



---

**PROCEDURE FOR THE PROTECTION OF PERSONS REPORTING  
BREACHES IN THE COMPANY**

---

**Contents**

- 1. Purpose ..... 3
- 2. Scope of application ..... 3
- 3. Terminology ..... 3
- 4. References..... 4
- 5. Duties and responsibilities ..... 5
- 6. Person who can make a disclosure (so-called whistle-blower) ..... 6
- 7. Internal disclosure channel. Manager..... 6
- 8. Management procedure for internal disclosures ..... 7
  - 8.1 Description of the internal reporting channel..... 7
  - 8.2 Written disclosure. .... 7
  - 8.3 Anonymous disclosure..... 8
  - 8.4 Verbal disclosure. .... 8
  - 8.5 Reporting disclosures to the wrong recipient. .... 8
  - 8.6 Preliminary enquiry procedure for the disclosure. .... 8
  - 8.7 Conflict of interest. .... 9
  - 8.8 Investigation. .... 10
  - 8.9 Storing internal disclosure documentation. .... 11
  - 8.10 Obligations regarding communicating information. .... 11
- 9. External disclosure. .... 11
- 10. Public disclosure..... 11
- 11. Duty of confidentiality..... 12
- 12. Protection of personal data. .... 13
- 13. Measures for protection and support..... 13
  - 13.1 Prohibition on reprisals..... 14
  - 13.2 Support measures..... 14
  - 13.3 Limitation whistle-blower’s liability..... 15
- 14. Disciplinary measures..... 15

## 1. Purpose

This procedure has been adopted by Podium Engineering S.r.l. (hereinafter also the “Company”) in accordance with the provision of Legislative Decree No. 24 of 10 March 2023, (abbreviated in the text to Decree or LD 24/2023), which implements EU Directive No. 2019/1937 of the European Parliament and Council of 23 October 2019, regarding the protection of persons who report breaches of domestic or European Union regulatory provisions (the so-called whistleblowing directive) harmful to the public interest or the Company of which they have become aware in the workplace.

This procedure was approved by the Board of Directors on 15/12/2023, together with specifying the organisational roles involved in the process for managing disclosures and their respective responsibilities.

This procedure comes into effect from the date of its approval by the Company’s Board of Directors.

This procedure may also be consulted on the Company’s website at the address: [www.podium-tech.com](http://www.podium-tech.com) and shall be affixed to the Company’s noticeboard.

## 2. Scope of application

This procedure applies to any disclosure of information regarding breaches (as set out more fully in paragraph 4) encountered in the workplace (meaning the employment relationship with the Company or the provision of professional/independent/collaborative services, both present or past), which are harmful to the public interest or the integrity of public administration or of the Company, disclosed via the appropriate reporting channels made available by the company itself

The scope of application of this procedure excludes:

- Disputes, claims or demands of a personal nature which relate solely to individual working relationships, or working relations with hierarchically senior persons;
- Breaches compulsorily governed by European Union or domestic regulations which already define the appropriate disclosure procedures;
- Breaches related to national security, as well as tenders regarding defence or national security matters.

## 3. Terminology

In terms of the Decree, the words have the meanings defined:

- **disclosures:** any written or verbal communication or communication made in conversation, provided it is not made anonymously, containing information about the breaches;
- **breaches:**
  - relevant unlawful conduct in terms of LD No. 231/2001;
  - unlawful acts which are covered in the application of domestic or European Union regulations relating to the following sectors: public tenders; financial services, products and markets and the prevention of money-laundering and financing terrorism; product safety and compliance; transport safety; protection of the environment; protection against radiation and nuclear safety;

food and feed security and the safety and wellbeing of animals, public health, consumer protection, protection of private life and personal data and security of networks and IT systems;

