Alberto Sassi S.p.A.

Whistleblowing Procedure

CONTENTS

[IN THIS DOCUMENT, FOR THE SAKE OF LINGUISTIC SIMPLICITY, THE USE OF "HE" IS intended to refer to all persons]

1. Purpose

This procedure was adopted by Alberto Sassi S.p.A. (hereinafter, the "Company") in compliance with the provisions of Italian Legislative Decree no. 24 of 10 March 2023 (hereinafter: Decree or "D.Lgs. 24/2023") which came into force on 30 March 2023, implementing Directive (EU) 2019/1937 of the European Parliament and of the Council dated 23 October 2019 (so-called whistleblowing directive), on the protection of persons who report breaches of national and Union law, harming the public interest or the integrity of the public administration or a private entity, they become aware of in a work-related context.

This procedure was validated by the CEO and will be ratified in the next meeting of the Board of Directors (hereinafter, the "BoD"), identifying the organisational roles involved in the management of whistleblowing reports and the related responsibilities.

In addition to the matters governed by this procedure, please also refer to the following section of the company website: Whistleblowing - Alberto Sassi

2. Field of application

This procedure applies to any information on breaches (as better specified in paragraph 4) acquired in a work-related context[1], harming the public interest or the integrity of the public administration or a private entity, and reported through specific reporting channels made available by the Company.

The following are excluded from the field of application of this procedure:

- **disputes, claims or requests linked to a personal interest relating exclusively to individual working relations, or work relations with superiors;**
- **breaches of national security, contracts relating to national security or defence;**

[1] Understood as a current or past employment relationship with or professional services provided to the organisation.

- **breaches mandatorily governed by Union or national laws[2] guaranteeing specific reporting procedures.**

3. References

- Legislative Decree No. 24 of 10 March 2023;
- Directive (EU) 2019/1937;
- European Regulation 2016/679 (GDPR);
- Privacy Code (D.Lgs. 196/2003 as amended);
- ANAC (National Anti-Corruption Authority, hereinafter "ANAC") Guidelines on the protection of persons reporting breaches of Union law and the protection of persons reporting breaches of national laws – procedures for the submission and management of external reports.

4. Definitions

- "**reports**": any oral or written communication, even in anonymous form, containing information on breaches;
- **"breaches"**: unlawful acts or omissions falling within the scope of major EU or national laws concerning public procurement, financial services, products and markets, prevention of money laundering, product safety and compliance, transport safety, protection of the environment, 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[3]; breaches (acts or omissions) affecting the financial interests of the EU (ref. Art. 325 of the TFEU); breaches (acts or omissions) of Union competition and State aid rules (ref. Art. 26(2) of the TFEU); breaches (acts or omissions) of corporate tax laws;
- "**information on breaches**": all information, including reasonable suspicions, concerning breaches committed or which, on the basis of concrete elements, could be committed in the organisation with which the reporting person or the person

[2] Refer to the annexes of Directive 2019/1937 and D.Lgs. 24/23.

[3] Refer to the annexes of Directive 2019/1937 and D.Lgs. 24/23.

making the report to the legal/accounting authorities holds a legal relationship as well as information concerning attempts to conceal such breaches;

- **"internal reporting**": transmission of "reports" using the established internal reporting channel;
- **"external reporting"**: oral or written communication of information on breaches submitted through external reporting channels[4];
- **"public disclosure"**: making of information on breaches available in the public domain, through the press or electronic means or in any case disclosure means that reach a large number of people;
- **"whistleblower":** a natural person who reports or publicly discloses information on breaches acquired in the context of his work-related activities;
- **"facilitator":** a natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential;
- **"work-related context":** current or past work activities through which, irrespective of the nature of those activities, a person acquires information on breaches and within which those persons could suffer retaliation if they reported or publicly disclosed such information to the legal or accounting authorities;
- **"person concerned":** 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;
- **"channel manager":** external party identified by the Company, in charge of managing the channel and the reports, with organisational and functional autonomy;
- **"internal contact person":** a person in the Company, identified by the administrative body, with whom the Channel Manager liaises during the whole report management process. If the internal contact person is the person concerned by the report, the role of internal contact person will be held by the administrative body;

[4] cf. art. 7, D.Lgs. 24/23

- **"retaliation":** any direct or indirect act or omission, even where only attempted or threatened, prompted by (and closely related to) reporting to a legal or accounting authority or by public disclosure, and which causes or may cause unjustified detriment to the reporting person;
- **"follow-up":** the action or actions taken by the person in charge of the reporting channel;
- **"feedback":** 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;
- **"platform":** internal reporting channel adopted by the Company (as better specified in paragraph 8) for transmitting information on breaches.

