

WHISTLEBLOWING PROCEDURE

Carlo Salvi S.p.A.

Index

1. INTRODUCTION TO WHISTLEBLOWING3

2. SUBJECTS..... 3

3. OBJECT4

3.1. Exclusions..... 9

3.2. Content of reports 9

4. REPORTING CHANNELS..... 10

5. REPORT MANAGER 11

6. MANAGEMENT OF REPORTS 12

7. PROTECTIONS 14

7.1. Confidentiality 14

7.2. Protection from retaliation 16

7.3. The support measures 17

7.4. Limitations of liability..... 17

7.5. Exclusions..... 18

7.6. The processing of personal data 18

8. THE EXTERNAL REPORTING CHANNEL..... 18

9. PUBLIC DISCLOSURE 19

10. COMPLAINT 19

11. SANCTIONS SYSTEM 19

1. INTRODUCTION TO WHISTLEBLOWING

The term “whistleblowing” refers to a report made by a person who, in the performance of his or her duties, becomes aware of an offence, risk or dangerous situation that may cause harm to the company/body he or she works for, as well as to clients, colleagues, citizens and any other category of subjects.

Carlo Salvi S.p.A. (hereinafter “the Company”), which is sensitive to ethical issues and the proper conduct of its business, has implemented internal systems for reporting violations in order to allow subjects identified by law to report violations of national or European Union regulations that harm the public interest or the integrity of the public administration or the private entity, which have come to their attention in a public or private work context, including violations of the Code of Ethics or of the Organization, Management and Control Model pursuant to Legislative Decree 231/01.

Whistleblowing regulations identify:

- the subjects who may initiate a report;
- the acts or facts that may be reported, as well as the requirements that reports must meet in order to be taken into account;
- the procedures for reporting alleged violations and the subjects responsible for receiving reports;
- the investigation process to be activated following receipt of the report;
- the guarantee of confidentiality and protection of the whistleblower, of any reported person and of the data contained in the report;
- the prohibition of retaliation and of discrimination against the whistleblower.

2. SUBJECTS

Reports may be sent by the subjects expressly identified by Legislative Decree 24/2023, namely:

- Company’s employees, including workers with part-time, intermittent, fixed-term, apprenticeship and ancillary employment contracts, as well as workers who perform occasional services, and temporary workers, trainees and volunteers;
- self-employed workers, freelancers, collaborators and consultants who work for the Company;
- suppliers, i.e. workers or collaborators who perform their work activities by supplying goods or services or carrying out works in favour of the Company;
- shareholders, i.e. natural persons who hold shares in the Company;
- people who, also *de facto*, perform administration, management, control, supervision or representation of the Company functions;

Moreover, within the framework of the Hatebur Group's compliance policies and system, going beyond the legal provisions, reports can also be sent in by customers, i.e. workers or collaborators who using goods or services from the Company.

All the persons listed above may make reports when the legal relationship:

- is in place,
- has not yet started, if the information was acquired during the recruitment process or in other pre-contractual stages,
- after its termination, if the information on breaches was acquired in the course of employment, or during the probationary period.

Furthermore, the protective measures provided for and described in Chapter 7 below are also extended to the following persons:

- facilitators, i.e. persons who assist the whistleblower in the reporting process, providing advice and support, and who operate within the same work context as the whistleblower;
- people in the same work environment as the whistleblower who are linked to the whistleblower by a stable emotional or family relationship up to the fourth degree of kinship (people linked by a network of relations arising from the fact that they work, or have worked in the past, in the same work environment as the whistleblower);
- work colleagues with a habitual and current relationship with the whistleblower (persons who, at the time of the report, work with the whistleblower and have a relationship with him/her characterised by such continuity as to determine a relationship of commonality between the parties);
- entities owned by the whistleblower (entities of which the whistleblower is the sole owner or in which the latter has a majority shareholding);
- entities for which the whistleblower works (i.e., employee of a company providing a supply service for the Company.);
- entities operating in the same work environment as the whistleblower (i.e. partnership between companies).

3. OBJECT

The procedure application field includes reports concerning conduct, acts, omissions, even attempted ones, which may be detrimental to the Company insofar as they harm its integrity or the public interest, which have come to knowledge in the context of work.




