

# **DISCLOSURE PROCEDURE OF WRONGDOINGS AND MISCONDUCT (SO CALLED *WHISTLEBLOWING*)**



## **Contents**

<b>1. Purpose and scope.</b>	<b>page 03</b>
<b>2. Definitions.</b>	<b>page 03</b>
<b>3. Recipients and scope of application.</b>	<b>page 05</b>
<b>4. Subject matter of the Disclosures.</b>	<b>page 06</b>
<b>5. Content of the Disclosures.</b>	<b>page 07</b>
<b>6. Disclosure Recipients.</b>	<b>page 08</b>
<b>7. Disclosure submission Procedure.</b>	<b>page 08</b>
<b>8. Internal Disclosure Management.</b>	<b>page 10</b>
<b>9. Protection measures.</b>	<b>page 12</b>
<b>9.1. Confidentiality obligations regarding Whistleblower identities.</b>	<b>page 12</b>
<b>9.2. Confidentiality obligations regarding the identity of those other than the Whistleblower.</b>	<b>page 12</b>
<b>9.3. Processing of Personal Data</b>	<b>page 13</b>
<b>9.4. Prohibition of retaliation.</b>	<b>page 13</b>
<b>9.5. Protection against retaliation.</b>	<b>page 14</b>
<b>10. Responsibilities of the Whistleblower.</b>	<b>page 15</b>
<b>11. Documentation archiving procedures.</b>	<b>page 16</b>
<b>12. Waivers and transactions.</b>	<b>page 16</b>
<b>13. Dissemination.</b>	<b>page 16</b>
<b>14. Penalties.</b>	<b>page 16</b>

## 1. Purpose and scope.

The Disclosure Management Procedure aims to ensure the confidentiality of the identity of those who, in good faith, disclose the occurrence of unlawful conduct and, pursuant to Leg. Decree no. 231/2001, by establishing clear and identified information channels suitable for the reception, analysis and processing of such disclosures.

The purpose of this tool is to allow **Abra Beta S.p.A.** to prevent the occurrence of wrongdoings and/or irregularities within the same or, in any case, with regard to the relations that third parties entertain with the former, by intercepting such conduct, in order to remedy and correct it thanks to the active and responsible involvement of all Stakeholders.

This procedure is an official document and, therefore, is approved by the Company Board of Directors, which is also responsible for updating and integrating the same.

## 2. Definitions

- **Whistleblower or Reporting Individual:** the Whistleblower is an individual who reports or publicly discloses information about violations obtained within the scope of the work context;
- **Facilitator:** an individual who assists the Whistleblower in the whistleblower process, operating within the same work context and whose assistance must be kept confidential;
- **Work-related context:** current or past work activities or professional services performed in relation to the Company (see § 3 lett. a) - o), through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information;

Whistleblowing or public disclosures or complaints to the Judicial and Accounting authorities;

- **Person concerned or Alleged Perpetrator:** means a natural or legal person who is referred to in the internal or external Disclosure or the public disclosure of the person accused of committing the breach or who is attributed to the disclosed or public ally disseminated breach;
- **Disclosure Recipients or Recipient:** a person who, in whatever capacity, is the recipient of all Whistleblowing disclosures;
- **Follow-up:** refers to the action adopted by the Recipient assigned to assessing the subsistence of the reported facts, the outcome of the investigations and any measures put in place;
- **Feedback:** refers to the communication to the Whistleblower of any information regarding the follow-up action carried out or to be carried out in the future;
- **Disclosure or Disclosing:** means the verbal or written communication of information on the breaches;

