# WHISTLEBLOWING PROCEDURE

Approved by the Board of Directors on October 27th, 2022

Revision approved by the Board of Directors on November 7th, 2023

*This document is an English translation from Italian. The Italian original shall prevail in case of differences in interpretation and/or factual errors.*

# TABLE OF CONTENTS

## 1. SCOPE AND PURPOSE OF THE PROCEDURE

This procedure has been adopted pursuant to **art. 6 co. 2-*bis***, **Legislative Decree 231/2001**, as replaced by **Legislative Decree no. 24 of 10 March 2023** ("*Implementation of Directive (EU) 2019/1937 of the European Parliament and Council, of 23 October 2019, regarding the protection of persons who report the violation of rules of Union law and containing provisions concerning the protection of persons who report the violation of rules of national law*").

Furthermore, the drafting of this document takes into account the Whistleblowing Guide Lines approved by the National Anti-Corruption Authority (hereinafter "**ANAC**") with **resolution no. 311 of 12 July 2023**.
Reporting is an act of expression of civic responsibility, through which the reporter (hereinafter "whistleblower") contributes to the emergence and prevention of risks and detrimental situations for the entity in which they belong and, as a reflection, for its interests.
The whistleblower is the person who reports violations of provisions of national law or Union law which damage public interest or the integrity of public administration or a private entity, of which they have been made aware in a private or public working environment.
This procedure has the purpose of identifying the general principles to regulate the process of **reception**, **analysis**, and **processing** of the **reports**, with the objective of incentivising its utilisation within The Italian Sea Group S.p.A. (hereinafter "TISG" or the "Company").

The reporting procedure warrants:

- The protection of confidentiality of the identities of the reporter and the alleged author of the violation, without prejudice to the discipline on investigations and procedures instituted by the judicial authority;
- The protection of the reporter against possible illicit actions, such as retaliation and discrimination, following the report;
- The development of an internal reporting channel granting the reporter's confidentiality.

This procedure, which is an integral part of the Organisation, Management and Control Model implemented by the Company pursuant to Legislative Decree 231/2001, **does not apply to public disclosures**, which are referred to in the contents of Legislative Decree 24/2023 and the aforementioned ANAC Guide Lines.

Furthermore, the scope of this procedure excludes any disciplinary measures implemented by the Company, through the appropriate representatives, as a consequence of the investigation carried out on the report.

## 2. RECIPIENTS OF THE PROCEDURE

The categories legitimised the persons operating in the Company's working environment are:

- Members of TISG's corporate bodies;
- Shareholders;
- All of those having functions of administration, direction, control, surveillance and/or representatives of the Company;
- The Company's employees;
- Partners, clients, suppliers, advisors, collaborators;
- Any other entities who have certified relationships with TISG.

The term "working environment" is wide and takes into account not only those who have a working relationship in the strict sense with the Company, but also those who have other type of legal relationships with TISG: advisors, collaborators, interns. This is also true when it comes to pre-contractual relationships, test periods, or subsequent situation arising after termination of the legal relationship if the information regarding the violations has been acquired throughout the relationship itself. Furthermore, the reporter can report facts learned by virtue of their role, but also news acquired in occasion and/or due to the performance of working duties, even by chance. What is relevant, indeed, is the existence of a certified relationship between the reporter and TISG, a relationship which concerns work or professional activities, present or past.

## 3. SUBJECTS AND CONTENTS OF THE REPORT

Subjects of the report are behaviours, acts, or omissions which damage public interest or the integrity of public administration of which the reporter has been made aware in the working environment and which consist of:

1. Violation of **national regulatory provisions** consisting of:
   - Administrative, accounting, civil, or criminal offenses;
   - Illicit behaviour relevant *ex* Legislative Decree 231/2001;
   - Violation of the Management and Ogranisation Model (the latter do not integrate predicate offences for the application of Legislative Decree 231/2001 and pertain to the Company's organisational aspects);