Pursuant to Legislative Decree 24/2023, the subject of the report may consist of either an action (act or conduct) or an omission, committed in the following areas:





- management of public tenders;
- rules governing financial services, products and markets, as well as rules to prevent money laundering and terrorism financing;
- rules protecting the environment;
- rules protecting public health;
- rules aimed at the protection of privacy and of personal data, as well as the security of networks and information systems;
- consumer protection rules.
- rules on product safety and compliance and transport safety, as well as food and feed safety and animal welfare;
- radiation protection and nuclear safety rules;
- competition rules;
- State aid rules;
- internal market rules relating to acts in breach of corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax rules;
- as well as unlawful conduct relevant under Legislative Decree 231/2001 or violations of the Organization and Management Model.






In order to materially specify the scope of application of this document, please find below some examples of facts that can be reported:



- violations of rules, both internal and external, governing the Company's activities, including those contained in the Company's Organization, Management and Control Model, as well as the principles and rules of conduct contained in the Code of Ethics;
- unlawful or fraudulent conduct by employees, members of the corporate bodies or third parties (suppliers, consultants, collaborators) that may directly or indirectly result in financial and/or image damage for the Company;
- the possible commission of offences by employees, members of corporate bodies or third parties (suppliers, consultants, collaborators) committed to the detriment of the Company or that may give rise to possible liability for the Company.

In order to allow the Head of Internal Channel a concrete initial screening of reports for which this procedure is applicable, a synoptic framework for guidance is given below.

REGULATORY PROVISION	INTERPRETATION	RELEVANCE TO THE ACTIVITIES OF CARLO SALVI
<p>Illegal conduct relevant under Legislative Decree 231/01 or violations of the Model (Art. 2(1)(a)(2))</p>	<p>This is a regulatory issue already considered under the previous regulatory framework.</p> <p>Included in this group of violations are not only the report regarding the commission by an employee of a "predicate offense" of Legislative Decree 231/2001, but also violations of the principles contained in the model itself that do not necessarily constitute an offense. For example:</p> <ul style="list-style-type: none"> • Violations of the principles and rules of conduct contained in the Code of Ethics; • Violation of the principles set forth in the general and special parts of the Model (i.e., failure to transmit flows to the SB / failure to behave correctly, transparently and cooperatively with internal company regulations); • Violation of the operating procedures specified as the guardianship of sensitive activities. 	
<p>Offenses committed in the management of public contracts (Art. 2(1)(a)(3))</p>	<p>In this case, No. 3 of Article 2 links the violation to specific national or European Union acts, as listed in Annex 1, Part 1(a), viz:</p> <ul style="list-style-type: none"> • Procedural rules for the award of public contracts and concessions, including in general terms Legislative Decree 50/2016; • Procedural rules for defense and security procurement; • Procedural rules for the awarding of contracts by utilities in the water, energy, transportation and postal services sectors. <p>Consequently, any violation of procedures for entering into a procurement and concession contract becomes relevant. For example:</p> <ul style="list-style-type: none"> • Failure to declare compliance with the requirements of Articles 94 and 95 of Legislative Decree 36/2023 for an economic operator wishing to participate in a procurement procedure; • Failure to comply with the procedure specified by Legislative Decree 36/2023 on the basis of the established requirements (i.e. open procedure, negotiated procedure without prior publication of the notice etc.). <p>Given the specificity and technicality of the regulations referred to in Legislative Decree 24/2023, which do not concern the activity carried out by the Company, the risk of reports being received in this area is low.</p>	
<p>Violations of regulations governing financial services, products and markets and prevention of money laundering and terrorist financing (Art. 2(1)(a)(3))</p>	<p>In this case, No. 3 of Article 2 links the violation to specific national or European Union acts.</p> <p>Specifically, Annex 1, Part 1(b) identifies standards that regulate consumer and investor protection in financial services markets and in the areas of credit, investment, occupational pensions, securities, investment funds etc.</p> <p>By way of example:</p> <ul style="list-style-type: none"> • Violation of regulations related to alternative investment funds (i.e., intangibles, venture capital, cryptocurrency); • Violation of the regulations related to the protection of consumers wishing to enter into real estate credit contracts (i.e., mortgage or loan), which affects credit intermediaries and, therefore, to banks and financial intermediaries; • violations of the regulation of OTC derivative contracts and related obligations (i.e., derivative contract reporting requirements or central clearing of OTC derivative contracts). These are contracts entered into outside regulated markets and made between contracting parties, such as a contract in which the parties exchange forward, periodic or one-time cash flows that are calculated by applying a definitive pattern; • violations of regulations regarding financial conglomerates, i.e., a group of firms that meets certain conditions (i.e., the parent firm is a regulated firm 	