- **Information on breaches:** means information, including founded suspicions, on actual or potential breaches, which were committed and, given the basis of the actual evidence, are very likely to occur in the organisation with which the Whistleblower, or the reporting person who lodges a complaint with the Judicial Authorities, works or has worked (see § 3 lett. a) - o), plus the elements relating to any activities undertaken to conceal such breaches. This does not include information on breaches which are clearly unfounded, already of complete public domain or information based solely on rumours or unreliable sources (often referred to as "office gossip") nor irregularities in the management or organisation of work activities;
- **Internal reporting:** means the oral or written communication of information on the breaches submitted via the internal reporting channel;
- **External reporting:** means the oral or written communication of information on breaches submitted via the external reporting channel, i.e. via the channel activated by ANAC;
- **Public disclosure or public disclosing:** the use of the press, electronic means and disclosure media, and any other means of reaching a large number of persons;
- **Breaches:** which refer to conduct, acts or omissions which harm public interest or the integrity of public administration or private entities, and which consist of:
  - 1) administrative, accounting, civil or criminal offences which do not fall within the scope of sections 3), 4), 5) and 6);
  - 2) significant unlawful conduct pursuant to Leg. Decree no. 231 of 8 June 2001 or breaches of the organisational and management models envisaged therein, which do not fall within the scope of numbers 3), 4), 5) and 6);
  - 3) offences covered by EU or national decrees indicated in the annex to Leg. Decree no. 24/2023 or national acts drawn up to transpose the EU acts indicated in EU Directive 2019/1937, even when not referred to in the annex to Leg. Decree no. 24/2023 in the following sectors: (e.g. public procurement; financial services, products, and markets, including anti-money laundering and counter-terrorist financing; product safety and compliance; transportation safety; environmental protection; radiation protection and nuclear safety; food and feed; as well as animal health and welfare; public health; consumer protection; privacy protection and personal data security; and the security of networks and information systems;
  - 4) acts or omissions with a damaging impact on the financial interests of the EU, as indicated in art. 325 of the Treaty on the Functioning of the European Union as indicated in the secondary legislation in relation to the European Union;
  - 5) acts or omissions relating to the internal market, as referred to in art. 26(2) of the Treaty on Functioning of the European Union. (TFEU), including breaches of European Union 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;

6) acts or conduct which undermine the object or purpose of the provisions of EU legal acts in sections 3), 4) and 5);

**○ Retaliation:** any conduct, act or omission, even solely attempted or threatened, which occurs as a result of the Disclosure, complaints lodged to the Judicial or Accounting Authority or public disclosure and which causes or is likely to cause unjust damage to the Whistleblower or to the Person who lodged the complaint directly or indirectly. The following are examples of retaliation actions:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- the suspension of training or any restriction on access to the same;
- a negative performance assessment or employment reference;
- the adoption of any disciplinary measures, other penalties, including financial penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- failure to convert a temporary employment contract into a permanent contract, where the worker had legitimate expectations of being offered a permanent contract;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation, particularly on *social media*, or adverse economic or financial effects, including loss of business opportunities and loss of income;
- 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;
- early termination or cancellation of a supply contract for goods or services;
- cancellation of a licence or permit;
- request for psychiatric or medical referrals;

**○ Company: Abra Beta S.p.A.**

### **3. Recipients and scope of application.**

This procedure is applicable, in particular, to all Company Stakeholders including all related, affiliated and subsidiary enterprises of the same, i.e.:

- a) Partners and Shareholders;
- b) Board of Directors;
- c) Directors;
- d) Auditors/Independent audit firm;
- e) Board of Statutory Auditors/Statutory Auditor;
- f) Supervisory Body;
- g) Private sector employees.

These are workers with part-time, intermittent, open-end, fixed term, agency, apprenticeship, ancillary work contracts, or those providing one-off services;

