WHISTLEBLOWING PROCEDURE

INDEX

1 FOREWORD 3
2 DEFINITIONS 4
3 SCOPE 5
3.1 PERSONAL SCOPE OF REPORTING 5
3.2 MATERIAL SCOPE OF REPORTING 7
3.3 REPORTING CONTENT EXCLUDED FROM THE APPLICATION OF THE WHISTLEBLOWING PROVISIONS 8
4 REPORTING CHANNELS 9
4.1 INTERNAL REPORTING CHANNELS AND THE INTERNAL REPORTING COMMITTEE. 9
4.2 EXTERNAL REPORTING CHANNELS 11
4.3 PUBLIC DISCLOSURE 11
5 SUBMITTING THE REPORT 13
6 ACKNOWLEDGEMENT OF RECEIPT AND TIMING AND COMMUNICATION TO THE INTERESTED PARTIES 13
7 THE INVESTIGATION 14
8 COOPERATION IN INVESTIGATIONS 14
9 PROTECTION MEASURES FOR THE WHISTLEBLOWER 14
10 PENALTIES 16
11 TRAINING 16
12 DATA PROTECTION AND RECORD KEEPING 17
13 DATA MANAGEMENT AND PRIVACY 17

1 FOREWORD

Whistleblowing is the act of reporting suspected wrongdoing or the risk of wrongdoing. Studies and experience show that a large proportion of wrongdoing is brought to the attention of the organisation concerned through reports from people within or close to the organisation.

For these reasons, organisations are increasingly considering introducing or improving whistleblowing policies and processes, whether in response to regulation or on a voluntary basis.

With the European Directive 2019/1937 on the protection of persons who report breaches of Union law, the European Union wanted to create a minimum standard for the protection of whistleblower rights in all Member States. Italy stepped in and implemented the European Directive with Legislative Decree no. 24 of 10 March 2023.

Orton s.r.l. (hereinafter also referred to as the "**Company**" or "**Orton**") intends to comply with the above legal requirements as described in this Procedure.

This Procedure provides the information necessary to ensure that the internal mechanism adopted by the Company to report actual or suspected wrongdoing or irregularities within the Company is accessible to all those covered by the legislation.

The whistleblowing management system adopted by Orton s.r.l. aims to achieve the following outcomes:

- encouraging and facilitating reporting of wrongdoing, demonstrating the commitment of corporate leadership to preventing and addressing it;
- supporting and protecting whistleblowers and other interested parties involved by encouraging people to come forward promptly;
- ensuring reports of wrongdoing are dealt with in a proper and timely manner, by reducing and preventing any prejudicial treatment;
- improving governance by encouraging a culture of openness, transparency, integrity and accountability;
- reducing the risks of wrongdoing.

This leads to the realisation of many benefits for the Company, including:

- allowing to identify and address wrongdoing at the earliest opportunity;
- helping prevent or minimise the loss of assets and aiding recovery of lost assets;
- ensuring compliance with Orton's policies, procedures and legal and social obligations;
- attracting and retaining personnel committed to Orton’s values and culture;

- demonstrating sound and ethical governance practices to markets, regulators and other interested parties.

This Procedure has been written in order to implement the following sources of legislation:

- EU Directive 2019/1937 (Whistleblowing Directive);
- Legislative Decree No. 24 of 10 March 2023, implementing (EU) Directive 2019/1937.

2 DEFINITIONS

For the purposes of this Procedure, the following definitions apply:

a) «**breaches**»: conduct, acts or omissions that harm the public interest or the integrity of the Company, as further specified in section 3.2 "Objective scope of reporting".
b) «**information on breaches**» means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the Company, as well as information about attempts to conceal such breaches;
c) «**reporting**» or «**report**» means the oral or written communication of information on breaches;
d) «**internal reporting**» means the oral or written communication of information on breaches, submitted through the internal reporting channel;
e) «**external reporting**» means the oral or written communication of information on breaches, submitted through the external reporting channel;
f) «**public disclosure**» or «**to publicly disclose**» means the making of information on breaches available in the public domain through the press or electronic media or otherwise through means of disclosure capable of reaching a large number of people;
g) «**reporting person/whistleblower**»: means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities
h) «**facilitator**»: means a natural person who assists[1] a reporting person in the reporting process in the same work-related context, and whose assistance should be confidential;
i) «**work-related context**» means current or past work activities carried out in the context of the relationships described in paragraph 3.1 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 to judicial authorities, regulatory or supervisory bodies;
j) «**person concerned**» means a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated;