	<p>and controls another firm in the financial sector, and at least one of the firms in the group operates in the insurance sector).</p> <p>In view of the specificity and technicality of the regulations referred to in Legislative Decree 24/2023, which do not in any way affect the activities carried out by the Company, the risk of reports being received in this area is low.</p>	
<p>Violation of product safety and compliance regulations (Art. 2(1)(a)(3))</p>	<p>In this case, No. 3 of Article 2 links the violation to specific national or European Union acts, which includes, for example, Legislative Decree 206/2005 (Consumer Code). The Consumer Code, in Part IV on the safety and quality of products placed on the market, identifies obligations on the manufacturer and distributor of products. However, these provisions refer to the placing of items on the market not regulated by specific regulations or to safety aspects not regulated by industry disciplines. In general terms, they could, therefore, be the subject of reportable violations through the whistleblowing channel:</p> <ul style="list-style-type: none"> • The placing of unsafe product on the market; • Failure to inform the consumer of information useful for assessing risks from normal use of the product; • Failure to conduct spot checks on marketed products. <p>Given the specificity and technicality of the regulations referred to in Legislative Decree 24/2023, which do not concern the activity carried out by the Company, the risk of reports being received in this area is low.</p>	
<p>Violation of transportation security regulations (Art. 2(1)(a)(3))</p>	<p>In this case, No. 3 of Article 2 links the violation to specific national or European Union acts, such as, for example, safety in the railways, civil aviation or road and maritime sectors</p> <p>Given the specificity and technicality of the regulations referred to in Legislative Decree 24/2023, which do not concern the activity carried out by the Company, the risk of reports being received in this area is low.</p>	
<p>Violation of environmental protection regulations (Art. 2(1)(a)(3))</p>	<p>In this case, No. 3 of Article 2 links the violation to specific national or European Union acts, including, first and foremost, Legislative Decree 152/06 (Consolidated Environmental Act). Therefore, they fall within the scope of Legislative Decree 24/2023 reports having to do with:</p> <ul style="list-style-type: none"> • Mismanagement of waste produced by the Company; • facts pertaining to the "reputation" of Carlo Salvi S.p.A.'s environmental suppliers (transporters, disposers); • Air and water quality; • contamination of owned land or presence on it of waste abandoned by third parties (even if from a criminal point of view these are not facts attributable to the Company). 	
<p>Violation of radiation protection and nuclear safety regulations (Art. 2(1)(a)(3))</p>	<p>In such a case, No. 3 of Article 2 links the violation to specific national or European Union acts, which cover very specific areas relevant to the nuclear energy sphere, such as:</p> <ul style="list-style-type: none"> • safety of nuclear facilities; • Protection of the public with regard to radioactive substances; • Responsible and safe management of spent nuclear fuel and radioactive waste. <p>Given the specificity and technicality of the regulations referred to in Legislative Decree 24/2023, which do not concern the activity carried out by the Company, the risk of reports being received in this area is low.</p>	
<p>Violation of regulations set to protect food and</p>	<p>In such a case, No. 3 of Article 2 links the violation to specific national or European Union acts related to regulations pertaining to circumscribed areas, such as, for example:</p>	