- breaches (acts or omissions) harmful to the financial interests of the European Union (in terms of Art. 325 of the Treaty on the Functioning of the European Union);
  - breaches (acts or omissions) of European Union regulations concerning competition and State assistance; breaches of regulations on Company taxes;
  - acts and conduct which frustrate the purpose and aims of the abovementioned provisions;
  - unlawful accounting, administrative and criminal offences not covered by the above lists.
- **information about breaches:** all information, including well-founded suspicions, concerning breaches committed or which, on the grounds of concrete indications, could be committed in respect of the business of the Company business with which the whistle-blower or those who report to the judicial/accounting authorities maintain a legal relationship, as well as information regarding conduct aimed at concealing such breaches;
  - **internal disclosure:** communication of information, disclosed through the established internal reporting channel;
  - **external disclosure:** transmission of information, disclosed through the external reporting channel;
  - **public disclosure:** placing information in the public domain about breaches through the press or by electronic means or, anyhow, through publication channels capable of reaching a great number of persons;
  - **whistle-blower:** a physical person who makes the report or public disclosure of information about breaches acquired in the person's workplace;
  - **manager:** a physical person, or internal organ, or an independent professional to whom the Company assigns the management of the reporting channel, with complete independence and specifically trained for carrying out the abovementioned mandate;
  - **facilitator:** a physical person who assists the whistle-blower in the reporting process, who works within the same workplace environment and whose assistance shall remain confidential;
  - **workplace:** work or professional activities, present or past, through which, irrespective of the nature of such activities, a person acquires information on breaches and in which environment risks suffering reprisals in the event of reporting or public disclosure or disclosure to judicial or accounting authorities;
  - **person involved:** a physical or juristic person referred to in the disclosure to whom the breach is attributed, or as person somehow complicit in the breach reported or publicly disclosed;
  - **reprisal:** any conduct, act or omission, even if only attempted or threatened, initiated because of the disclosure, or because of report to the judicial or accounting authorities or because publicly disclosed which results or may result in unfair damage directly or indirectly to the whistle-blower(s);
  - **follow-up:** action or actions launched by the person mandated to manage the reporting channel to assess the circumstances of the matters disclosed, the outcome of the investigation and any possible measures taken;
  - **feedback:** communication to the whistle-blower of the follow-up that has been instituted or which is intended to be instituted in respect of the disclosure;

#### 4. References

- Legislative Decree No. 24 of 10 March 2023;

- EU Directive No. 2019/1937;
- European Regulation No. 2016/679 (GDPR);
- Privacy Code (LD No. 196/2003);
- ANAC (National Anti-corruption Authority) guidelines for the protection of persons who make disclosures of breaches of European Union law and protection of persons who disclose breaches of domestic regulations - procedures for the submission and management of external disclosures.

## 5. Duties and responsibilities

The Company shall:

- make available, also in this procedure, clear information on the channel concerning the procedures and requirements for making an internal disclosure;
- issue an acknowledgment of receipt to the whistle-blower within the stipulated time frame;
- evaluate the credibility criteria of the disclosure;
- distribute the disclosure to any further internal persons involved, as defined for this procedure and coordinate any investigations, their outcomes and the review to be transmitted to the whistle-blower;
- inform the whistle-blower of the outcome at the termination of the management of the disclosure process;
- maintain communication with the whistle-blower including discussions, if requested by the latter; if necessary, manage further deliberations, manage enquiries, investigations and carry out actions to verify and assess the validity and scope of the disclosure;
- file and store documentation on the disclosure for the requisite regulatory period;
- ensure enforcement of the principle of confidentiality;
- provide a report to the person responsible for the internal disclosure channel regarding the decisions taken by the Company for the additional investigation of the matter raised by the disclosure;
- monitor the investigation phase by any internal departments involved or by any external professional bodies charged with investigation activities;
- devise programmes for improvement so as to avoid a repetition of the events raised by the disclosure;
- make available through Company channels all information relating to the channel, to the procedures and to the requisites for making internal disclosures;
- manage follow-up activities and any public disclosure in necessary instances;
- ensure enforcement of the principle of confidentiality.

The whistle-blower shall:

- report the disclosures in accordance with this procedure;
- be required to supply evidentiary information in regard to the matter disclosed.

The Manager shall:

- perform the function assigned for managing the internal channel made available by the Company, strictly in accordance with the provisions of Art. 5 of the Decree.

The Legal representative shall:

- interact with ANAC in cases of any external disclosure or any investigative activities initiated by the latter.