2. Violation of **European regulatory provisions** related to the following sectors:
   - Offenses which fall into the application of the European Union acts related to the following sectors: public procurement; services, products, and financial markets and prevention of money-laundering and financing of terrorism; safety and conformity of products; safety of transformation; protection of the environment; radioprotection and nuclear safety; safety of the food and feed and animals' health and welfare; public health; consumers' protection; protection of private life and protection of personal data and security of networks and information systems. By way of example consider so-called environmental offences such as discharge, emission, or any other disposal of dangerous materials in the air, land, or water or illicit collection, transportation, recovery or disposal of dangerous waste;
   - Acts or omissions which damage the financial interests of the EU *ex* art. 325 of the Treaty on the Functioning of the European Union (fight against fraud). By way of example, consider fraud, corruption, or any other illegal activity connected to EU expenses;
   - Acts or omissions regarding the internal market, *ex* art. 26, § 2, of the Treaty on the Functioning of the European Union: that is, violations on the subject of competition and State aid, corporate tax and mechanisms with the purpose of having a tax benefit which negate the object or the purpose of the applicable regulation on the subject of corporate tax;
   - Acts or behaviours which negate the object or the purpose of provision *ex* the acts of the EU in the previously identified sectors. By way of example, think of a company which, due to its merits and abilities, operates the market in a leading position, which with its behaviour could negate an effective and fair competition in the internal market through the employment of so-called abusive practices (adoption of so called

"predatory prices", target discounts, bundling) contrary to the protection of free competition.

Furthermore, are object of reports:

- Information, including well-founded suspicions, regarding committed violation or violations which, on the basis of concrete elements, the whistleblower believes could be committed;
- Information related to behaviour aimed at concealing the aforementioned violations (e.g. concealment or destruction of evidence regarding the committed violation).

The following are not included in the information on the violations to be reported:

- Information which are clearly unfunded;
- Information which are already public knowledge, as well as information acquired on the basis of unreliable indiscretions or rumours (so-called "word on the street").

| **Legislative Decree 24/2023, art. 1 § 2** |
|---|
| **WHAT CANNOT BE SUBJECT TO A REPORT** |
| Complaints, demands, or requests linked to a personal interest of the reporter which attain exclusively to their individual working relationships, or related to their personal working relationship with hierarchically superior individuals. |
| Reports of violations where already compulsorily disciplined by the European Union or national acts indicated in part II of the annex to the Decree or by national acts constituting implementation of EU acts indicated in part II of annex to the EU Directive 2019/1937, although not indicated in part II of the annex to the Decree. |
| Reports of violations regarding national security issues, as well as contracts related to national defence or security concerns, except where those concerns fall within the relevant secondary EU legislation. |

*(Source: ANAC Guidelines)*

In any case, national/European provisions are applied on:

- Classified information;
- Attorney-client privilege;
- Doctor-patient privilege;
- Confidentiality of resolutions by institutional bodies;
- Criminal procedural rules;
- Judiciary's autonomy and independence;
- National defence and order and public security;
- Exercise of labour rights.

Reasons which have led a person to report are irrelevant for the purpose of handling the report and of the protection from retaliation.

Reports regarding a complaint, a claim, or a request linked to the reporter's personal interests are not considered whistleblowing reports.

## 4. INTERNAL REPORTING CHANNEL

The management of the internal channel is assigned, following a Board resolution, to a joint Whistleblowing Committee (hereinafter the "Committee") composed by the Head of Internal Audit and two members of the Auditing Body *ex* Legislative Decree 231/2001 (hereinafter, "AB"). The Committee is authorised by TISG to managed personal data and it is the recipient of a specific training regarding privacy and whistleblowing, even referencing real case studies.

Reports happen through an IT platform, accessible through the following link https://tisg.segnalazioni.eu/#/, made available in the footer of the website https://theitalianseagroup.com/.

Through the use of cryptography instruments, such platform grants confidentiality:

- Of the reporter;
- Of the enabler (any person assisting the reporter through the reporting process, operating within the same working environment);
- Of the person involved and/or the subjects in any case mentioned within the report;
- Of the contents of the report and related documentation.