<p>feed safety and animal health and welfare (Art. 2(1)(a)(3))</p>	<ul style="list-style-type: none"> • The general principles and requirements of food law and in the field of food safety • Violations related to the obligation to register operators, establishments and animals; • Violations related to trade, import, conservation of wildlife and exotic animals; • Violations related to regulations pertaining to animal protection on farms. <p>Given the specificity and technicality of the regulations referred to in Legislative Decree 24/2023, which do not concern the activity carried out by the Company, the risk of reports being received in this area is low.</p>	
<p>Violation of regulations set to protect public health (Art. 2(1)(a)(3))</p>	<p>In such a case, No. 3 of Article 2 links the violation to specific national or European Union acts, relating to strictly identified and very technical and circumscribed areas, such as, for example:</p> <ul style="list-style-type: none"> • Collection, testing, processing, storage and distribution of human blood and blood components; • Donation, procurement, testing, processing, preservation and distribution of human tissues and cells; • education of the national network of rare diseases and exemption of participation in the cost of health care services; • veterinary medicines. <p>In view of the specificity and technicality of the regulations referred to in Legislative Decree 24/2023, which do not in any way affect the activities carried out by the Company, the risk of reports being received in this area is low.</p>	
<p>Violation of the rules set out to protect the consumer (Art. 2(1)(a)(3))</p>	<p>In this case, No. 3 of Article 2 links the violation to specific national or European Union acts, including, among others, the Consumer Code and Legislative Decree 173/2021 on contracts for the provision of digital content and digital services. Thus, we can speculate:</p> <ul style="list-style-type: none"> • Introduction of unfair terms into the contract; • Information not appropriate to the communication technique or not clear and understandable; • Failure to inform the consumer about updates available and necessary to maintain compliance. <p>Given the specificity and technicality of the regulations referred to in Legislative Decree 24/2023, which do not concern the activity carried out by the Company, the risk of reports being received in this area is low.</p>	
<p>Violation of regulations aimed at privacy and personal data protection, as well as network and information system security (Art. 2(1)(a)(3))</p>	<p>In this case, No. 3 of Art. 2 links the violation to specific national or European Union acts, among which the Privacy Code and the GDPR, implemented in the system by Legislative Decree 101/2018, are mentioned. Therefore, they fall within the scope of Legislative Decree 24/2023 reports having to do with:</p> <ul style="list-style-type: none"> • failure to inform; • Failure to update the treatment register; • Failure to seek consent from those whose data are being processed; • Use of video surveillance in the absence of requirements (i.e., double disclosure). <p>It also includes any reports concerning the failure to implement aspects regarding confidentiality and data protection in the case of whistleblowing.</p>	
<p>Violation affecting the financial interests of the European Union under Article 325 TFEU. (Art. 2(1)(a)(4))</p>	<p>As is well known, Article 325 TFEU requires member states to take measures to combat fraud, which harms the financial interests of the European Union. This means, therefore, that conduct aimed at the diversion of tax revenues or EU funds is punished within national legal systems. By way of example, the following may fall within the scope:</p> <ul style="list-style-type: none"> • fraud detrimental to the financial interests of the EU, which may result from the submission of false statements or documents resulting in the misappropriation of funds or property from the EU or the inaccurate declaration of VAT to disguise a non-payment; • Corrupt activities in which European or national officials are involved; 	

	<ul style="list-style-type: none"> any illegal activity related to European Union expenditures, such as the irregular use of European Union funds earmarked for specific projects. 	
<p>Violation of internal market rules, including violations of competition and state aid rules and violations related to acts that violate corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law (Art. 2(1)(a)(5))</p>	<p>Violations of internal market regulations concern, as indicated by Legislative Decree 24/2023:</p> <ul style="list-style-type: none"> regulations pertaining to competition; regulations pertaining to state aid; Legislation in tax and fiscal matters. <p>Thus, such violations could be configured, by way of example: in acts of unfair competition, such as the use of distinctive names or signs likely to create confusion with those already adopted by others, or in the dissemination of news and appreciations about the competitor's products and activities likely to bring them into disrepute. Such acts are apt to constitute a tort of a civil nature and, when done with threats or violence, of a criminal nature. In failure to pay taxes, for which administrative penalties apply, or in fraudulent and unfaithful tax returns. The latter behaviors are abstractly capable of configuring criminal offenses, which are, likewise, predicate offenses of Legislative Decree 231/2001.</p>	
<p>Offenses that frustrate the object or purpose of the provisions of EU acts in the above areas (Art. 2(1)(a)(6))</p>	<p>For example, abusive practices, as defined by the Court of Justice of the European Union, should be brought within this scope. As an example, one can think of an enterprise operating in a dominant position in the market. Although it is not expressly forbidden for an enterprise to gain such a status, there is a risk that by the enterprise's conduct, effective and fair free competition in the internal market will be undermined through the use of abusive practices, such as, for example, the adoption of predatory pricing or tying sales). Under this assumption, therefore, the objective of the European Union with respect to the protection of free competition would be frustrated.</p>	

3.1. Exclusions

The following are excluded from reports of interest under the whistleblowing legislation and, therefore, will not be handled in accordance with this document:

- grievances or claims or requests having to do with interpersonal matters. Grievances of a personal nature of the whistleblower or claims/requests that fall under the discipline of the employment relationship or relations with the supervisor or colleagues should continue to be sent to Human Resources;
- complaints related to inefficiencies or problems with the services performed by the Company, which do not affect the quality of the product (in terms of its safety);
- mere rumors or "hearsay."