5. Responsibilities

The channel manager, also using the platform:

- makes available information, also through this procedure, the information published on the platform, clear information on the channel, the procedures and the assumptions for submitting internal reports;
- confirms the receipt of the report in the set times to the reporting person;
- assesses the criteria for being able to process the report;
- submits the report to the internal contact person, as defined in this procedure, and the SB (where required), and informs of the start of any investigations, their outcome and the feedback to provide to the whistleblower;
- provides feedback to the whistleblower on the closure of the report management process;
- maintains contact with the whistleblower and, if applicable, manages the request for additional information and any interviews with the whistleblower, if required;
- files and retains the reporting documentation for the period required by law;
- ensures compliance with the principle of confidentiality.

The internal contact person:

- identifies the persons in the Company to be involved and informs them of the analysis performed by the channel manager;

- is appointed to provide feedback to the channel manager on the decisions taken by the Company to investigate the reported matter;
- implements the recommendations given by the channel manager to investigate the reported matter;
- coordinates and monitors any investigations carried out with internal functions/appointed external teams;
- identifies improvement plans to prevent the recurrence of the reported matters;
- agrees with the channel manager on the start of any investigations, their outcome and the feedback to provide to the whistleblower;
- ensures that all information required on the channel, the procedures and the assumptions for submitting internal reports are made available on the company channels;
- with the support of the relevant company functions, manages the activities relating to any public disclosure, where required;
- ensures compliance with the principle of confidentiality.

The whistleblower:

- submits the reports in compliance with this procedure;
- is bound to provide substantiating information relating to the reported matter.

The legal representative:

- liaises with ANAC in the event of any external reports or to activate inspections by ANAC.

The BoD:

- approves this procedure along with the related organisational roles;
- ensures compliance with the protection measures for the reporting person.

6. Persons who may submit reports (so-called "whistleblower")

The following persons may submit reports:

- employees;
- contracted workers performing their activities for public and private entities;

- freelance workers;
- volunteers;
- consultants;
- shareholders;
- directors;
- providers of services to third parties for any reason (whatever the nature of such activity) against payment or otherwise;
- interns, salaried or otherwise;
- persons exercising administrative, managerial, control, supervisory or representational functions, even where the related activities are performed only in fact and not in law.

The category also includes all persons who, for any reason, become aware of criminal offences committed in the work-related context of the Company:

- before the start of the employment relationship;
- during the trial period;
- following termination of the relationship.

7. Internal contact person

The Company has appointed Rosario Cascino as the internal contact person pursuant to this procedure.

8. Internal reporting channel

The Company has established an internal reporting channel that the whistleblower must use to report information on the breaches. The establishment of this channel ensures a more effective prevention and verification of breaches. This choice responds to the principle of fostering strong communication and corporate social responsibility, and helps to improve its organisation.

The internal reporting channel offers both written and oral reporting methods, using the "@Whistleblowing" platform found at the link Whistleblowing - Alberto Sassi .

When accessing the platform, the whistleblower can use the voice mail system to request a direct meeting with the reporting manager.

The internal reporting channel ensures the confidentiality of the whistleblower, the facilitator (where present), the persons involved or in any case mentioned in the report, as well as the related contents and documentation submitted, at the time of the report or subsequently.

8.1 Party in charge of the channel management (so-called "channel manager")

The channel is managed by:

- BDO Advisory Services S.r.l., represented by Giuseppe Carnesecchi (giuseppe.carnesecchi@bdo.it), the specifically trained external party meeting the requirements of autonomy and independence.

The channel and reporting manager works exclusively to acquire the report and access the platform, with the exception of the case in which the report contains information relating to the activities undertaken by the auditing company "BDO Italia S.p.A." or to accounting matters; in these circumstances, the internal channel is managed by the Chairman of the Board of Auditors, Matteo Sanna.

8.2 Features of the internal reporting channel

The Company's internal reporting channel is managed by the web-based "Whistleblowing" platform which can be accessed from all devices (PC, Tablet, Smartphone).

The data entered on the platform are segregated according to the logical Company section and subjected to a scripting algorithm before archiving. The transmission safety is guaranteed by safe communication protocols.

After entering the report (whether anonymous or otherwise) the platform provides a non-reproducible 12-digit alphanumeric code, generated randomly and automatically by the IT platform, which the whistleblower can use at any time to view the processing status of the report and interact with the manager using the messaging tool.

If the report is not anonymous, the whistleblower's data ("user data") are not accessible to the channel manager. At its discretion, the channel manager may view these fields (so-called "cleartext fields") only following appropriately traced justification in the platform.