In order to facilitate the reporter, there is the possibility to make reports orally, upon the reporter's request, through a direct meeting scheduled within a reasonable term. The meeting request shall be sent via mail in a closed envelope, with the label "reserved", at the attention of the Whistleblowing Committee at the registered office in Viale Cristoforo Colombo 4bis, Marina di Carrara (MS).

The meeting request shall contain solely the contacts of the inquirer; the contents and elements of the report will be orally detailed within the meeting, of which the Committee will draft and keep a specific record.

It is specified that ordinary e-mail and legal mail are not adequate means to grant confidentiality.

The reporter has the obligation to specify whether they want to maintain their identity confidential, and whether they want to exercise the protection provided to whistleblowers.

*Anonymous reports*
Anonymous reports, that is those for which it is not possible to assess the identity of the reporter, where adequately detailed, are equivalent to ordinary reports.

TISG considers anonymous reports received through the internal channels in the same way as ordinary reports, and manages them through the same criteria established for the latter.

In case of anonymous reports, the protection measures for retaliation are applicable:
- If the reporter has been subsequently identified and has been subjected to retaliation (*internal channel*);
- If the reporter, subsequently identified, has notified ANAC of having been subjected to retaliation (*external channel*).

TISG is obliged to register the anonymous reports received and to keep the relative documentation in accordance to current regulation, making it available for retrieval in case the reporter notifies ANAC of having been subject to retaliation due to the anonymous report.

*Elements of the report*
The report shall be as detailed as possible in order to allow for a clear comprehension of the facts. In particular, from the report have to be deduced:
- The time and place circumstances in which the fact object of the report has taken place;
- A description of the facts;
- The general information or other elements which can allow for the identification of the subject to which attribute the reported facts.

Furthermore, it is appropriate to attach suitable documentation to provide elements of substantiality of the facts object of the report, as well as the indication of other subjects which may potentially be aware of the facts. Wherever the report is not adequately detailed, the Committee can ask for integrations to the reporter through the dedicated channel or even in person, wherever the reporter has asked for a direct meeting.

The decision to request integration is remitted to the discretion of the Committee, which shall consider, for this purpose, the prominent interest of protecting the Company's integrity.

It is understood that such request cannot be intended as entirely supplementary with respect to a completely inadequate report: the reporter, in the main proceedings, has the burden of precisely describe the illicit facts which they intend to bring to the Company's attention for the protection of its integrity.

*Preliminary investigation*
The Committee:

- Provides a notice of receipt to the reporter through the IT platform **within seven days from the receipt date**;
- Maintains communication with the reporter;
- Gives an appropriate follow-up regarding the received reports;
- Provides feedback to the reporter.

In particular, the Committee verifies, respecting reasonable timing and confidentiality of the data, the existence of the essential requirements of the report in order to evaluate its eligibility and therefore agree the provided protection to the reporter. By way of example, the report may be rejected due to:

- Clear baselessness due to the absence of factual elements adequate to justify an investigation;
- Generic contents, which does not allow for the comprehension of the facts;
- Inappropriate or ineffective attached documentation.

After evaluating the eligibility of the report, the Committee starts an internal investigation on the reported facts or behaviour to evaluate their existence and, upon conclusion, provides feedback to the reporter, notifying them the follow-up (*rectius*: consequential actions) which will occur or is intended to occur following the report.
To carry out the investigation, the Committee can start a dialogue with the whistleblower, asking for clarification, documents, and additional information, through the IT platform or even in person; where necessary, the Committee may collect records and documents from other offices of the administration, ask for their support, involve third parties through audits and other requests, always being mindful of not compromising the protection of the confidentiality of the reporter and the reported. The latter can be addressed, upon their own request, even through paperwork proceedings through the acquisition of written observations and documents. The reported does not always have the right to be informed of the report regarding them, but can be informed only within the context of any proceedings being started against them following the conclusion of the management of the report and in case these proceedings are funded wholly or partly on the report.