3.2. Content of reports

The Company may also take into consideration anonymous reports, provided that they are adequately substantiated and made with a wealth of details, i.e. they are such as to bring to light facts and situations linking them to specific contexts (i.e.: documentary evidence, indication of names or particular qualifications, mention of specific offices, proceedings or particular events, etc.).

The report - even the non-anonymous one - must be detailed and as complete and exhaustive as possible.

The whistleblower is required to provide all the available and useful elements to allow the due and appropriate checks and verifications to be carried out to ascertain the validity of the reported facts, such as:

- a clear and complete description of the facts being reported;
- the circumstances of time and place in which the reported facts were committed;
- the personal details or other elements that allow for the identification of the person(s) who has/have carried out the reported facts (i.e., qualification, place of employment where he/she carries out the activity);
- any documents supporting the report;
- the indication of any other individuals who may report on the facts being reported;
- any other information that may provide useful feedback about the existence of the reported facts.

For a report to be substantiated, these requirements do not necessarily have to be met simultaneously, in view of the fact that the whistleblower may not be in full possession of all the required information.

4. REPORTING CHANNELS

Reports can be made

- in writing as a message via the Whistleblower-Portal of Hatebur Group / Carlo Salvi (<https://hateburgroup.integrityline.io/?lang=it>) (hereafter, the "Software"), as a suitable reporting channel to ensure, in an IT manner, the confidentiality of the whistleblower's identity in compliance with the regulations, with the possibility of uploading documents and video content;
- orally, with a face-to-face meeting with the Whistleblowing Committee or one of its members, to request by filling in request on the Whistleblower-Portal.

The content of the meeting will be recorded in a report drafted by the reporting manager and signed by the reporter to confirm the accuracy of what was reported

Through the IT channel - and, therefore, through the Software - the whistleblower will be guided through each stage of the report and will be asked, in order to better circumstantiate the report, to compulsorily fill out a series of fields, respecting the requirements set out in section 4.3 above.

5. REPORT MANAGER

The entity responsible for receiving and handling reports is the Whistleblowing Committee, composed of:

- CEO Carlo Salvi;
- CEO Hatebur Group
- Chairman of Supervisory Body

In the event that the alert concerns a member of the Committee, it will be handled by those members who do not have a conflict. Then, the member involved by the report is excluded from its management.

Depending on the content of the report, the Whistleblowing Committee, after coordinating by e-mail or directly, decides which Member should be assigned to the report (Case Manager).

Several people may be assigned to the same report.

The name of the Case Manager will be matched to each single report received.

In the management of operational activities, the Case Manager may avail itself of the support of specifically authorized internal resources by means of a special communication given in writing; in addition, in carrying out the preliminary investigation, the Case Manager may be supported by the corporate organizational structures from time to time competent or by external professionals appointed for the purpose.

In the event that a report is sent through channels other than those listed above, the person receiving such a report shall:

- forward it - using the internal channel described above - to the Reporting Committee immediately and, in any case, no later than 7 days after its receipt,
- simultaneously notify the whistleblower of such transmission, where possible.

6. MANAGEMENT OF REPORTS

Once the report is received, according to the channel provided in this procedure, it is handled in four steps:

- a) *protocol and custody;*
- b) *preliminary investigation;*
- c) *Investigation and communication of the outcome;*
- d) *storage.*

a) **Protocol and custody**

In case the report is made through the Software, it will be the Software itself to provide for full and confidential protocol in accordance with the relevant regulations.

b) **Preliminary investigation**

The purpose of the preliminary investigation is to verify the merits of the report received.

Once the report is received, individual Case Manager evaluate it and check for urgency and/or the need for timely feedback/intervention.

First, the Case Manager verifies:

- the admissibility of the report, that is, whether it falls within the objective scope of Legislative Decree 24/2023
- if the vagueness of its content does not allow for an understanding of the facts.