The report can be viewed and managed only by the channel manager. The manager's unique access credentials expire every 3 months. The password policy complies with international best practices.

Data Retention is governed according to set expiry dates with automatic reminders sent to the channel manager who deletes the data once expired.

BDO, the company providing the platform services, is certified to ISO27001.

The processing of personal data must always consider and comply with the obligations imposed by the GDPR and by D.Lgs. 196/2003 as amended. In its capacity as Controller, through the internal reporting channel the Company is bound to conduct a preliminary analysis of the organisational design including the fundamental assessment of the potential impacts on data protection (Art. 35, GDPR).

8.3 Features of reports and anonymous reports

The report must be as substantiated as possible in order to allow the persons in charge of receiving and managing the reports to analyse the facts. In particular, the following must be clear:

- the circumstances - time and place - in which the reported fact occurred;
- a description of the fact;
- the personal details or other elements used to identify the person to whom the reported fact is attributed.

Reported information on breaches must be truthful. Mere suppositions or unreliable indiscretions (so-called hearsay), information of public domain, incorrect information (with the exception of genuine error), clearly unfounded or misleading or merely harmful or offensive reports are not considered. However, the whistleblower does not have to be certain of the actual occurrence of the reported facts or the identity of their actual author.

It is also useful for the whistleblower to provide documents which can offer substantiated elements of the reported facts, as well as an indication of other persons potentially aware of the facts.

Where substantiated, anonymous reports are equivalent to normal reports and in this case, in the scope of this procedure, also with reference to the protection of the whistleblower, where subsequently identified, and to the retention obligations.

8.4 Report management process

The whistleblower submits the report on the specific internal channel.

The whistleblower initiates the report using the above-indicated link, in written form, completing a guided form, or in oral form using a voice message system.

If the whistleblower provides oral information during a meeting with the channel manager, with the consent of the whistleblower the information is documented by the channel manager, recording the interview on an oral recording device or by drafting a report. In the latter case, the whistleblower can check, correct and/or confirm the report of the meeting by signing it.

The report management process begins when the channel manager receives the report. The channel manager proceeds to "process" the report according to the set process flow chart.

On receipt of the report, the person in charge sends a receipt to the whistleblower within 7 days following receipt.

The report manager proceeds with an initial check of the correctness of the procedure used by the whistleblower and the contents of the report, both with reference to the field of application defined in this procedure (so-called pertinence of the contents of the report), and its verifiability on the basis of the information provided. If the report is not pertinent, the channel manager formalises the outcome of the checks and notifies the whistleblower within a reasonable time (no more than 3 months) and files the report. The manager promptly informs the internal contact person, ensuring compliance with the principle of confidentiality, who provides the information to the Company.

If additional elements are required, the channel manager will contact the whistleblower through the platform. If within 3 months following a request for additional information, the whistleblower does not provide such additional information, the channel manager proceeds to archive the report, notifying the whistleblower and the internal contact person.

Having checked the pertinence of the report and acquired all the elements, the channel manager, in compliance with the principle of confidentiality, informs the internal contact person.

On closure of the investigation, the internal contact person drafts a final report and submits the results to the channel manager in order to provide feedback to the whistleblower. Feedback must be sent to the whistleblower within three months following the date of the receipt notice, i.e., within seven days following the submission of the report. Only in exceptional cases, if required by the complexity of the report, or considering the whistleblower's response times, the channel manager, having promptly informed the whistleblower before the deadline, with appropriate justification, may continue the investigation for the required time, periodically updating the whistleblower.

The internal contact person will assess, on a case-by-case basis, with the Company if and which company function must be appropriately involved in the related analysis and for any consequent measures, again in compliance with the principle of confidentiality.

In the event of defamation or slander, confirmed even with a first-degree conviction, the Company proceeds with disciplinary action towards the whistleblower.

It is specified that, from the receipt of the report up to its closure, all persons in a conflict of interest must abstain from taking decisions in order to ensure the compliance with the principle of impartiality.

8.5 Transmission of reports submitted to wrong recipients

If the report is transmitted using means other than those illustrated in this procedure and is therefore **received by a person other than those in charge of receiving them, the recipient is bound to forward it within seven days to the party in charge at the e-mail address given in paragraph 8.1, informing the reporting person of the transmission and ensuring the chain of custody of the information** in compliance with the confidentiality obligations and those referred to in paragraph 8.2. The Company assesses disciplinary sanctions in the event of failure on the part of those wrongly receiving the report to comply with the transmission obligations.