- h) those who, despite not falling within the category of Employees, still work for the Company and/or work under the control and management of the Company (for example: self-employed persons, including those referred to in Chapter I of Law 81/2017, as well as those operating under collaboration-based relationships pursuant to art. 409 of the Code of Civil Procedure and art. 2 of Leg. Decree no. 81/2015, those who work with private sector entities, workers or collaborators who work with private sector entities providing goods or services or work for third parties, volunteers and paid and unpaid trainees);
- i) those who, although they are outside the Company, work directly and indirectly for the Company, or with the Company (e.g. consultants and professional freelancers);
- j) any other entity that has relations with the Company for the purpose the Whistleblowing disclosures;
- k) financial promoters, interns, contract/project workers, temporary workers;
- l) facilitators, meaning those who assist the Whistleblower in the Whistleblowing process, operating within the same work context and whose assistance must be kept confidential;
- m) individuals operating in the same work context as the Whistleblower, those who lodged a complaint to the Judicial and Accounting Authorities, or those who made a public disclosure and have a stable emotional bond or a kinship relationship up to the fourth degree;
- n) work colleagues of the Whistleblower or those who submitted a disclosure to the Judicial Authorities or made a public disclosure, those who operate in the same work context as the same and have a habitual and ongoing relationship with that person;
- o) entities owned - exclusively or jointly with third parties - by the Whistleblower or the person who has lodged a complaint with the Judicial Authority or has made a public disclosure or for whom the same persons work, as well as entities operating in the same work context as those persons.

The protection of Whistleblowers also applies when the Disclosure, the complaint lodged with the Judicial and Accounting Authorities or the public disclosure of information occurs as follows:

- when the juridical work relationship has not yet commenced, if the information on the breaches were acquired during the contract tender process or other pre-contract phases;
- during a trial period;
- after the termination of the relationship if the information was acquired during the course of said relationship.

#### **4. Subject matter of the Disclosure.**

Disclosures pursuant to Leg. Decree no. 24/2023 refer to circumstantial information related to:

- conduct, acts or omissions which harm public interest or the integrity of public administration or private entities, as indicated in § 2 (see definition of Breaches);
- any other breaches of any laws, regulations, policies, regulations or company procedures as illustrated in § 2 (see definition of Breaches).

**Whistleblowing Disclosures are not applicable to:**

- situations of a strictly personal nature, i.e. complaints, disputes or personal requests of the Whistleblower or those who lodged a complaint with the Judicial Authority and refer exclusively to individual employment relationships, as well as those relating to the employment relationships with higher-ranking persons. This excludes, by way of example and not limited to: disclosure concerning employment disputes, discrimination between colleagues, interpersonal conflicts between the Whistleblower and another worker;
- breaches already subjected to the mandatory European Union or national acts listed in Part II, annexed to Leg. Decree no. 24/2023, or by national regulations transposing the European Union acts listed in Part II, annexed to Directive (EU) 2019/1937, even those not listed in the Annex to Leg. Decree no. 23/2024;
- breaches of issues of national security, as well as procurement tenders related to national defence and security aspects, except when these aspects fall within the scope of European Union law.

The above also applies to the hypothesis of complaints and public dissemination.

## 5. Content of the Disclosure.

Disclosures shall be lodged in **good faith** to protect the integrity of the Company and shall be **based on precise facts** (which cannot be interpreted in a different manner) **and consistent elements** (various evidence pointing in the same direction), of which the Whistleblowers have become aware of whilst performing their duties and/or pursuant to their relationship with the Company.

The Whistleblower must provide all the necessary elements to allow the assigned parties to conduct the appropriate investigations and assessments to confirm the validity of the disclosed alleged wrongdoings.

To this end, the Whistleblower disclosure shall contain the following elements:

1. the identity details of the Whistleblower (name, surname, place and date of birth), as well as contact details for the notification of any subsequent updates;
2. an open and complete description of the facts raised in the Disclosure;
3. the circumstances in terms of the time and place in which the Disclosed event occurred;
4. the events leading to the reason that the subject of the Disclosure occurred;
5. any general information or other elements that make it possible to identify the subject(s) who allegedly carried out the disclosed wrongdoings, if such information is available;
6. information on any other individuals who can provide evidence on the disclosed wrongdoings;
7. attachment/indication of any documentation that can confirm the disclosed wrongdoings;
8. any other information that can provide useful feedback on the existence of the disclosed wrongdoings
9. clear indication that the Whistleblower wants to keep his/her identity confidential and take advantage of the safeguards put in place to provide protection against retaliation.

## 6. Disclosure Recipients.

The Disclosures can be submitted via the internal and external reporting channel according to the regulatory conditions envisaged by Leg. Decree no. 24/2023.