Whenever, following the activities, the Committee ascertains elements of clear baselessness of the report, they dispose for the filing of the report with adequate reasoning. Wherever, on the other hand, the Committee deems the report legitimate, they immediately involve the Board of Directors

or external institutions, based on each entity's competence. Indeed, the Committee is not involved in the assessment of individual responsibilities of any nature, nor is it involved in verification of rightfulness or merit regarding acts or proceedings adopted by the Company object to the report.

Feedback can also simply be interlocutory, consisting in the communication of the information related to the aforementioned activities which the Committee intends to carry out and to the state of the investigation. In such case, at the end of the investigation, the Committee shall notify the findings to the reporter.

*Revision of internal procedures or processes*
In cases where a report did not imply the emergence of possible responsibility from the involved entities, but has highlighted some weaknesses or issues within internal processes, the Committee can ask for the revision of single procedures and, where necessary, the amendment of the Organisation, management, and control Model.

*Reports sent to a non-competent entity*
Whenever an internal report has been presented with different means than those detailed in this procedure to a different entity than the Committee, wherever the report explicitly declares that they want to benefit from protection in terms of whistleblowing or such intention is deductible from the report (e.g. a reference to the relevant regulation), this shall be considered a "whistleblowing report" and shall be transmitted to the Committee within seven days of receipt, contextually notifying transmission to the reporter. On the contrary, if the reporter does not explicitly declare that they want to benefit from protection, or such intention is not deductible from the report, this shall be considered an ordinary report.
In order to grant the management and traceability of the reports, the Committee drafts and updates all related information within the dedicated platform.
The archive for the filing of the documents – electronic and/or paper – related to reports received through different means than the ones provided, is exclusively kept by the Committee, in compliance with data protection regulation.

| **THE INTERNAL REPORTING CHANNEL** | |
|---|---|
| **Confidentiality** | TISG grants confidentiality:<br>- Of the reporter<br>- Of the enabler<br>- Of the person involved or the individuals mentioned in the report<br>- Of the contents of the report and related documentation |
| **Means of reporting** | Means of reporting are in electronic form (online platform) with cryptography instruments.<br>Alternatively, there is the possibility of reporting orally (meeting with the Committee) |
| **Management of the report** | The management of the report is assigned to a joint Whistleblowing Committee (Internal Audit + two members of the AB) |
| **Activities of the Committee** | - Provides to the reporter a notice of receipt of the report within seven days of the receipt date<br>- Maintains communication with the reporter<br>- Gives an appropriate follow-up to the received reports<br>- Provides feedback to the reporter |
| **Reports sent to an internal entity other than the Committee** | If the report is considered a "whistleblowing report" it has to be transmitted, within seven days from the receipt date, to the Committee, immediately providing notice of transmission to the reporter. |

## 5. USE OF AN EXTERNAL CHANNEL (ANAC)

The choice of the reporting channel is no longer attributed to the whistleblower's discretion, since **the use of the internal channel is favoured as a priority** and the appeal to an external report is possible at the following conditions:

| Conditions to resort to the ANAC external channel |
|---|
| **1) If the obligatory internal channel**<br>- is inactive<br>- is active, but it is not compliant with the provisions of the regulator regarding the entities and means of presenting reports |
| **2) if the person has already reported internally**, but has not received a follow-up |
| **3) the reporter has reasonable grounds to believe that if they make an internal report**<br>- the report would not receive an effective follow-up<br>- the report could imply a risk of retaliation |
| **4) the reporter has reasonable grounds to believe** that the violation may constitute an imminent or clear danger for the public interest |

*(Source: ANAC Guide Lines)*

For the means of reporting to the external channel, please refer to the information published by ANAC (https://www.anticorruzione.it/-/whistleblowing).