The Board of Directors/Single Director shall:

- ensure the adoption of any provisions in compliance with what is set out in the disciplinary system determined in the Organisational Model;
- approve this procedure within the framework of the assigned relevant organisational roles;
- ensure the application of protection measures for the whistle-blower.

## 6. Person who can make a disclosure (so-called whistle-blower)

The following may initiate a disclosure:

- employees;
- independent service providers and collaborators who perform their work at the Company;
- freelance professionals;
- consultants;
- volunteers and trainees, even if not on the payroll;
- shareholders;
- directors;
- service providers for third parties of any nature (irrespective of the kind of activities) even if no fee is being paid;
- persons exercising the office of administration, direction, control, supervision, or representation, even if the relevant performance is carried out *de facto* and not by right.

Moreover, all persons are also included in this category who, in whatever role, become aware of offences in the Company's workplace or:

- in cases where the employment relationship has not yet commenced;
- during the probationary period;
- on termination of the relationship.

## 7. Internal disclosure channel. Manager.

The Company has established an internal reporting channel which the whistle-blower must use to report information on breaches. The use of this channel ensures a more effective prevention and verification of breaches. This option satisfies the principle of a culture of intercommunication and corporate social responsibility, as well as improvement in the internal organisation of the Company.

The management of the internal reporting channel is assigned to the Manager, who shall be identified in the role of Quality Manager of the Company, granted full independence and suitable training to perform the assigned function in accordance with Art. 4(2) of the Decree.

The internal reporting channel provides only for the use of analogue written or verbal means.

The internal reporting channel shall ensure confidentiality of the identity of the whistle-blower, the facilitator (if applicable), of the persons involved or mentioned in the disclosure, as well as the contents thereof, annexed documentation as well as that of any person subsequently included.

## 8. Management procedure for internal disclosures

### 8.1 Description of the internal reporting channel.

The internal reporting channel is based on analogue written disclosure exclusively effected via postal registered letter.

The disclosure must be made using three sealed envelopes, the first two shall be numbered and contain the following information:

- Envelope Number 1: in this envelope must set out the identification data of the whistle-blower, together with a photocopy of his/her identity document;
- Envelope Number 2: in this envelope the details of the disclosure must be set out;
- The abovementioned two envelopes must be inserted into the third envelope;
- The third envelope must indicate, above and beyond the Company address, the notice: Confidential – for the attention of the Whistle-blowing Manager.

The Disclosure may be opened, read, and managed by the whistle-blowing manager alone, or any other persons authorised by the Manager in the event that further investigation of the disclosure matter is deemed necessary.

Processing of personal data shall be in accordance and comply with the duties provided for by the GDPR and by LD No. 196/2003 and amendments and additions thereto. The Company, as Data Controller, through the internal reporting channel shall be obliged to effect a preliminary analysis of the overall organisational structure including its possible impact on the protection of data (Art. 35 of the GDPR).

### 8.2 Written disclosure.

It is essential that the disclosure be as fully detailed as possible so that it is possible for the appointed Manager to assess the circumstances to admit and manage the disclosures. In particular, it is indispensable that the following be made clear:

- the timeframe and the place where the matter described in the disclosure was observed;
- the details of the matter;
- the personal details or other evidence which makes it possible to identify the person to whom the matters disclosed may be attributed.

Information concerning breaches must be truthful. Simple suppositions, barely credible indiscretions (so-called corridor gossip) as well as news in the public domain, falsehoods, (except those arising from innocent

mistake), manifestly unfounded or misleading, or merely pernicious or offensive will not be taken into consideration. On the other hand, it is not necessary that the whistle-blower be absolutely sure of the actual occurrence of the matters disclosed and the identity of the perpetrator thereof.

It is preferable that the person disclosing the breach provides documents which may give grounds for the matters disclosed, as well as an indication of other persons who may possibly be aware of the facts.

### **8.3 Anonymous disclosure.**

Anonymous disclosures, even if backed up by evidence, shall under no circumstances be taken into consideration.

Nevertheless, they shall be filed together with the others, solely with the aim of protecting the person making the disclosure, should his/her identity be later revealed.

### **8.4 Verbal disclosure.**

Besides making disclosure in analogical written form, the whistle-blower may also do so verbally, by requesting a meeting with the Whistle-blowing manager.