[1] By using the term 'assistance', the Regulation refers to a person who provides advice and assistance to the whistleblower.

k) «**retaliation**» means any direct or indirect act or omission[2], including any attempts or threats, which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person;
l) «**follow-up**» means any action taken by the recipient of a report, to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry or an investigation;
m) «**feedback**» means the provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up

3 SCOPE

Reports must relate to conduct, acts or omissions of which the reporting person or whistleblower has become aware in the course of his or her work. Therefore, it is important that a qualifying relationship exists between the whistleblower and the Company that relates to current or past work or professional activities.

3.1 PERSONAL SCOPE OF REPORTING

Legislative Decree No. 24 of 10 March 2023 defines the personal scope of the regulation. In particular, the following person can make a report and will be protected from retaliation:

1) **Persons having the status of worker,** including:
   - workers whose employment status is governed by Legislative Decree No. 81/2015. These are, for example, part-time, job-on-call, fixed-term, temporary, staff leasing, apprenticeship and ancillary employment relationships.
   - employees providing services on an occasional basis[3]
2) **Persons having self-employed status** working for the Company, including:

[2] Examples include dismissal, suspension or equivalent; downgrading or non-promotion; change of duties, change of job, reduction in pay, change of working hours; suspension of training or any restriction on access to it; negative performance appraisal or negative reference; the imposition of disciplinary measures or any other sanction, including a fine; coercion, intimidation or harassment; discrimination or other unfavourable treatment; failure to convert a fixed-term contract into an open-ended contract; coercion, intimidation, harassment or ostracism; discrimination or other unfavourable treatment; 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, in particular on social media, or economic or financial loss, including loss of economic opportunities and loss of income; inclusion on inappropriate lists on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future; early termination or cancellation of a contract for the supply of goods or services; cancellation of a licence or permit; a requirement to undergo psychiatric or medical examinations.

[3] The employment relationship is governed by Article 54-bis of Decree-Law No. 50/2017, converted into law, with amendments, by Law No. 96/2017.

- self-employed workers indicated in Chapter I of Law No. 81/2017. This includes, for example, self-employed persons exercising intellectual professions for which registration in special registers or lists is required, such as architects, surveyors, etc.
- holders of a collaboration relationship referred to in Article 409 No. 3 of the Code of Civil Procedure. That is, agency, commercial representation and other collaborative relationships resulting in the provision of continuous and coordinated work, mainly personal, even if not of a subordinate nature. For example, lawyers, engineers who provide their work for the Company by organising it autonomously (para-subordinate relationship).
- holders of a collaboration relationship referred to in Article 2 of Legislative Decree No. 81/2015. These are - pursuant to para. 1 of the aforementioned provision - collaborations organised by the principal that take the form of exclusively personal and continuous work services, the manner of performance of which is organised by the principal also with reference to "the time and place of work" (so-called "hetero-organisation").

3) **Freelancers and consultants** working for the Company;
4) **Paid and unpaid interns or trainees** working for the Company;
5) **Any persons working under the supervision and direction of contractors, subcontractors and suppliers**, i.e. workers or collaborators, who work for public or private sector entities providing goods or services or carrying out works for the Company;
6) **Persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members**, even if these functions are exercised on a de facto basis[4] .

The protection afforded to such persons also extends to persons other than the whistleblower who may be subject to retaliation, even indirectly, because of their role in the reporting, disclosure or whistleblowing process and/or the particular relationship linking them to the whistleblower or reporting person. Such persons include:

- **The facilitator**: For example, the facilitator could be a colleague from a different office from the whistleblower's, who assists the whistleblower in the whistleblowing process on a confidential basis, i.e. without disclosing the information obtained. The facilitator could be a colleague who is also a trade unionist, if he or she assists the whistleblower in his or her name and on his or her behalf, without revealing the trade union acronym.[5] .