## 6. FORMS OF PROTECTION OF THE WHISTLEBLOWER

The reporter benefits of the protection described below only if, at the moment of the report, they acted in good faith, or if they had reasonable grounds to believe that the information on the reported violation were true.

| The protection system provided for in Legislative Decree 24/2023 includes: |
|---|
| **The protection of confidentiality** of the reporter, of the enabler, of the person involved and the persons mentioned in the report |
| **The protection from any retaliation** from the Company in reason of the report and the conditions of its applicability |
| **The limitations of responsibility** regarding the revelation and disclosure of certain categories of information which operate under certain conditions |

Protection measures are also applied to:

a) The enabler (individual who assists the reporter in the reporting process, operating within the same working environment and whose assistance shall be kept confidential);
b) The persons operating in the same working environment as the reporter which are linked by a stable emotional bond or family relationship within the fourth degree;
c) Colleagues of the reporter who work in the same context and have a habitual relationship with the reporter;
d) Entities owned by the reporter or for which the reporter works, as well as entities operating in the same working environment of the aforementioned persons.

### 6.1. Protection of confidentiality

TISG grants protection of the confidentiality throughout the compliance with the following principles:

- The identity of the reporter shall not be revealed to persons other than the entities competent to receive or follow through the reports
- The prohibition to reveal the whistleblower's identity does not only refer to the name of the reporter, but also to all elements of the report through which it is possible to find, even indirectly, the reporter's identity
- The reporter's identity is protected in the criminal, accounting, and disciplinary proceedings.
- The identities of the persons involved and the persons mentioned within the report, as well as the identity of the enabler assisting the reporter, are also protected through the use of cryptography instruments
- Confidentiality is granted even in cases in which the report, upon the reporter's request, is carried out by means of an in-person meeting with the Committee
- The reporter's confidentiality is protected even in cases which – for any reason – the report is received by personnel other than the Committee, to which, in any way, the report shall be transmitted without delay**.**

In the following cases, to reveal the reporter's identity, other than their explicit consent, a written communication of the reasons behind such revelation is requested:

- In the disciplinary proceedings, wherever the reveal of the reporter's identity is essential to defend the subject towards which disciplinary charges have been contested;
- In proceedings established following internal or external reports, wherever such revelation is essential even in defence of the individual involved.

The internal channel provides adequate measures for the management of the reports in order to protect the reporter's confidentiality, the report's contents and related documentation.

### 6.2. Protection of personal data

TISG ensures the protection of personal data not only to the reporter, but also to the other individuals to which protection of confidentiality is applied, including the enabler, the person involved and the person mentioned within the report, as persons concerned by treatment of data.

| **Qualifications of the entities treating personal data** | |
|---|---|
| **Data controllers** | - TISG for the internal channel<br>- ANAC for the external channel<br>- Other competent authorities to which reports are transmitted |
| **Data processors** | - External suppliers (e.g., the Company supplying the IT platform) |
| **Authorised persons** | - Persons who have been explicitly identified by TISG to handle and treat reports |

Data controllers, data processors, and authorised persons shall respect the following fundamental principles:

- Manage data in a legal, correct, and transparent way;
- Collect data with the sole purpose of managing and process the reports;
- Guarantee that the data is adequate, relevant, and limited to what is necessary for the purpose for which they are treated;
- Ensure that the data are correct and updated;
- Keep the data for the time necessary to the processing of the specific report (not over five years starting from the date of notice of the conclusion of the reporting procedure);
- Ensure treatment such that the confidentiality of personal data is granted, including the protection, through appropriate technical and organisational measures, from unauthorised or illicit treatment and from the loss, destruction, or accidental damage of data;
- Respect the principles of privacy by design and privacy by default;
- Carry out the impact evaluation on data protection;
- Provide to the possible concerned persons, *ex ante*, a policy regarding the processing of personal data through the publishing of informational documents (e.g., on the website, the platform, or brief policies regarding the use of oral means of reporting);
- Ensure the updating of the register of processing activities;
- Guarantee the prohibition of tracing reporting channels;
- Guarantee, where possible, the traceability of the activities of the authorised personnel in compliance with the guarantees of reporter's protection

*(Source: ANAC Guide Lines)*

The responsibility in case of violation of the discipline on personal data protection falls on:

- The data controller, where such violation is committed by the persons authorised or by the data processor;
- The data processor, in case such violation is committed by persons authorised by them.