If the report is involuntarily sent to persons other than the legitimate recipients, the whistleblower must demonstrate mere negligence and the absence of any personal interest in the incorrect sending.

8.6 Retention of internal reporting documentation

Internal reports and all related documentation annexed or provided subsequently are retained, with a specific digital chain of custody, for the time required to process the report.

In any case, the documentation is retained only for the identified time period up to a maximum of five years following the date of notification of the final outcome of the reporting procedure.

In all the mentioned cases, the procedure for retaining internal reports and the related documentation must comply with Union and national guarantees on the processing of personal data as well as the applicable confidentiality measures.

8.7 Information obligations

The information on the channel, the procedures and the assumptions for reporting can be found on the Intranet portal "InSassi" in the section "Company" →"Organisation and internal rules" → "Internal rules", in the Employee Portal and the company noticeboards. Furthermore, this information is made available in a specific section of the website, aiming to make it known to persons who, while not attending the work place, hold legal relations with the Company.

The Company establishes its own internal reporting channel having sought the opinion of the trade union representatives and organisations.

9. External reporting

In the following conditions, the whistleblower may submit a report to ANAC through an external channel:

- if, in the work-related context, the establishment of the internal reporting channel is not mandatory or the channel is not established or does not comply with the specified requirements;
- when the whistleblower has already submitted an internal report that has not be followed up;

- if the whistleblower has reasonable grounds for thinking that, by submitting an internal report, it would not be effectively followed up or that such report would lead to retaliation towards them;
- if the whistleblower has reasonable grounds to believe that the reported breach may constitute a clear or imminent danger to the public interest.

The body authorised to receive external reports is ANAC, in the appropriately adopted methods and procedures (Resolution no. 311 of 12 July 2023 - Guidelines on the protection of persons reporting breaches of Union law and the protection of persons reporting breaches of national laws. Procedures for the submission and management of external reports. - www.anticorruzione.it).

10. Public disclosure

In a residual and subordinate manner, the whistleblower may proceed with public disclosure in the following cases:

- when internal or external reports have already been made, or the matter has been reported externally without any feedback in the set times;
- if they have reasonable grounds to believe that the breach constitutes a clear or imminent danger to the public interest;
- when they have reasonable grounds to believe that the external report has a risk of retaliation or can have no effect due to the specific circumstances of the actual case, such as those in which proof may be concealed or destroyed or if it is reasonably feared that the person receiving the report may be colluding with the author of the breach or be involved in the breach itself.

11. Confidentiality obligation

All reports and the related annexes are not used beyond the time required to follow them up.

It is envisaged that the identity of the whistleblower along with any other information which could directly or indirectly reveal such identity may not be disclosed without the express consent of the whistleblower to persons other than those who are authorised to receive it or to follow up the reports, or are expressly authorised to process such information pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article 2(14) of the law on the protection of personal data, D.Lgs. 30 June 2003, no. 196.

The Company protects the identity of the persons concerned, the facilitators and the persons mentioned in the report until the conclusion of the proceedings following the report, in compliance with the same guarantees provided for the reporting person.

The circumstances mitigating the protection of the right to confidentiality include:

- within legal proceedings, the identity of the whistleblower is covered by secrecy obligations in the methods and limits provided for by Article 329 of the criminal code: the documents of the preliminary investigations are covered by obligations of secrecy up until the moment in which the suspect has the right to know, and in any case not beyond the closure of that phase;
- within proceedings before the Court of Auditors, the identity of the whistleblower may not be disclosed until the closure of the preliminary proceedings;
- within disciplinary proceedings, the identity of the whistleblower may not be disclosed if the dispute over the disciplinary action is based on separate investigations in addition to the report, even where this is a consequence of it;
- if the dispute is based wholly or partly on the report and the knowledge of the whistleblower's identity is indispensable for the accused's defence, the report can be used for the purpose of the disciplinary proceedings only with the express consent of the whistleblower to reveal their identity;
- in disciplinary proceedings towards the suspected author of the reported conduct, formal written notice will be sent to the whistleblower containing the reasons for the disclosure of the confidential data if the disciplinary is indispensable also for the defence of the person concerned.

Given the above-listed mitigations, the person concerned, at their request, may also be heard on a documentary basis, through the acquisition of written observations and documents.

The confidentiality obligations include:

- the removal of the report and the annexed documentation from the right of access to administrative documents provided for in Articles 22 et seq. of Italian law no. 241/1990 and generalised open access as referred to in Articles 5 et seq. of D.Lgs. no. 33/2013;

- the administrations and bodies involved in the management of reports guarantee confidentiality during all phases of the reporting proceedings, including any transfer of the reports to other competent authorities.