[4] These are persons who are closely associated with the Company and in which they exercise certain functions, even in the absence of a regular investiture (de facto exercise of functions). They may, for example, be members of the Board of Directors, even if they do not hold an executive position, or members of Supervisory Bodies.

[5] It should be noted that, on the other hand, if he assists the whistleblower through the use of the trade union acronym, he does not have the role of an intermediary. In this case, the provisions on the consultation of trade union representatives and on the repression of anti-union behaviour, as set out in Law No. 300/1970, continue to apply. Bearing in mind that the legislator's aim is to expose unlawful acts by guaranteeing, among other things, the whistleblower's freedom of expression, including with the help of others, it follows that the facilitator must also be guaranteed protection in terms of confidentiality. This concerns both the identity of the informant and the activity in which the assistance takes place. This need for protection can be deduced from the wording of the

- **Persons in the same work-related context [6] who are related to them by a stable affective bond[7] or kinship up to the fourth degree**. The term "persons in the same work-related context as the whistleblower" refers to persons who are linked by a network of relationships arising from the fact that they work or have worked in the past in the same work-related context as the whistleblower or reporting person, e.g. colleagues, former colleagues, employees. A prerequisite for the application of protection in such cases is the existence of a stable emotional or kinship relationship with the whistleblower up to the fourth degree.
- **Work colleagues with a usual and current relationship with the reporting person**. In the case of work colleagues, however, the legislator has provided that they should be those who work with the whistleblower at the time of the report. However, for the protection to apply, this requirement must be accompanied by a "usual and current" relationship with the whistleblower. The regulation therefore refers to relationships which are not merely sporadic, occasional, episodic and exceptional, but which are present, systematic and prolonged over time, characterised by a certain continuity such as to establish a relationship of "commonality", of friendship between the parties. In such cases, therefore, one refers only to activities carried out in the present and not also to those of the past.
- **Entities owned[8] by the reporting person or making a public disclosure or for which such persons work as well as entities operating in the same work-related context [9] as such persons.**. In fact, retaliation may also be taken against legal entities that the whistleblower owns, works for or is otherwise associated with in a work-related context. This includes, for example, withdrawing services from, blacklisting or boycotting such a person.

3.2 MATERIAL SCOPE OF REPORTING

In order to outline the material scope that can be reported through the whistleblowing channel, reference is made to Article 1 of Legislative Decree No. 24 of 10 March 2023.

The material scope of reporting relates to:

provision, which expressly states that "assistance shall be confidential". On the other hand, the exclusion of such protection with regard to the intermediary could risk revealing the identity of the whistleblower who has sought the intermediary's assistance.

6 In fact, this concept includes past or present work or professional activities, regardless of the nature of such activities, through which a person acquires information about violations and in the context of which he or she could risk retaliation in the event of a public disclosure or a complaint to the judicial or accounting authorities.

7 It is considered that this expression could refer primarily to those who live together with the whistleblower. However, in line with the rationale of extending the protection against retaliation as far as possible, it is considered that the notion of stable affective bond can be understood not only as cohabitation in the strict sense, but also as a relationship of an affective nature characterised by a certain stability both in terms of time and in terms of shared life. An affective bond that therefore involves a specific person. Consider, for example, a colleague (or ex-colleague) of the reporting person who nevertheless maintains an affective relationship with him/her, even if this relationship does not take the form of actual sharing of the same dwelling.

8 It is considered that this concept can be understood in a broad sense, covering both cases where an entity is the sole owner of an undertaking and cases where it has a majority shareholding with third parties.

9 However, in such a case, a link, albeit indirect, with the reporting party can be established if these entities are part of the working environment of the reporting party. In fact, a dense network of relationships and interconnections may also develop between entities, resulting, for example, in business partnerships.

- **Breaches of national law:** This category includes criminal, civil, administrative or accounting offences that are not specifically identified as breaches of EU law. Such offences also include:
  - predicate offences for the application of Legislative Decree No. 231/2001;
  - violations[10] of the organisational and management models provided for in the aforementioned Legislative Decree No. 231/2001.
- **Breaches of European legislation**
  These are:
  - Offences in breach of the EU legislation listed in Annex 1 to Legislative Decree No. 24/2023 and any national provisions for its implementation. In particular, these offences relate to the following areas: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; protection of the environment; radiation protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; protection of privacy and personal data, and security of network and information systems;
  - Breaches affecting the financial interests of the European Union (Article 325 TFEU - fight against fraud and any other illegal activity affecting the financial interests of the EU), as defined in EU regulations, directives, decisions, recommendations and opinions. This includes, for example, fraud, corruption and any other illegal activity related to EU expenditure;
  - Breaches relating to the internal market that jeopardise the free movement of goods, persons, services and capital (Article 26(2) TFEU). This includes breaches of 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;
  - Acts or conduct which defeat the object or purpose of the provisions of the European Union in the areas referred to in the preceding points.