In such cases, the Guarantor for personal data protection can adopt disciplinary measures and, if provided by law, apply monetary administrative sanctions. Such administrative sanctions are not applicable in relation to processing carried out in the judicial field. The same violations can, furthermore, fall under criminal law and lead to civil liability.
The persons involved or mentioned within the report, with reference to their personal data processed in the context of the report cannot exercise – for the time and limitation in which this constitutes a proportionate and necessary measure – the rights normally granted by EU Regulation 2016/679 to the concerned individuals (right to access personal data, right to rectify personal data, right to obtain cancellation of personal data or the so-called right to oblivion, right to limitation of processing, right to personal data portability and right of opposition to treatment). From the exercise of such rights could derive an effective and concrete prejudice to the protection of confidentiality of the reporter's identity.

Thus, in such cases, the possibility is precluded, for the reported individual or the person mentioned in the report, wherever they believe that the processing regarding them violates the aforementioned rights, to address the data controller and, in absence of answer from the latter, to propose a claim to the Guarantor of personal data protection.

### 6.3. Protection from retaliation

Any kind of retaliation, even **attempted** or **threatened**, is forbidden.

Retaliation is defined as: *"Any behaviour, action, or omission, even only attempted or threatened, carried out because of the report, the complaint to judicial or accounting authority, or of the public disclosure which causes or may cause unfair damages to the reporter or the person who made the complaint, directly or indirectly".*

Retaliation may show with actions, measures, behaviours, or omission which cause or may cause an unfair damage to the reporter, directly or indirectly.

It is necessary to have a link/strict connection between the report and the alleged retaliation.

The ANAC Guide Lines list, without limitation, the following retaliatory behaviour:

a) Termination, suspension, or equivalent measures;
b) Demotion or lack of promotion;
c) Change in functions, location, reduction of salary, change in working hours;
d) Suspension from training or any other restriction to training;
e) Demerit or negative references;
f) Adoption of disciplinary measures or other sanctions, even monetary;
g) Coercion, intimidation, harassment, or ostracism;
h) Discrimination or any unfavourable treatment;
i) Lack of conversion of a working contract at the end of a temporary contract into a permanent contract, wherever the worker had a legitimate expectation for the conversion;
j) Non-renewal or early termination of a temporary working contract;
k) Damages, even to the person's reputation, in particular on social media, or economic or financial prejudices, including the loss of economic opportunities and the loss of income;
l) Insertion in inappropriate lists on the basis of a sectorial or industrial agreement, formal or informal, which could imply the impossibility of the person to find employment in the sector or industry in the future;
m) Early termination or annulment of the supply contract of goods and services;
n) Annulment of a license or a permit;
o) Request of subjection to psychiatric or medial inspection.

The application of the system of protection against retaliation is subordinate to the following conditions:

1. The subject has reported on the basis of a **reasonable belief** that the information on the reported violations are **true and fall under the objective field of application of the decree**
2. The report has been carried out **in compliance with the discipline of Legislative Decree 24/2023**
3. A **relationship of consequentiality** between the report and the retaliatory measures experienced is necessary
4. Mere **suspicions** or **"rumours"** are **not sufficient**.

These conditions do not detect the certainty of the facts nor the personal reasons which led the subject to report.

In lack of these conditions:

- Reports do not fall under the whistleblowing discipline, thus the protection provided does not apply to the reporter;

- In the same way, the provided protection is excluded also for other subjects, which in reason of their role within the reporting process and/or the particular relationship with the reporter, are indirectly subject to retaliation.

*(Source: ANAC Guide Lines)*

Notice of retaliation, even attempted, or threatened, must be carried out **exclusively through ANAC**.
The latter evaluates the retaliatory behaviour connected to the report: wherever the reporter proves to have carried out a report and suffered a damage, it is assumed that such damage is a consequence of the report. In this case, the author of the alleged retaliation has the burden to prove that this is not connected to the report in any way. Such inversion of the burden of evidence does not work on the other subjects (enablers and other subjects operating in the same working environment and having a habitual and current relationship with the reporter).
Following the investigation, in case of assessment of the retaliatory nature of the measure, the latter is declared null and the sanctions described in § 8 are applied to the liable entity.