Such meeting shall be held in a place suitable for ensuring confidentiality of the person making the disclosure within 15 working days of the request, except where it is made in the Company's holiday closing period, in which case the time limit shall be postponed till the first day of reopening.

With the consent of the whistle-blower, a record of the proceedings shall be made on a recording device suitable for storing and for verbal reproduction of same; in the event of consent not being given or in the absence of appropriate recording devices, minutes of the verbal proceedings shall be taken, which shall be perused by the whistle-blower, who shall be entitled to rectify the text, signing it together with the person(s) who prepared it and who attended the meeting.

### **8.5 Reporting disclosures to the wrong recipient.**

In the event that the disclosure is reported to a person different to the person designated to receive it, the person receiving such is obliged within seven days to transmit it to the Manager, notifying the whistle-blower thereof.

In the case of an involuntary reporting of the disclosure to a person different to the person authorised to receive it, the whistle-blower shall show that this was done out of negligence and that he/she had no personal interest in the erroneous reporting.

### **8.6 Preliminary enquiry procedure for the disclosure.**

On receipt of the written disclosure, the Company shall forward it without delay to the Manager without opening it.

In the event of the premature opening of the disclosure by the Company's reception personnel because of the lack of the notification "Confidential – for the attention of the Whistle-blowing Manager", or by mistake, the Manager, on receipt of the disclosure, shall draft a suitable report describing the condition of the document and identifying the person(s) who opened it.



Once the disclosure has been received, the Manager shall, within seven days, ensure that acknowledgement of receipt is transmitted to the whistle-blower. In the event that the details of the person making the disclosure are not provided or is not otherwise unknown to or unknowable by the Manager, the disclosure will be filed without further ado.

The Manager shall first make an assessment as to whether the disclosure requires further action, ascertaining in the first instance if all the procedural requirements referred to in paragraph 8.1. have been followed, if the person making the disclosure falls into the categories authorised to do so and that the disclosure does not concern matters beyond the applicable scope of the regulations.

If the outcome of the investigation as to whether to proceed with the disclosure is positive, the Manager shall then conduct further enquiries as to whether the disclosure is admissible and in particular verifying whether:

- all the data constituting essential parts of the disclosure have been collected. In particular:
  - the timeframe and the place where the matter described in the disclosure was observed;
  - the details of the matter;
  - the personal details or other evidence which makes it possible to identify the person to whom the matters disclosed may be attributed.
- The factual evidence relating to the breaches governed by legislation is not manifestly unfounded;
- The presentation of the facts is not made in a generic way so as to make them incomprehensible to the Manager;
- No steps have been taken to attach documentation so the breaches committed cannot be determined.

After this further enquiry, the Manager, where deemed necessary, may request clarification from the person making the disclosure to undertake further investigation, as better set out in paragraph 8.8 below.

After the assessment of whether to proceed to deal with the disclosure and the admissibility of the disclosure, the Manager shall institute measures to declare the disclosure prosecutable and admissible or whether there are reasons simply to archive it and shall notify the whistle-blower thereof within three months of receipt of the disclosure.

### **8.7 Conflict of interest.**

It is to be noted that, from the time of receipt of the disclosure to the end of the investigation, any person who may be in a situation of conflict of interest, must declare their own position, not taking any decisions to ensure the application of the principle of impartiality.

In the event that the disclosure concerns the Manager, the disclosure shall be addressed directly to the Company's Chairman of the Board of Directors/Sole Director, who shall carry out the activities assigned to the Manager as set out above, if necessary, relying on specialised external consultants to carry out the investigation.

## 8.8 Investigation.

Whenever it is necessary to obtain additional evidence, the Manager shall contact the whistle-blower at the address he/she has indicated. In the event that the whistle-blower does not provide the additional information requested within three months of the request for such information, the Manager at his/her discretion shall file the disclosure while informing the whistle-blower thereof.

Once the Manager has confirmed that the disclosure is well-founded and has received the necessary additional evidence from the whistle-blower, the Manager may decide to set in motion all the enquiries necessary for further investigation of what has been disclosed.