3.3 REPORTING CONTENT EXCLUDED FROM THE APPLICATION OF THE WHISTLEBLOWING PROVISIONS

In order to understand what the material scope of reporting may be, it is important to bear in mind that the legislator has specified what may not be the subject of reporting or public disclosure.

[10] It should be noted that these infringements do not constitute predicate offences for the application of Legislative Decree No. 231/2001 and relate to organisational aspects of the entity that adopts them.

These exclusions must therefore be given due consideration and can be summarised as follows:

- disputes, claims or requests relating to a personal interest of the reporting person or of the person making a complaint to the judicial or accounting authorities and relating exclusively to his or her individual employment relationship. Therefore, reports concerning, for example, labour disputes, discrimination between colleagues, interpersonal conflicts between the reporting person and another employee are excluded;
- reports of violations where they are already mandatorily regulated by European Union legislation and the implementing provisions of the Italian legal system, which already guarantee specific reporting procedures. Therefore, the reporting of such violations remains excluded from the scope of Legislative Decree No. 24/2013, as well as those provided for in other special regulations on whistleblowing in specific sectors, as mentioned above;
- reports of breaches of national security, as well as contracts relating to defence or national security aspects, unless such aspects are covered by the relevant secondary legislation of the European Union. On the contrary, Legislative Decree No. 24/2023 applies to contracts awarded in the fields of defence and security, with the exception of those expressly excluded by the above-mentioned regulations..

4 REPORTING CHANNELS

The Company, in consultation with trade union representatives or organisations, has established this Procedure for receiving and handling reports and has established and activated appropriate internal reporting channels.

4.1 INTERNAL REPORTING CHANNELS AND THE INTERNAL REPORTING COMMITTEE

The Company has established an autonomous reporting channel that guarantees the anonymity of reports.
The channel ensures that reports can be submitted in a variety of written, oral and multilingual forms. Through this channel, the report reaches the Internal Committee, which is responsible for the investigation and decision-making phase of the report.
It is also possible to make the report in person by making an appointment to meet with one or more members of the Committee authorised to handle whistleblowing reports.
The channels established by Orton for the submission of whistleblowing reports to the aforementioned Committee are accessible at http://www.imihotline.com and, in accordance with the provisions of Legislative Decree 24/2003:

- guarantee the confidentiality of the whistleblower, the intermediary, the person involved or, in any case, the persons mentioned in the report, the content of the report and the related documentation.
- allow for reporting:
  - in writing, also in computerised form through the Navex online platform, which allows the reporting person to choose between two different online reporting channels, the local one or that of the IMI Group holding company.
  - orally, through a telephone line activated on the online platform operated by NAVEX Global, Inc. ("Navex") or, alternatively, through voice messaging systems on the same platform.
  - or, at the request of the reporting person, in a face-to-face meeting with a member of the Committee, to be arranged within a reasonable time.

The whistleblower will be given the opportunity to make the report anonymous through the Navex platform. Anonymous reports received will be treated in the same way as other reports submitted without the whistleblower's anonymity.

The ad hoc Committee set up to receive and manage reports from potential whistleblowers has independent powers of initiative and control and is composed of the following three professionals:

- the Supervisory Board of Orton (Chairman of the Committee)
- the Divisional General Counsel IMI Critical Engineering.
- the Senior Legal and Compliance Counsel Italy IMI Critical Engineering.

The Committee, known as the "Whistleblowing Committee", acts with full autonomy and does not require prior authorisation to request documents, conduct interviews and/or carry out on-site inspections in connection with the investigation of reports received.
The Committee takes decisions by a majority of its members and reports directly to the Company's Board of Directors.
If a report concerns one of the members of the Whistleblowing Committee, the Navex platform will not automatically make the report available to that person.