12. Protection of personal data

All personal data, including notifications between competent authorities, are processed according to:

- Regulation (EU) 2016/679;
- D.Lgs. no. 196 of 30 June 2003 as amended.

Personal data is communicated by European Union institutions, bodies and organisations in conformity with Regulation (EU) 2018/1725.

Personal data relating to the receipt and management of reports is processed by the Controller in compliance with the principles set forth in Articles 5 and 25 of Regulation (EU) 2016/679, firstly providing the appropriate information to the whistleblowers and persons concerned and adopting appropriate measures to protect the rights and freedoms of the data subjects.

The privacy policy, also summarising their rights and the methods for exercising them, can be found at Whistleblowing - Alberto Sassi .

13. Protection and support measures

Appropriate measures have been established to protect whistleblowers from direct and indirect retaliation.

The protection measures apply if, at the time of reporting, the reporting person had reasonable grounds to believe that the reported information on breaches was true (cf. paragraph 8.3), objective and that the reporting procedure was complied with.

In the event of defamation or slander, confirmed even with a first-degree conviction, these protections are not guaranteed.

The protection measures also apply to:

a) facilitators;

b) people in the same work-related context as the whistleblower/reporter bound by stable personal relations or kinship up to the fourth degree;

c) the work colleagues of the whistleblower/reporter working in the same work-related context who have habitual relations with them;

d) the bodies owned by the whistleblower/reporter or those for whom the same person works, as well as the bodies working in the same work-related context as the person.

13.1 Prohibition of retaliation

The recipients of the measures provided for the previous paragraph may not suffer any retaliation.

Acts in breach of the prohibition of retaliation are invalid.

Within legal or administrative proceedings or out-of-court disputes relating to the ascertainment of illegal conduct, acts or omissions towards whistleblowers, it is presumed that such conduct is due to the report. The burden of proving that such conduct or acts are justified by reasons beyond the report lies with the party performing the retaliation.

Whistleblowers may report any actual, attempted or threatened retaliation they believe they have suffered to ANAC.

ANAC informs the national labour inspectorate for the measures under their responsibility.

13.2 Support measures

The whistleblower may contact third-sector bodies included in the list published on the ANAC website. These bodies perform activities of general interest for the pursuit, not for profit, of civic, social utility and charitable purposes ("*promotion of the culture of legality, peace amongst peoples, non-violence and unarmed defence; promotion of human, civil, social and political rights, as well as the rights of consumers and users of activities of general interest, promotion of equal opportunities and mutual help initiatives, including time banks and ethical purchasing groups*") which have signed agreements with ANAC.

The support measures consist of the free provision of information, assistance and advice on reporting methods and protection against retaliation available through the

provisions of national and Union law, on the rights of the person concerned as well as the methods and conditions of access to state-funded legal aid.

13.3 Limitation of liability of the whistleblower

There is no liability (including civil or administrative liability) for anyone disclosing information on breaches:

- covered by the obligation to secrecy,
- relating to the protection of copyright,
- on the provisions concerning the protection of personal data,
- offending the reputation of the person concerned or reported,

if, at the time of reporting, there were reasonable grounds for believing that the reporting of such information was necessary to disclose the breach and the report was made consistently with the conditions for protection.

Furthermore, the protection measures also include:

- that the right to submit a report and the related protections may not be limited contractually or by agreement;
- the exclusion of all other liability, including civil or administrative liability, for acquiring or having access to information on breaches, unless such conduct is a criminal offence;
- the exclusion of all other liability in relation to conduct, acts or omissions where connected to the reporting and strictly necessary for disclosing the breach, or in any case not connected to the reporting.

14. Sanctioning regime

The Company will adopt the disciplinary and compensation measures provided for in the current national bargaining contract in force for the private metal engineering industry - Federmeccanica, as well as all permitted civil and criminal actions, towards those who the Company ascertains to be responsible for offences relating to:

- the commission of or proposed retaliation, actual or attempted hindering of reporting of breach of the confidentiality obligations;

- failure to establish the reporting channels, failure to adopt procedures for their management, or the adoption of procedures that do not comply with the requirements of the decree or failure to check and analyse the reports;
- civil liability of the whistleblower, confirmed even with a first-degree conviction, for defamation or slander in cases of wilful misconduct or gross negligence, unless they have already been convicted, even in first degree, for crimes of defamation or slander;
- towards anyone breaching this procedure.

If these offences are confirmed, ANAC may apply an administrative fine (€500 to €50,000).

Annexes

Italian Legislative Decree No. 24 of 10 March 2023 Official Journal or Whistleblowing - Alberto Sassi