In particular, as well as to formulate recommendations for the adoption of the necessary corrective measures in the sectors and in the corporate processes concerned, with the aim of reinforcing the internal control system, the Manager may, for example:

- examine the documentation received from the person making the disclosure and that obtained from the internal organs or from the external persons concerned;
- acquire information from the whistle-blower, guaranteeing confidentiality concerning his his/her identity, and/or from other persons within the corporate structure or from external persons involved in various capacities, who may be aware of the facts or the circumstances relating to the disclosure, by consulting them, which shall be, if necessary, recorded;
- make use of external consultants.

The person involved shall in any event be heard and consulted including via printed means by gathering written observations and documents.

In any event, the Manager shall ensure the concealment of data and all information which may tend to reveal the identity of the whistle-blower.

The Manager shall obtain an undertaking to maintain confidentiality regarding the facts dealt with and the identity of the persons involved from all internal and external persons involved in the investigation.

The Manager shall evaluate, case by case, with the Company, whether and which corporate sections should appropriately be involved for the relevant enquiries, to be carried out nevertheless under the principle of confidentiality and adopting of any subsequent measures.

The Manager, at the end of the investigation shall see to the drafting of a written final report.

The report may provide for:

- the filing of the disclosure for lack of properly grounded motivation;
- the declaration of the reliability of the disclosure with the transmission of the documentation to the corporate bodies responsible for the requisite provisions or measures to be adopted.

No final provision shall be applied, nor may disciplinary action be undertaken by the Manager.

A report on the outcome of the investigation must be provided to the whistle-blower within three months of the receipt of the disclosure, or within seven days of the time of presentation thereof.

Only in exceptional cases, when the complexity of the disclosure demands it, or depending on the response time of the whistle-blower, the Manager, having previously timeously informed the latter before the expiry of the time limit, may continue with the investigation for the time required, updating the whistle-blower periodically and notifying the latter of the final outcome.

In the event of defamation or libel, confirmed by a ruling in a Court of first instance, the Company shall initiate disciplinary measures against the whistle-blower.

#### **8.9 Storing internal disclosure documentation.**

Internal disclosure and all associated documentation, or documentation acquired at the request of the Manager for additional evidence, shall be stored strictly for the period necessary for processing the disclosure itself and, in any case, only for a maximum period of five years as from the notification of the final outcome of the disclosure procedure

In all the cases mentioned, it is necessary that procedure for storing the disclosure and associated documentation, comply with European Community and domestic rules concerning the processing of personal data as well as the requisite protection measures for confidentiality relating to the whistle-blower and the other persons involved.

#### **8.10 Obligations regarding communicating information.**

Information regarding the channel, the procedures, and the preconditions for making a disclosure shall be displayed in the workplace, by affixing to the notice board for corporate communication. The same information shall also be uploaded in the appropriate section of the corporate website.

### **9. External disclosure.**

Under the following conditions, the whistle-blower may make a disclosure via the external channel of ANAC:

- in the event that, in the work environment, the channel for internal disclosure is not compulsory, or the channel itself has not been activated, or is not compliant with the necessary regulatory requirements;
- when the person making the disclosure has already made an internal disclosure in vain;
- if the whistle-blower has well-founded reason to consider that in making a disclosure internally no effective follow-up has been initiated, or that it, in and of itself may result in the risk of reprisals against him/her;
- in cases where the person making the disclosures has good reason to believe that the breach disclosed could pose an imminent or clear threat to the public interest.

The external organ authorised to receive external disclosures is ANAC in accordance with the methods and procedures duly adopted and available for consultation on the website [www.anticorruzione.it](http://www.anticorruzione.it).

### **10. Public disclosure.**

As residual and optional alternatives, the whistle-blower may resort to public disclosure in the following circumstances:

- when he/she has previously made an internal or external disclosure or has directly made an external disclosure without having received any feedback within the requisite time;
- in cases where he/she has well-founded reason to believe that the breach constitutes an imminent or clear threat to the public interest;
- when he/she has well-founded reason to believe that the external disclosure may result in the risk of reprisals, or could fail to result in effective follow-up because of the specific circumstances of the actual case, or those circumstances that could cause the evidence to be concealed or destroyed, or when there are well-founded concerns that the person receiving the disclosure may have colluded with the perpetrator of the breach or even be involved in the breach itself.