Whistleblowers should use internal reporting channels to report potential wrongdoing in the first instance, provided that the reporting persons believe that the report of potential wrongdoing can be dealt with effectively within the relevant organisation and that there is no risk of retaliation.

If the internal report is made to someone other than the person designated and authorised by the Company, the report must be forwarded to the relevant person within seven days of receipt, with simultaneous notification to the reporting person.

4.2 EXTERNAL REPORTING CHANNELS

Notwithstanding the preference for the internal channel, as explained above, the Decree provides for the possibility of reporting through an external channel.

ANAC is the authority responsible for activating and managing this channel, which guarantees the confidentiality of the identity of the reporting person, of the person involved and of the person mentioned in the report, as well as the content of the report and the related documents, also by using encryption tools.

However, access to this channel is only permitted under certain conditions expressly laid down by law.
In particular, the whistleblower may make an external report if, at the time of making the report:

1. the internal channel, although mandatory, is not active or, even if active, does not comply with the provisions of the Decree regarding the subjects and methods of internal reporting, which must be able to guarantee the confidentiality of the identity of the reporter and other protected subjects.
2. the whistleblower has already reported internally and the designated person or office has not followed up. Reference is made to cases where the internal channel has been used but has not functioned properly, in the sense that the report has not been dealt with within a reasonable time or no action has been taken to remedy the breach.
3. the whistleblower has reasonable grounds to believe, on the basis of factual circumstances and information actually obtained and not on the basis of mere inferences, that, if he or she were to make an internal report, the following would occur:
   - reporting would not be effectively followed up. This may be the case, for example, if the person ultimately responsible in the work context is involved in the breach, if there is a risk that the breach or related evidence could be concealed or destroyed, if the effectiveness of investigations by the competent authorities could otherwise be compromised, or even if it is felt that ANAC would be better placed to deal with the specific breach, particularly in matters within its competence;
   - this could lead to the risk of retaliation.
4. the reporting person has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest. This may be the case, for example, where the breach requires urgent action to protect the health and safety of individuals or to protect the environment.

4.3 PUBLIC DISCLOSURE

Legislative Decree No. 24/2023 introduced an additional method of reporting, which is public disclosure.
Public disclosure involves the use of the press, electronic media or other means of dissemination capable of reaching a large number of people to make information about violations available to the public.
Public disclosure of breaches must be in accordance with the conditions laid down by the legislator in order for the person making the disclosure to then have the benefit of the protection afforded by the Regulation. Therefore, protection will be recognised if one of the following conditions is met at the time of disclosure:

1. an internal report to which the company has not replied within the prescribed time limit (three months from the date of acknowledgement of receipt or, failing that, within three months from the expiry of the seven-day period following the submission of the report) has been followed by an external report to ANAC which has not provided the reporting person with a reply within a reasonable time (three months or, in the case of justified and reasoned requests, six months from the date of the acknowledgement of receipt of the external report or, in the absence of such acknowledgement, from the expiry of the seven-day period following its receipt).
2. the person has already made an external report directly to ANAC, which has not responded to the person making the report within a reasonable period (three months or, for justified and substantiated reasons, six months from the date of receipt of the external report or, failing that, from the expiry of seven days from the date of receipt) on the measures planned or taken to follow up the report.
3. the person makes a public disclosure directly because he or she believes, on reasonable grounds based on the circumstances of the particular case, that the breach may pose an imminent or obvious danger to the public interest. For example, an emergency situation or the risk of irreversible harm, including to the physical safety of one or more persons, which requires that the breach be disclosed immediately and widely in order to prevent its effects.
4. the person directly makes a public disclosure because he or she believes, on the basis of reasonable grounds based on the circumstances of the specific case, that the external report may involve a risk of retaliation or may not be effectively followed up, for example, because he or she fears that evidence may be concealed or destroyed or that the recipient of the report may be in collusion with or involved in the breach. Consider, for example, the case where the recipient of a report of a breach, with the agreement of the person involved in the breach, dismisses the report without justification.