The management of the Company's internal reporting channel is appointed to the **Recipient, an independent external entity specifically trained** to manage the channel, with a budget to cover the assessment activities and the possibility of involving other entities, inside or outside the Company, that may be required in order to manage the Whistleblowing Disclosure.

## 7. Disclosure submission procedure.

### ○ Internal disclosures.

Disclosures can be submitted **in written or verbal forms** using the following channels:

i) **dedicated platform** called '*Whistleblowing Disclosures*', directly accessible from the Company's website or at the following address <https://whistleblowing.abrabeta.it> (also Platform), **installed and managed by an independent, external specialised entity**.

When accessing the platform, the user can select, **by encrypted communication**:

- a **written disclosure**, filling in a questionnaire, which facilitates the collection of information and with the possibility of attaching annex documents to the Disclosure;
- a **verbal disclosure**, by recording a voice message, pressing the microphone button to start and the stop button to finish, with automatic saving of the *files*.

Access to the Platform **does not require any identification process**: after submitting the Disclosure, the Whistleblower will receive a unique personal code for each Disclosure (so-called *Key Code*), which is required to receive updates on the Disclosure and add any further information. The *Key Code* is not available to the Company and must be kept by the Whistleblower;

or, alternatively

ii) registered letter with advice of receipt or standard mail in a sealed envelope addressed to the Recipient, Atty. Matteo Alessandro Pagani, Via Turati n. 26, 20121, Milan (MI), **with the following wording on the outside of the envelope and in the subject of the letter, '*Strictly Confidential – Whistleblowing Disclosure*'**.

The Disclosure must be placed in two closed envelopes: the first with the Whistleblower's identification details together with a photocopy of an identification document; the second with the Disclosure, so as to separate the Whistleblower's identification details from the actual Whistleblowing Disclosure. Both envelopes should then be placed in a third sealed envelope with the wording '*Strictly Confidential – Whistleblowing Disclosure*' on the outside.

Whichever channel is selected, Whistleblowers can request a meeting with the designated Recipient.



In the event that the Disclosure Recipient is in a position of conflict of interest in relation to a specific Disclosure (e.g. if the same is the Whistleblower or a Reported Person), ANAC deems it necessary that one of the conditions for issuing an external report is met.

The **internal channel** allows Whistleblowers to submit a communication which can put them in contact with the Recipient (and vice versa), guaranteeing the strictest confidentiality of the Whistleblower (and the subjects indicated in art. 4, paragraph 1, Leg. Decree n

o. 24/2023), regarding the content of the Disclosure Report and the annexes, both in relation to third parties and the system administrators.

In any case, the confidentiality of the relationship and communications between the Whistleblower and the Recipient is guaranteed at all times.

All Whistleblower Disclosures received by a person other than the Recipient must be sent to the latter within 7 days of receipt, notifying the Whistleblower of the transmission details, while respecting all confidentiality requirements (for example, if a closed envelope is received indicating that it is a *Whistleblowing Disclosure*, the person receiving it must send it to the Recipient without opening it).

#### ○ External disclosure.

External disclosures can only be submitted in one of the following conditions:

i) the work context does not envisage the mandatory activation of an internal Reporting channel or this, despite being mandatory, is not enabled and therefore fails to conform with the requirements of Leg. Decree no. 24/2023; ii) the Whistleblower has already submitted an internal Disclosure but has not received any feedback; (iii) the Whistleblower has reasonable grounds to believe that if he/she should submit an Internal Disclosure to the same, it would not be followed up, or that the Disclosure itself might give rise to retaliation risks; (iv) the Whistleblower has reasonable grounds to believe that the infringement could constitute an imminent or obvious danger to the public interest.

Disclosures can be addressed to ANAC via an external Reporting channel, either in written form – via an IT platform available on the ANAC website – or in verbal form via telephone, voice messaging systems or, at the request of the Whistleblower, in a face-to-face meeting.

The External report submitted to entities other than ANAC shall be sent, within 7 days of receipt, to the relevant entity, simultaneously notifying details on the transmission to the Whistleblower.