### 6.4. Limitation of responsibility

The reporter is granted limitation of responsibility with regards to the revelation and the disclosure of certain categories of information.

In particular, it is not considered liable whoever reveals or discloses information on violations:
- Covered by professional, scientific, and industrial secrecy obligation;
- Of loyalty and faithfulness duties;
- Related to copyright violations;
- Related to personal data protection;
- Which offend the reputation of the involved individual.

In order to give effect to limitation of responsibility, two conditions must cumulatively occur:
1) **Reasonable grounds**, at the moment of the revelation or disclosure of information, to believe that the revelation or disclosure is necessary to **highlight the violation**;
2) the report must be carried out **in compliance with conditions provided in Legislative Decree 24/2023**.

The reporter does not incur in any liability, even civil or administrative in nature, for the licit acquisition of information on the violation or the legal access to them.

Criminal liability and any other liability, even civil or administrative in nature, of the reporter is not excluded for behaviours, actions, or omissions not linked to the report or that are not strictly necessary to reveal the violation.

## 7. RESPONSIBILITIES OF THE REPORTER

Protection mentioned in §6.4 are not granted in cases where it is assessed, even with first instance judgement, the criminal liability of the reporter for crimes of libel or defamation, or their civil liability, for the same title, in cases of intent or gross negligence.
Therefore, this procedure is without prejudice to the criminal and disciplinary liability of the whistleblower, in the hypothesis of a libelous or defamatory report pursuant to the Criminal Cord and art. 2043 of the Italian Civil Code.

Sources of liability, furthermore, in a disciplinary setting or any other competent setting, all clearly opportunistic reports and/or reports carried out with the sole purpose of damaging the person reported or other subjects, and any other hypothesis of inappropriate use or intentional exploitation of the institution.

## 8. SANCTIONS

Pursuant to art. 21 of Legislative Decree 24/2023, without prejudice to the sanctions provided by the Disciplinary Code of the Company, ANAc applies to the liable party the following monetary administrative sanctions:

a) From 10,000 to 50,000 Euros when it assesses that the individual identified as the responsible party has executed retaliations;
b) From 10,000 to 50,000 Euros when it assesses that the individual identified as the responsible party has obstructed or attempted to obstruct the report;
c) From 10,000 to 50,000 Euros when it assesses that the individual identified as responsible party has violated the confidentiality obligation;
d) From 10,000 to 50,000 Euros when it assesses that there are no established reporting channels (in this case, the responsible party is considered the recipient body);
e) From 10,000 to 50,000 Euros when it assesses that no procedures have been adopted for the carrying out and the management of the reports, or that the adoption of such procedures is not compliant with the provisions of the decree (in this case, the responsible party is considered the recipient body);
f) From 10,000 to 50,000 Euros when it assesses that no verification or analysis activity has been carried out on received reports (in this case, the responsible party is considered to be the manager of the reports);
g) From 500 to 2,500 Euros when it is assessed, even with first instance judgement, civil liability of the reporting person for defamation or libel in cases of intent or gross negligence, unless they have already been condemned, even in first instance of judgement, for defamation or libel, or in any case for the same crimes committed with a complaint to the judicial authority.

## 9. INFORMATION AND TRAINING

The information on the use of the internal and external channel:

- Are exposed in the workplace in a visible point, accessible to all the aforementioned individuals;
- In a dedicated section of the Company's institutional website.

This procedure is examined in the courses and training sessions regarding the Organisation, Management, and Control Model *ex* Legislative Decree 231/2001.

## 10. FINAL DISPOSITIONS

For all issues not addressed by this procedure, please refer to provisions of Legislative Decree 24/2023 and article 6 of Legislative Decree 231/2001, as substituted by aforementioned Legislative Decree 24/2023.