In the case of a public disclosure, where the person voluntarily discloses his or her identity, the protection of confidentiality does not apply, without prejudice to all the other forms of protection provided by the decree for whistleblowers. On the other hand, if the whistleblower discloses violations using, for example, a pseudonym or a nickname that does not allow the whistleblower to be identified, ANAC will treat the disclosure in the

same way as an anonymous report and will ensure that it is recorded in order to ensure that, in the event that the whistleblower's identity is subsequently revealed, the whistleblower will be protected in the event of retaliation.

5 SUBMITTING THE REPORT

It is necessary that the report be as circumstantial as possible to enable the function authorised to receive and process reports to consider the facts.
In particular, the report must clearly state:

- the circumstances of the time and place where the reported event occurred.
- the description of the fact.
- the personal details or other elements allowing the identification of the person to whom the reported facts may be attributed.

It is also useful to include documents that may provide evidence of the facts to be reported, as well as an indication of other persons who may be aware of the facts.

6 ACKNOWLEDGEMENT OF RECEIPT AND TIMING AND COMMUNICATION TO THE INTERESTED PARTIES

The Whistleblowing Committee:

- provide the whistleblower with an acknowledgement of receipt of the report within seven days of receipt.
- engage in dialogue with the whistleblower.
- follow up properly on reports received.
- provide the reporter with feedback on the outcome of the report within three months of the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within three months of the expiry of the seven-day period following the submission of the report.

Proper follow-up implies, first and foremost, an assessment of whether the essential requirements of the report are met, in order to assess its admissibility and thus to provide the reporter with the envisaged protection, while respecting reasonable time limits and data confidentiality.
Notification to the data subject, as understood above, may be delayed for as long as there is an objective risk that the ability to effectively investigate the matter or gather the necessary evidence may be compromised.

7 THE INVESTIGATION

After assessing the admissibility of the whistleblowing report, the Whistleblowing Committee will initiate the internal investigation of the reported facts or conduct to determine whether they exist.
Investigations will be completed as quickly as possible without compromising accuracy, quality or depth.

8 COOPERATION IN INVESTIGATIONS

All employees and outsiders working for Orton must cooperate with any investigation by providing all requested information and answering truthfully and completely all relevant questions during the investigation. Failure to cooperate with an investigation may be grounds for appropriate disciplinary action.

9 PROTECTION MEASURES FOR THE WHISTLEBLOWER

An important pillar of the whole discipline is the system of protection for whistleblowers, public disclosures and reporters, which - as already mentioned - also extends to persons other than the whistleblower and the reporter who, precisely because of their role in the reporting process and/or the special relationship between them and the reporter, may be subject to retaliation.

The protection of whistleblowers also applies if the whistleblowing, the report to judicial or accounting authorities or the public disclosure of information takes place in the following cases:

a) when the legal relationship has not yet commenced, if information on breaches has been obtained during the selection process or at other pre-contractual stages.
b) during the probationary period.
c) after the termination of the legal relationship, if the information on breaches was acquired in the course of that relationship.

The system of protection provided for by Legislative Decree No. 24/2023 consists of the following types of protection:

1. the confidentiality of the reporter, the facilitator, the person concerned and the persons mentioned in the report. The obligation to protect confidentiality requires that any disclosure of the identity of the whistleblower to persons other than those responsible for receiving or following up on the whistleblower's report should always be made with the explicit consent of the whistleblower. It is therefore essential that administrations and relevant bodies, in their capacity as data controllers, authorise all staff involved in the processing of personal data. As

mentioned above, the persons thus identified must receive adequate professional training, including on the applicable data protection rules, in order to handle the reports. It should also be clarified that the prohibition of disclosure of the identity of the whistleblower refers not only to the name of the whistleblower but also to any other information or element of the report, including any accompanying documents, from which the disclosure of the identity of the whistleblower could be directly or indirectly deduced.

2. protection from any retaliatory action taken by the Company as a result of the report.
3. limitations on liability in relation to the disclosure and dissemination of certain categories of information, which may apply in certain circumstances.
4. 4. the provision of support measures by third sector organisations included in a specific list published by ANAC.

There is a prohibition on any waiver or settlement of the rights and remedies provided by the Act that is not signed in the Protected Venue. As a result, waivers and settlements, whether in whole or in part (e.g. by agreement or other contractual terms), of the right to make reports, disclosures or complaints under the Act are void a priori.