## 11. Duty of confidentiality.

Any disclosure and the relevant annexures shall not be used beyond the time necessary to deal with the matter.

It is understood that the identity of the whistle-blower together with any other information which it may elicit, directly or indirectly, such identity shall not be revealed without the express consent of the whistle-blower him/herself, to any persons different to those competent to receive or deal with the disclosure, as expressly authorised for the processing of such data in terms of Articles 29 and 32(4), of EU Regulation No. 2016/679 and Article 2(14) of the code for the protection of personal data as provided for in LD No. 196 of 30 June 2003.

The Company shall keep confidential the identity of the persons involved, of facilitators and persons mentioned in the disclosure until the conclusion of the proceedings carried out regarding the disclosure itself, and applying the same guarantees provided for the whistle-blower.

Circumstances which may affect the protection of the right to confidentiality may include:

- in criminal proceedings, the identity of the whistle-blower is subject to confidentiality in accordance with the methods and limitations set out in Article 329 of the Criminal Procedure Code: the duty of confidentiality of actions taken in the preliminary investigation up to the time when the suspect has no right to be made aware of the investigation and in any case not beyond the end of such phase;
- in proceedings brought before the Court of Auditors, the identity of the whistle-blower may not be revealed until the investigatory phase has ended;
- in disciplinary proceedings, the identity of the whistle-blower may not be revealed unless the dispute concerning the disciplinary complaint is based on specific and further analyses of the disclosure, even if resulting therefrom;
- where a dispute is based, wholly or in part on the disclosure and knowledge of the identity of the person making the disclosure is indispensable for the defence of the suspect, the disclosure will only be able to be used for purposes of disciplinary proceedings only in the presence of and with the express consent of the whistle-blower to having his/her identity revealed;
- in cases of disciplinary proceedings brought against the alleged perpetrator of the conduct disclosed, notification will be given to the whistle-blower in written form of the reasons for the revealing of confidential data when the disclosure is indispensable to the defence of the person involved.

The following are included in the duty of confidentiality:

- suspension regarding the disclosure and the document attached thereto from the right of access to administrative actions as provided for in Article 22 *et seqq.* of Act No. 241/1990 and from general civil access in terms of Article 5 *et seqq.* of LD No. 33/2013;
- administrations and bodies involved in the management of disclosures guarantee confidentiality throughout all the phases of the whistleblowing procedure, including the possible transfer of the disclosure to other competent authorities.

## 12. Protection of personal data.

Any processing of personal data, including communication with competent authorities, is governed by the rules of:

- (EU) Regulation 2016/679;
- by Legislative Decree No. 196 of 30 June 2003, and subsequent additional and integrations.

The communication of personal data by institutions, organs or bodies of the European Union is carried out in compliance with (EU) Regulation No. 2018/1725.

The processing of personal data relating to the receipt and management of disclosures is carried out by the data controller, in accordance with the principles of Articles 5 and 25 of (EU) Regulation 2016/679, after providing suitable information to the whistle-blower and to persons involved as well as adopting measures appropriate for the rights and freedoms of interested parties.

## 13. Measures for protection and support.

Adequate measures are provided for the protection of whistle-blowers against direct and indirect reprisals.

Protection measures apply if, at the time of the disclosure, the whistle-blower has good reason to believe that the information concerning the breaches disclosed are true, fall within the scope of and are in accordance with the disclosure procedure.

In cases of defamation or libel, confirmed by a ruling in a court of first instance, the safeguards are not guaranteed.

Protection measures also apply to:

- a) to facilitators;
- b) to persons in the same working environment as the person making the disclosure/whistle-blower or persons who are associated by reason of a stable emotional relationship or kinship up to the fourth degree;
- c) work colleagues of the person making the disclosure/whistle-blower who work in the same working environment and with whom he/she has a regular and current relationship;
- d) to entities belonging to the person making the disclosure/whistle-blower or for which such person works, as well as to entities which operate in the same working environment as the aforementioned person.