#### ○ Public disclosure

The Whistleblower can also disseminate a public disclosure by printed means, electronic means or, in any case dissemination means which are capable of reaching a large number of persons.

In this case, the Whistleblower can benefit from the protection envisaged by Leg. Decree no. 24/2023 if, at the time of public disclosure, one of the following conditions is applicable:

a) the Whistleblower has already submitted an internal Disclosure and, subsequently, an external Disclosure, via the internal disclosure channel, or the external disclosure channel without any feedback

within the terms envisaged by Leg. Decree no. 24/2023, in terms of the measures put in place or adopted to manage the reported Disclosures;

- b) The Whistleblower has already submitted an external Disclosure via the external disclosure channel without any feedback within the terms envisaged by Leg. Decree no. 24/2023;
- c) The Whistleblower has reasonable grounds to believe that the infringement could constitute an imminent or obvious danger to the public interest.
- d) The Whistleblower has reasonable grounds to believe that external Disclosure may involve a risk of retaliation or may not have been followed up effectively e.g. due to the specific circumstances of the case in question, such as those where evidence may be concealed or destroyed, or where there are reasonable grounds for believing that the person who received the report may be in collusion with or involved with the alleged wrongdoer, or is involved with the breach itself.

#### ○ Complaint.

The Whistleblower may consider contacting the Judicial or Accounting Authorities, by lodging a complaint regarding the unlawful conduct which he/she has become aware of within the employment context.

### 8. Internal Disclosure Management.

As part of the management of the **internal disclosure channel**, the Disclosure Recipient shall issue to the Whistleblower an advice of Disclosure receipt within 7 days from the date of receipt of the same and proceed with the **eligibility and admissibility assessment** of the same.

As regards to eligibility, the Recipient verifies the subsistence of the subjective and objective aspects and, more specifically that the Whistleblower is duly entitled to submit the Disclosure and that the subject matter of the Disclosure falls within the scope of the regulations.

Once the eligibility of the Disclosure has been validated, the Recipient then continues with the admissibility assessment. In particular, a check is carried out to ensure it contains all the elements indicated in § 5 of this procedure.

If such information is not provided, the Disclosure can be deemed inadmissible due to:

- lack of data constituting essential elements of the Disclosure;
- manifest unfounded evidence of the elements related to the type-based breaches by the legislator;
- presentation of facts of general content which do not allow the relevant departments or designated person to understand them;
- production of documentation without an actual Disclosure reporting the violations.

If the Disclosure is found to be impracticable and/or inadmissible, the Recipient shall file the Disclosure while ensuring traceability of the underlying reasons.

If, on the other hand, the conditions for eligibility and admissibility of the Disclosure are met, the Recipient shall start the **internal investigation to assess the validity of the reported facts and conduct**, in accordance with the principles of objectivity, competence and professional diligence, and shall carry out the following activities:

(i) maintain contact with the Whistleblower and request additional clarifications, documents and information from the latter as and where necessary; (ii) listen to the Whistleblower and/or the persons mentioned in the Disclosure; (iii) acquires Company records and documents; (iv) has the possibility to involve other business functions, to which the duty of confidentiality clause is extended and where breach of conduct may give rise to disciplinary action; (v) may use specialised external entities (e.g. IT expert), with an extension of the confidentiality obligations.

The Recipient shall provide feedback to the Whistleblower three months from the notice of receipt or, if no such notice is envisaged, three months from the expiry of the seven-day period from the date of presentation of the Disclosure. Since more time may be required to verify certain Disclosures, at the time of expiry, the Recipient may report the following to the Whistleblower:

- the archiving of the Whistleblower Disclosure (for instance, if it turns out to be an irrelevant Disclosure);
- the verification of the validity of the Disclosure and its transmission to the Company, more specifically, to the competent Corporate Bodies;
- the activity carried out so far and/or the activity to be carried out in the future. In this case, the Recipient will also inform the Whistleblower of the subsequent final outcome of the investigation (i.e. filing or verification of the validity of the Disclosure and transmission to the Company).