Similarly, it is not permissible to require the whistleblower, or any other protected person, to deprive himself or herself of the possibility of accessing the means of protection to which he or she is entitled (protection of confidentiality, from any retaliation suffered as a result of the report, disclosure or whistleblowing made, or limitation of liability resulting from the report, disclosure or whistleblowing if the conditions are met). A fortiori, these protections cannot be voluntarily waived.

It should be noted, however, that the above does not apply to waivers and settlements signed in protected venues (judicial, trade union, administrative).

Indeed, the whistleblower and other protected persons may validly waive their rights and remedies or settle if this is done before a court, following a compulsory conciliation attempt or following mediation and conciliation agreements prepared by trade union organisations.

In these cases, the fact that such acts are carried out before bodies whose composition guarantees authority and impartiality allows the position of the person who resigns or settles to be considered more protected, also in terms of greater genuineness and spontaneity of consent.

Orton will treat any complaint, victimisation or harassment as a serious matter which may result in disciplinary action up to and including termination of employment.

If a reporting person suffers harm as a result of reporting potential wrongdoing, the burden of proof shifts to the person who took the harmful action, who should then be required to prove that the action taken was in no way related to the report.

Finally, it should be noted that in order to ensure compliance with the obligation of confidentiality, the Decree provides that ANAC will impose an administrative fine on Data Controllers in the event of a breach of this obligation.

10 PENALTIES

The Whistleblowing Committee may decide, on the basis of its findings at the end of the preliminary investigation, to file the report and forward the information to the Board of Directors in the case of clear and manifest unfoundedness and gross negligence or intentional misconduct on the part of the person making the report. The Board of Directors will consider the appropriateness of initiating disciplinary proceedings against the whistleblower within the Company.

The sanctions that may be imposed on those who have made manifestly unfounded reports with gross negligence or willful misconduct are those set out in the Collective Agreements:

- National Collective Bargaining Agreement for Metalworkers (Contratto Collettivo Nazionale di Lavoro Metalmeccanico)
- Industry Managers Collective Bargaining Agreement (Contratto Collettivo Dirigenti Industria)

Legislative Decree No. 24 of 10 March 2023 also requires companies that have implemented an organisational, management and control model pursuant to Legislative Decree no. 231/01 to ensure that the disciplinary sanctions provided for therein are also directed against those who are

a. responsible for retaliation, obstruction or attempted obstruction of reporting
b. responsible for failing to establish reporting channels, to establish procedures for making and handling reports (or to establish procedures that are not compliant), to verify and analyse the reports received;
c. have been convicted, even at first instance, of defamation or libel or, in any case, of the same offences committed while reporting to the judicial or accounting authorities.

11 TRAINING

The Whistleblowing Committee and all Orton employees, particularly those designated in the process to handle the report of potential wrongdoing, will receive specific training on the personal and material scope of whistleblowing and the submission, handling and follow-up of reports of potential wrongdoing.

12 DATA PROTECTION AND RECORD KEEPING

All data and information relating to the reporting of potential wrongdoing

- must be properly stored and retrievable;
- may be used as evidence in enforcement actions where appropriate;
- will be treated confidentially, unless required to do so by the relevant authorities.

Personal data that is not relevant to the handling of a report of potential wrongdoing will not be collected or, if collected inadvertently, will be deleted without undue delay.
Personal data that is found to be unfounded during the reporting process must be promptly destroyed or anonymised.
Internal and external reports and related documentation will be kept for as long as necessary to process the report, and in any case for no longer than five years from the date of communication of the final outcome of the reporting process, in compliance with confidentiality obligations under European and national data protection laws.

13 DATA MANAGEMENT AND PRIVACY

The data and documents reported will be stored in accordance with the provisions of European Regulation 679/2016 and Legislative Decree No. 196 of 30 June 2003:
The processing of personal data related to the receipt and handling of reports is carried out by public and private sector entities and by ANAC, in its capacity as data controller, in compliance with European and national principles on the protection of personal data, by providing adequate information to the reporting persons and to the persons involved in the reports, and by adopting appropriate measures to protect the rights and freedoms of the persons concerned.
Furthermore, the rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679 may be exercised within the limits of Article 2 of Legislative Decree No. 196 of 30 June 2003.