### 13.1 Prohibition on reprisals.

The whistle-blower and the persons named in the previous paragraph may not be subjected to any retaliatory actions. By way of example but not limited thereto, the following may be considered retaliatory actions:

- dismissal, suspension or equivalent measures;
- demotion or lack of promotion;
- change of functions;
- change of work place;
- reduction of salary;
- change to working hours;
- suspension of training or any restriction of access to any such training;
- adverse personnel reports or negative references;
- adoption of disciplinary measures or other penalties, including financial penalties;
- coercion;
- intimidation;
- harassment;
- ostracism;
- discrimination, or in any case unfavourable treatment;
- failure to convert a fixed-term employment contract to a permanent contract of employment, where the employee had a reasonable expectation of such conversion;
- failure to renew or early termination of a fixed-term employment contract;
- harm, including to personal reputation, in particular on social media,
- economic or financial prejudice, including loss of economic opportunities and loss of income;
- insertion of an inaccurate listing based on a sectoral or industrial agreement whether formal or informal, which could make it impossible for the person to find work in the sector or industry in future;
- the early termination or cancellation of contract to supply goods or services;
- cancellation of a licence or permission;
- a request to submit to medical or psychiatric examination.

Actions taken in breach of the prohibition on reprisals are void.

In legal or administrative proceedings, or also in cases of extrajudicial disputes for verifying prohibited conduct, acts or omissions against whistle-blowers, it will be assumed that such has occurred as a result of the disclosure. The onus of proving that such conduct or acts are motivated by reasons other than the disclosure rests on the person who has committed the retaliatory acts.

Whistle-blowers may communicate to ANAC any reprisal which they have suffered, or which was attempted or could potentially be foreseen.

L'ANAC will inform the National Labour Inspectorate, so the appropriate measures can be adopted.

### 13.2 Support measures.

The whistle-blower may have recourse to Tertiary Sector bodies on the list published on the ANAC site. Where bodies carrying out activities of general interest are concerned, not for financial gain, for public

interest, community and socially-oriented purposes (“fostering a culture of compliance, peace between peoples, non-violence and unarmed defence; promotion and safeguarding of human, civil, social and political rights, as well as the rights of consumers and users of general interest activities, promotion of equal opportunities and initiatives for reciprocal assistance, including time banks and co-operative purchasing groups”) and which have signed agreements with ANAC.

The support measures provided consist of information, assistance and free consultations on whistleblowing methods and protection from reprisals provided by national and European Union Regulations, on the rights of persons involved, as well as on the methods and conditions for access to legal aid at State expense.

### **13.3 Limitation whistle-blower’s liability.**

There is no liability (either of a civil or administrative nature) for anyone disclosing or publishing information concerning breaches:

- covered by a duty of secrecy,
- relating to protection of copyright,
- provisions relating to the protection of personal data,
- which harm the reputation of the person involved or reported,

if, at the time of disclosure or publication, sound reasons existed to that it was deemed necessary to disclose or publish such information to disclose the breach and that the disclosure was made in accordance with protection conditions.

Furthermore, the following are specifically noted among the protection measures:

- the rights to make a disclosure and the relative protection cannot be limited by contractual agreement;
- the exclusion of any liability, either civil or administrative, for acquiring or for access to the information concerning the breach, except in circumstances where such conduct constitutes an offence;
- the exclusion of any other liability concerning conduct, acts or omissions carried out if linked to the disclosure and strictly necessary for disclosing the breach or, in any event, not associated with the disclosure.

## **14. Disciplinary measures.**

Following approval of this procedure, it is intended that the Company’s Disciplinary Code be amended and the provisions for penalties are to be included to be applied to those who are found to be responsible for the following conduct:

- acts of reprisal or proposals for the adoption of such acts, interference with the disclosure (even attempted), or breach of the duty of confidentiality;
- failure to establish channels for disclosure, failure to adopt procedures for the management of same, the adoption of procedures which do not comply with the requirements of the decree, or failure to take action to verify and analyse disclosures;

- criminal liability of the whistle-blower, confirmed by a ruling in a Court of First Instance, for offences of defamation or libel, or civil responsibility for the same reason, in the event of wilful intent or gross negligence;

as well as well as towards anyone who contravenes this procedure.

ANAC may intervene for the same offences by applying administrative fines (from Euro 500 to Euro 50 000) in the event that such offences are verified.