If either of the two hypotheses listed above finds concrete evidence, the Case Manager files the report stating the reason, and notify the whistleblower, if not anonymous, possibly routing him or her to the Competent Company Functions to proceed in the appropriate forum.

If the report appears to be circumstantial - with precise and concordant factual elements - the investigation steps are proceeded with.

c) **Investigation and communication of the outcome**

Preliminary investigation is the set of activities aimed at verifying the content of the reports received and acquiring elements useful for the subsequent evaluation phase, ensuring maximum confidentiality on the identity of the whistleblower and the subject of the report.

The main purpose of the investigation is to verify the truthfulness of the information submitted for investigation, by providing a timely description of the established facts through objective audit procedures and investigative techniques.

If the report is found to fall within the objective scope of Legislative Decree 24/2023 and is supported by sufficient evidence to proceed, the Committee or the Case Manager in charge shall initiate the investigation phase and, to this end, may:

- request clarifications and additions from the whistleblower, if not anonymous;
- request clarification from any other parties involved in the report with the necessary precautions taken (i.e., when the identity of the whistleblower is not properly specified in the report, or when the report is not properly substantiated);
- Acquire internal Company documents;
- proceed to the hearing of other corporate officers who, on the basis of the contents of the report, might be informed of the facts that are the subject of the report;
- make use, if the report makes it necessary, of external consultants specialized in carrying out investigative activities or experts in specialized legal subjects related to the subject of the report;
- proceed to the hearing of the whistleblower if it does not affect the performance of the activities and protections guaranteed to the whistleblower under Chapter 7 below.

Minutes must be prepared for each hearing and signed by all the attendants (including the whistleblower).

Within 3 months of the feedback provided to the whistleblower about the receipt of his or her report, the Committee terminates the investigative activities and communicates the outcome to the whistleblower.

If the report is of particular complexity, investigative activities shall continue, but the whistleblower shall be informed of this (always within the same time limit of 3 months starting from the day on which the whistleblower was acknowledged about the receipt of his/her report).

As mentioned above, feedback is provided even if the report does not fall within the objective scope of Legislative Decree 24/2023.

Upon completion of the checks, the Committee:

- file the report if it is unfounded;
- whether it does not believe that there are grounds for dismissing the report:
 - 1) informs the Board of Directors of the outcome of the investigation, with a view to taking such measures and/or actions as may be necessary in the specific case for the protection of the Company, including reporting to the competent authorities;
 - 2) communicates the outcome of the assessment to the Company's Management, so that it can implement any improvement actions identified, as well as for the initiation of management measures within its competence, including, if the prerequisites exist, the exercise of disciplinary action.

d) Storage

In order to ensure traceability, confidentiality, preservation and retrievability of data throughout the process, documents are stored and archived in digital format, via the Software.

All documentation will be retained, subject to further legal deadlines in cases expressly provided for, for 5 years from the date of closure of activities.

7. PROTECTIONS

The forms of protection listed below are accorded to whistleblowers and other persons indicated in paragraph 2 above, provided that they:

- have made the report in good faith, reporting true facts and having well-founded reason to believe that the circumstance that was the subject of the report was true (i.e., the whistleblower must have specified the circumstances of time and place and specifically described the fact, the reporter must not have knowingly reported erroneous or patently unfounded information) and that the same fell within the objective scope of the report;
- the whistleblower has complied with the procedure set forth in this company document.

The protections described in this paragraph do not apply when the liability of the whistleblower for the crimes of slander or defamation or the same crimes related to whistleblowing or the civil liability of the whistleblower for intentionally reporting false information with malice or negligence has been established by judgment (including first degree). In these cases, disciplinary sanctions may also apply.

7.1. Confidentiality

Except for the "Exclusions" provided in Section 7.5 below, the identity of the whistleblower is protected in any context resulting from the report.

The use of the Software ensures complete confidentiality of the reporter, as only the Reporting Committee can access the report, and the report is indicated with a specific ID used in all official documents and communications during the course of the investigative activity.

As part of any disciplinary proceedings instituted against the reported person:

- if the facts charged were based on separate and additional investigations to the report, even if consequential to the report, the identity of the reporting person may not be disclosed;
- if the facts charged were based in whole or in part on the report, the identity of the whistleblower may be disclosed to the person(s) involved in the report if two requirements are met simultaneously:
 - the consent of the whistleblower;
 - the proven need on the part of the reported person to know the name of the whistleblower for the purpose of a full exercise of the right of defense.