In the event that the Disclosure is deemed valid, the Recipient shall inform the Whistleblower and, at the same time, provide similar information to the alleged Perpetrator in an autonomous and confidential manner.

Where the investigations carried out reveal situations of serious infringements or where there is a reasonable suspicion that a criminal offence has been committed, the Recipient shall immediately notify the Whistleblower and send its assessment to the **Board of Directors**; and at the first possible meeting, to the other external and independent Supervisory bodies.

In the event that the Disclosure is deemed valid, the Company will take the necessary steps to resolve the breach definitively and take any disciplinary action it deems appropriate and necessary with respect to the personnel involved (by way of example only: disciplinary action against an employee and/or collaborator; action against Directors and Mayors; complaint to the Judicial Authority).

In the event that the Disclosure reports a level of severity that requires urgent action, the Recipient will inform the **Chair of the Board of Directors**, who will subsequently inform the Board of Directors. Moreover, the Recipient may consider reporting the event to the Judicial Authority.

To conclude, it should be noted that **in the case where anonymous Disclosure reports are received, the Recipient shall register them, and archive them in a manner which makes it easy to trace them if the Whistleblower, or the person who lodged the complaint, notifies ANAC with a complaint regarding acts of retaliation suffered because of the anonymous Disclosure or complaint.**

## **9. Protection measures.**

### **9.1. Confidentiality obligations regarding Whistleblower identities.**

Except in cases which contemplate a responsibility pursuant to acts of slander and defamation have been committed, under the provisions of the Code of Civil Procedure or art. 2043 of the Italian Civil Code, and those situations where anonymity is not enforceable by law (e.g. criminal, tax or administrative investigations, supervisory body audits), the identity of the Whistleblower is protected in any context subsequent to the Disclosure. Therefore, except for the express situations above, the identity of the Whistleblowers and any other information disclosed without their express consent and all those who receive or are involved in the management of the Disclosures are required to protect the confidentiality of such information.

Likewise, the content of the Disclosure and its documentation shall always be kept strictly confidential.

As for, more specifically, the context of the disciplinary proceedings against the alleged perpetrator, if the disclosed wrongdoings are, in whole or in part, confirmed and knowledge of the identity of the Whistleblower is absolutely essential to the defence counsel of the accused, the identity of the Whistleblower can only be revealed to the disciplinary authority and to the accused perpetrator of such misconduct in cases with the following conditions:

- the sending of a written notice to the Whistleblower with clarification as to the reasons of the disclosure of identity relevant confidential data.
- the Whistleblower has granted his/her express consent.

The Person concerned can be heard or, at his or her express request, also be heard by means of a cartulary procedure, through the acquisition of written observations and documents.

### **9.2. Confidentiality obligations regarding the identity of those other than the Whistleblower.**

With the same safeguards as those envisaged for the Whistleblowers, the identity of the following entities shall also be protected:

- Facilitators, meaning those who assist the Whistleblower in the Whistleblower process, operating within the same work context and whose assistance must be kept confidential;
- individuals operating in the same work context as the Whistleblower, those who lodged a complaint to the Judicial and Accounting Authorities, or those who made a public disclosure and have a stable emotional bond or a kinship relationship up to the fourth degree;
- work colleagues of the Whistleblower or those who lodged a complaint to the Judicial Authorities or made a public disclosure, those who operate in the same work context as the same and have a habitual and ongoing relationship with that person;
- entities owned - exclusively or jointly with third parties - by the Whistleblower or the person who lodged a complaint with the Judicial Authority or has made a public disclosure or for whom the same persons work, as well as entities operating in the same work context as those persons.

All subjects who receive or are involved in the management of Disclosures are, therefore, retained to safeguard the confidentiality of the aforementioned information.

### **9.3. Processing of Personal Data.**

The processing of personal data shall be carried out in accordance with the GDPR regulation.

Personal data which are manifestly irrelevant for the processing of a specific Disclosure shall not be collected or, if collected accidentally, shall be deleted without undue delay.

