In the context of judicial or administrative proceedings or extra-judicial litigation concerning the ascertainment of the conduct, acts or omissions prohibited under this paragraph with respect to the whistleblower, it shall be presumed that such conduct or acts were put in place as a result of the whistleblowing, public disclosure or complaint to the judicial or accounting authorities. The onus of proving that such conduct or acts are motivated by reasons unrelated to the whistleblowing, public disclosure or complaint shall be on the person who has carried them .

Examples of retaliatory behaviour

- dismissal, suspension or equivalent measures;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references;
- the adoption of disciplinary measures;
- coercion, intimidation, harassment ostracism;
- discrimination or otherwise unfavourable treatment;
- the failure to convert a fixed-term employment contract into an employment contract of indefinite duration, 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, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- the early conclusion of the contract for the supply of goods or services;

Retention of documentation relating to alerts

Reports, any annexes and all supporting documents also relating to the management of reports (or copies thereof), are kept by the Supervisory Board for the time necessary for their processing and, in any case, for no longer than five years from the date of the communication of the final outcome of the reporting procedure (in compliance with the confidentiality obligations set out in this procedure and in the binding legislation).

These requirements must also be complied with in the case of any oral communications/reports transcribed by the Supervisory Board.

Access to the archive is only allowed to the Supervisory Board and is protected in accordance with the applicable privacy/data protection regulations.