Therefore, subject to the above exceptions, the identity of the reporter and further information regarding the report received cannot be shared, without the consent of the whistleblower, with parties other than the Committee and the facilities involved in investigating reports.

In particular, regarding the scope of disciplinary proceedings initiated against the whistleblower, the identity of the whistleblower may be disclosed, with his/her express consent, to the function responsible for disciplinary measures when the disciplinary charge is based, in whole or in part, on the whistleblower's report and knowledge of the whistleblower's identity is absolutely essential to the defense of the accused.

In such cases, written notice shall be given to the reporter of the reasons for the disclosure of the confidential data.

In the case of the initiation of proceedings before the Court of Auditors against the whistleblower, the identity of the whistleblower is not disclosed until the investigation is closed.

After this deadline, the identity of the whistleblower can be disclosed by the Accounting Authority for use in the proceedings.

In the context of criminal proceeding, initiated against the reported person, the identity is covered by official secrecy until the preliminary investigation is closed.

Should the judicial authority want to know the name of the whistleblower for investigative needs, the relevant corporate function shall provide the identity of the whistleblower.

In any case, the liability of the whistleblower remains unaffected if the report was made in bad faith and, therefore, liability by way of slander or defamation under the provisions of the Criminal Code or Article 2043 of the Civil Code can be established. If it is established by the Committee or a member of them that the whistleblower is acting in bad faith, the protection of confidentiality is waived, and the reported person is informed of the whistleblower's identity in order to grant the reported person the right to file a suit for libel or slander.

7.2. Protection from retaliation

No form of retaliation or discriminatory measures shall be permitted or tolerated against the whistleblower and other persons named in Chapter 2.

By way of example, retaliation is considered to be:

- dismissal, suspension or equivalent measures;
- grade demotion or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- demerit notes or negative references;
- adoption of disciplinary measures or other sanction, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavorable treatment;
- failure to convert a fixed-term employment contract to a permanent employment contract where the employee had a legitimate expectation of said conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- inclusion on improper 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 the contract for the provision of goods or services;
- cancellation of a license or permit;
- request for submission to medical examination.

Protected people who believe they have been retaliated against may notify ANAC.

If it is attempted or threatened retaliation, the whistleblower must provide evidence from which the actual existence of the threat can be inferred. If facts are attached by the whistleblower, the onus is on the person who attempted or threatened retaliation to prove that the facts attached are unrelated to the report made.

If in judicial or administrative proceedings or out-of-court litigation or claim for compensation filed with the Judicial Authority the whistleblower proves that he or she made a report and was retaliated against, the person who engaged in such conduct must prove otherwise (prove that the action taken has no connection with the report).

The reversal of the burden of proof does not apply to parties other than whistleblowers (i.e., facilitators, reporter-owned entity etc.).

7.3. The support measures

The whistleblower has the option of turning to Third Sector entities (a list of which can be found at ANAC's website), which provide assistance and advice free of charge on:

- how to report;
- the protection from retaliation recognized by national and European Union regulatory provisions;
- the rights of the person involved;
- the terms and conditions of access to legal aid.

7.4. Limitations of liability

The whistleblower does not incur any kind of civil, criminal, administrative or disciplinary liability when disclosing information covered by the obligation of secrecy, with respect to:

- disclosure and use of official secrets (Article 326 of the Criminal Code);
- disclosure of professional secrecy (Article 622 of the Criminal Code);
- disclosure of scientific and industrial secrets (Article 623 of the Criminal Code);
- violation of the duty of loyalty and loyalty (Article 2105 of the Criminal Code);
- violation of copyright protection provisions;
- violation of the provisions on the protection of personal data;
- disclosure or dissemination of information about violations that offend the reputation of the person involved.

The limitation of liability also applies to conduct, acts or omissions put in place by the entity or person if related to the report and strictly necessary to disclose the violation (not superfluous).

The exemption from liability operates only if certain conditions are met, such as:

- the acquisition of information or access to documents was done lawfully (i.e., the whistleblower made copies of records/accessed another colleague's e-mail with his or her consent);
- at the time of the report, the whistleblower had reasonable grounds for believing that the information was necessary for the breach to be uncovered (the prerequisite is not met, for example, in the case of vindictive or opportunistic purposes).
- the whistleblower had reasonable grounds to believe that the information was true and was within the scope of the reports, having also made the report in the manner prescribed by this Procedure.