The processing of personal data is carried out by the Controller, providing appropriate information to Whistleblowers and the persons involved pursuant to art. 13 and 14 of the GDPR.

The Recipient - by means of its members if collegiate - shall process the data as an "Authorised" entity pursuant to and by the combined effect of art. 29 of GDPR and art. 2 *quaterdecies* of Leg. Decree no. 196/2003 as amended (also *Privacy Code*). Therefore, the Recipient shall receive appointments and specific operating instructions on such data processing.

Pursuant to art. 2 *undecies*, par. 1 lett. (f) of the *Privacy Code* the rights referred to in arts. 15 to 22 of the GDPR may be restricted or may not be exercised with a request submitted to the Data Controller, if the performance of their work activities can cause an actual compromise to the confidentiality of the identity of the Whistleblower who reports the same pursuant to Leg. Decree no. 24/2023, the wrongdoing that came to his/her knowledge during the course of their duties.

Based on a Data Protection Impact Assessment (DPIA), the Company guarantees appropriate technical and organisational measures to ensure a level of security suitable in relation to the specific risks arising from the processing operations carried out, and regulating the relationship in the event of the involvement of external suppliers.

### **9.4. Prohibition of retaliation.**

The Company does not tolerate, even if solely attempted or threatened – in the broadest sense indicated in § 2 – any form of retaliation against the Whistleblower or anyone who has collaborated in the Disclosure verification activities, pursuant to art. 17 of Leg. Decree no. 24/2023. It remains understood that any disciplinary action which may have been undertaken with a retaliatory purpose shall be deemed null and void.

The protection measures pursuant to Leg. Decree no. 24/2023 apply also to:

- the Facilitators;
- individuals operating in the same work context as the Whistleblower, those who lodged a complaint to the Judicial and Accounting Authorities, or those who made a public disclosure and have a stable emotional bond or a kinship relationship up to the fourth degree;

- work colleagues of the Whistleblower or those who lodged a complaint to the Judicial Authorities or made a public disclosure, those who operate in the same work context as the same and have a habitual and ongoing relationship with that person;
- entities owned by the Whistleblower or the person who lodged a complaint with the Judicial Authority or has made a public disclosure or for whom the same persons work, as well as entities operating in the same work context as those persons,

where the following conditions subsist:

- a) at the time of the Disclosure or the complaint to the Judicial or Accounting Authorities or public disclosure, the Whistleblower (or complainant) had reasonable grounds to believe that the information on the indicated breaches, of public disclosure or reported are true and fall within the scope of Leg. Decree no. 24/2023 (i.e. breaches of national or EU standards and regulations that constitute a danger to the public interest or the integrity of the Public Administration or the Company, they became aware of within the work context);
- b) the Disclosure or public disclosure has been carried out in accordance with the provisions of Leg. Decree no. 24/2023 in relation to the reporting channels and public disclosure.

Protection under Leg. Decree no. 24/2023 is not guaranteed - and disciplinary sanctions are applicable to the Whistleblower or complainant - when the Whistleblower is charged or convicted in first degree for libel, defamation, other crimes committed and reported to the Judicial or Accounting Authorities, or its civil responsibilities for the same form of conduct, in cases of wilful misconduct or gross negligence, unless the responsibility restrictions envisaged by art. 20 Leg. Decree no. 24/2023.

#### **9.5. Protection against retaliation.**

The Whistleblowers and the entities indicated in § 9.4. of this procedure can report any retaliation they believe they have suffered, even only attempted or threatened, to ANAC, via its own IT platform.

ANAC informs the National Labour Inspectorate of the measures within its competence and, in order to acquire essential elements when assessing acts of retaliation, even if only attempted or threatened, it can use the Civil Service Inspectorate and the National Labour Inspectorate.

The procedure conducted by ANAC is completed with the adoption of a dismissal order or, where acts of retaliation are established, even if only attempted or threatened, with a disciplinary fine (from € 10.000 to € 50,000), against the person responsible for the same.

Whistleblowers who have been dismissed because of the Whistleblower disclosure, public dissemination or complaint to the Judicial or Accounting Authority are entitled to be reinstated to their previous job, pursuant to art. 18 of Law 300/1970 and art. 2 of Leg. Decree no. 23/2015.

## **10. Responsibilities of the Whistleblower.**

It is the responsibility of Whistleblowers to submit Disclosures in good faith in line with the spirit on which this regulation is based. This procedure in the event of slanderous or defamatory disclosures under the Criminal Code and art. 2043 of the Italian Civil Code, does not relieve the criminal, and disciplinary responsibility of the Whistleblower pursuant to cases of wilful misconduct or gross negligence.

Any form of abuse of the Whistleblowing Procedure, such as disclosures that are manifestly opportunistic and/or submitted with the sole purpose of harming the complained or other persons, shall also give rise to liability in disciplinary proceedings and in other competent jurisdictions, and any other hypothesis of misuse or intentional exploitation of the institution subject to this procedure.

Whistleblowers on the other hand are not punishable if they reveal or disseminate:

- information on breaches covered by confidentiality obligations other than that indicated in art. 1, par. 3, Leg. Decree no. 24/2023, i.e.: classified information; professional forensic and medical secrecy; secrecy of judicial and court deliberations;
- information concerning breach of copyrights;
- information concerning breaches related to the protection of personal data;
- information concerning breaches that offend the reputation of the person involved or reported when the following conditions are met:
  - a) there were reasonable grounds, at the time of disclosure or dissemination of the information, to believe that the information is necessary to disclose the infringement;
  - b) the Disclosure (i.e. public dissemination or complaint) was submitted according to the requirements of Leg. Decree no. 24/2023.

Therefore, the above-mentioned limitation operates where the reasons for the disclosure or dissemination are not based on mere allegations, gossip, or vengeful, opportunistic or sensational purposes.

In any case this does exclude liabilities for conduct that:

- is not linked to the Whistleblowing disclosure;
- are not strictly necessary in order to reveal the breach;
- constitute the unlawful acquisition of information or access to documents.

Where the acquisition constitutes a criminal offence (for example, unlawful access to a computer system), criminal liability and all other civil, administrative and disciplinary liabilities shall remain applicable, while the extraction of documents to which they had legitimate access shall not be punishable.

#### **11. Documentation archiving procedures.**

The Recipient is required to document, with the retention of electronic and/or hard copy documents, the Disclosures received, in order to ensure full traceability of the interventions carried out so as to fulfil their institutional functions.

Documents in electronic format shall be stored in a computer file protected by authentication credentials and only known to the Recipient and to all persons expressly authorised by the Recipient.

In the case of disclosures made clearly in bad faith, the Recipient reserves the right to file them after deleting the names and other elements that may allow identification of the alleged perpetrators.

Hard copies of the documents shall be retained in an archive which shall only be accessible to the Recipient and to persons expressly authorised by the same.

Such data are retained by the Recipient for the time strictly necessary for process the Disclosure and, in any case, for no longer than 5 years from the date of communication of the final outcome of the Whistleblowing procedure.

Further instructions or reference to other documents may be added to this procedure during the application phase.

#### **12. Waivers and transactions.**

Waivers and transactions, complete or partial, concerning the rights and means of protection envisaged by Leg. Decree no. 24/23, are prohibited, unless they are carried out pursuant to art. 2113, par. IV of the Italian Civil Code, i.e. in protected judicial, administrative and financial environments.

#### **13. Dissemination.**

This procedure shall be posted on the Company's website, on the Employee noticeboard and circulated via email/company portal. It is mandatory for all employees to read it immediately.

For subjects who do not fall within the scope of the category referred to in the previous sub-paragraph, the Whistleblower process will be posted to a dedicated area on the corporate website.

#### **14. Penalties.**

In addition to the penalties expressly provided for in Leg. Decree no. 24/2023, any further infringement shall be prosecuted in accordance with the CCNL (National Collective Bargaining Agreement) applied to the persons responsible for the infringement.