7.5. Exclusions

The measures and protections provided for in this Chapter, and described above, do not apply to those who have made the report in bad faith or, when, liability by way of slander or defamation can be established pursuant to the provisions of the Criminal Code or Article 2043 of the Civil Code and the hypotheses in which anonymity cannot be enforced by law (i.e., criminal, tax or administrative investigations, inspections by supervisory bodies).

7.6. The processing of personal data

Acquisition and management of reports are carried out in accordance with data protection regulations.

The Company has prepared a specific disclosure for the whistleblower.

8. THE EXTERNAL REPORTING CHANNEL

The whistleblower may make an external report to ANAC upon the occurrence of one of the following conditions:

- the internal channel, although mandatory, is not active;
- the internal channel activated by Carlo Salvi S.p.A. does not comply with the provisions of Legislative Decree 24/2023 in reference to the subjects and methods of submission of reports;
- the whistleblower has made a report through the internal channel activated by Carlo Salvi S.p.A., but this has not been followed up (i.e., the report was not processed within the stipulated time limits or no action was taken as a result of the actual establishment of the reported violation);
- the whistleblower has reasonable grounds to believe that the internal report would not be effectively followed up (i.e., evidence could be concealed or destroyed); in such a case, the whistleblower must attach factual circumstances and information to support the his or her claim;
- the whistleblower has reasonable grounds to believe that internal reporting could result in the risk of retaliation (i.e., violation of the obligation to keep the identity of the whistleblower confidential); in this case, the whistleblower must attach factual circumstances and information to support the his or her claim;
- the whistleblower has reasonable grounds to believe that the violation may pose an imminent or obvious danger to the public interest (i.e., violation requiring urgent action, to safeguard the health and safety of persons).
- without these prerequisites, the report is not handled by ANAC and the individual does not benefit from the protections outlined in Chapter 7.

The external reporting channel cannot be used in the event of a relevant violation under Legislative Decree 231/2001 and the Organizational Model.

9. PUBLIC DISCLOSURE

The whistleblower may make the report by public disclosure, putting the information in the public domain (i.e., press or social media) only if the he or she:

- has made an internal report and one external report to ANAC, and neither report was responded to within the deadline;
- has made an external report directly and it was not responded to within the deadline;
- has reasonable grounds to believe that the violation may pose an imminent or obvious danger to the public interest (i.e., emergency situation or risk of irreversible harm);
- has well-founded reason to believe that the external report may pose a risk of retaliation or may not be effectively followed up (i.e., evidence may be concealed or destroyed or the person who received the reports may be colluding with or involved with the perpetrator).

The whistleblower must attach factual circumstances and information to support the allegation.

Without these prerequisites, the person does not benefit from the protections described in Chapter 7.

The external reporting channel cannot be used in the event of a relevant violation under Legislative Decree 231/2001 and the Organizational Model.

10. COMPLAINT

The whistleblower can freely turn to the relevant national judicial and accounting authorities, benefiting from the protections provided.

This is without prejudice to the obligation of individuals who hold the title of public official or public service appointee to report to the competent judicial authorities pursuant to Articles 361 and 362 of the Criminal Code.

11. SANCTIONS SYSTEM

Sanctions are provided for non-compliance with this Procedure.

Specifically, the following are provided:

- disciplinary sanctions against the whistleblower who has made reports in bad faith and which turn out to be unfounded, if he or she is found by judgment (even of first instance) to be criminally liable for the crimes of slander or defamation or for the same crimes related to the report, or to be civilly liable for intentionally reporting false information with malice or negligence;
- sanctions against the Committee or a member of them or people in charge of the investigation in case of violation of the to keep the identity of the whistleblower and the content of the report confidential;

- disciplinary sanction upon the reported person in the event that the Committee, at the outcome of the investigation, determines that the report is justified and internal disciplinary proceedings are initiated.

Any form of abuse, such as opportunistic reports and/or reports made for the sole purpose of harming the reported person or others, as well as any other hypothesis of improper use or intentional instrumentalization of whistleblowing, are also a source of liability in disciplinary and other competent fora.