WHISTLEBLOWING POLICY

(pursuant to Legislative Decree 24/2023)

Approved on **14/12/23**

1. NORMATIVE AND DOCUMENTARY REFERENCES

- Legislative Decree 10 March 2023 No 24 of '*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws*';

- Directive (EU) 1937/2019 on '*The protection of persons who report breaches of Union law*';

- Regulation (EU) 2016/679 on '*the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)*';

- Law No. 179/2017, containing '*Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship*';

- "*Guidelines on the protection of persons who report violations of Union law and protection of persons who report violations of national laws. Procedures for the submission and management of external reports*" (ANAC - Approved by resolution no. 311 of 12 July 2023);

- Confindustria '*New Discipline* <<Whistleblowing>> *Operational Guide for Private Entities*' (October 2023);

- Legislative Decree No. 231 of 8 June 2001 on '*The regulation of the administrative liability of legal persons, companies and associations, including those without legal personality*' in its current content;

- "*Guidelines for the construction of Organisation, Management and Control Models, pursuant to Legislative Decree No. 231 of 8 June 2001*" issued by Confindustria and updated in June 2021;

- Organisation, Management and Control Model adopted by Società Agglomerati Industriali Bosi S.p.A., pursuant to Legislative Decree No. 231/2001 in the edition in force from time to time;

- Code of Ethics adopted by Società Agglomerati Industriali Bosi S.p.A. in the edition in force from time to time;

- Company Policies and Procedures in force from time to time.

2. PURPOSE AND AIM

Società Agglomerati Industriali Bosi S.p.A. (hereinafter, for the sake of brevity, the "**Company**") has adopted a "*Whistleblowing*" system (hereinafter also "**Whistleblowing**"), in order to be able to promptly and effectively identify and counter possible unlawful or irregular conduct, with the aim of spreading a culture of ethics, legality and transparency within its corporate organisation.

The purpose of this Policy is to provide clear information on the channel, procedures and prerequisites for making internal reports, as well as on the channel, procedures and prerequisites for making external reports, pursuant to Legislative Decree 24/2023, and to implement the provisions of the Organisation, Management and Control Model and the Code of Ethics already adopted by the Company.

3. ENTITLED PARTIES AND SUBJECT OF THE REPORT

3.1 Persons entitled to report

Pursuant to Legislative Decree 24/2023, the following categories of persons may make a Report:

- Employees or Collaborators;
- Suppliers, subcontractors and their employees and collaborators;
- Freelancers, consultants, self-employed;
- Volunteers and trainees, paid or unpaid;
- Shareholders or persons with administrative, management, supervisory, control or representative functions;
- Former employees, former collaborators;
- persons who no longer hold one of the positions indicated above if the information on violations was acquired in the course of the report itself;
- Persons undergoing selection, probation or whose legal relationship with the organisation has not yet begun.

3.2 Behaviour, acts or omissions to be reported

Pursuant to Legislative Decree no. 24/2023, conduct, acts or omissions (hereinafter referred to as 'breaches') detrimental to the interest or integrity of the Company and consisting of

1) administrative, accounting, civil or criminal offences that do not fall under (3), (4), (5) and (6);

2) unlawful conduct relevant pursuant to Legislative Decree No. 231 of 8 June 2001, or violations of the Organisation and Management Model adopted by the Company pursuant to the aforementioned legislation and which do not fall under numbers 3), 4), 5) and 6);

3) offences falling within the scope of the European Union or national acts set out in the Annex to this Decree or national acts constituting implementation of the European Union acts set out in the Annex to Directive (EU) 2019/1937, although not set out in the Annex to this Decree, relating to the following areas: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and security of networks and information systems;

4) acts or omissions affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union specified in the relevant secondary law of the European Union;

5) acts or omissions relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including infringements of EU competition and State aid rules, as well as infringements relating to the internal market related 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 law;

6) acts or conduct that frustrate the object or purpose of the provisions of Union acts in the areas indicated in (3), (4) and (5).

3.3 Actions, facts and conduct that cannot be reported

It should be noted that the Whistleblowing tool must not be used to offend or harm the personal and/or professional honour and/or decorum of the person or persons to whom the reported facts are referred, or to knowingly disseminate unfounded or malicious allegations.

In particular, and by way of example but not limited to, **it is** therefore **prohibited**:

(i) the use of insulting or denigrating expressions;

(ii) sending Reports for purely defamatory, slanderous, revengeful or otherwise malicious purposes;

(iii) sending Reports of a discriminatory nature, insofar as they refer to sexual, religious or political orientation or to the racial or ethnic origin of the Reported Subject;

(iv) the sending of Reports made for the sole purpose of harming the Reported Subject.

Reports are also excluded from the scope of this policy:

- linked to a personal interest of the Whistleblower, relating to his/her individual employment relationships, or inherent to employment relationships with hierarchically superior figures (e.g. labour disputes, discrimination, interpersonal conflicts between colleagues, reports on data processing carried out in the context of the individual employment relationship in the absence of an infringement of the public interest or of the integrity of the private body or public administration);
- in matters of security and national defence;
- relating to violations already compulsorily regulated in certain special sectors.

4. INTERNAL SIGNALLING CHANNEL

4.1 Internal Signalling Channel

SAIB provides an internal reporting channel divided into **WRITTEN REPORTS AND ORAL REPORTS**.

WRITTEN REPORT
(A. COMPUTER PLATFORM AND B. PAPER REPORTING)

A. The Company provides a specific IT platform (**the My Whistleblowing add-on to the My Governance software).**

This platform is managed by the Reporting Manager, as indicated below.

The aforementioned platform stores the data in a fully encrypted manner, ensuring that access to it is permitted only to those expressly authorised by the company.

Through the Platform it is also possible to send Anonymous Reports[1]. Even in the case of anonymous Reports, contact between the Reporting Party and the persons entrusted by the Company with the management of Reports is guaranteed.

In any case, in order to enable the most complete and accurate management possible, the Report must contain the following minimum information:

(i) a clear and complete description of the facts that are the subject of the report;

(ii) the circumstances of time and place in which the facts that are the subject of the report were committed;

(iii) personal details or other elements allowing the identification of the person(s) who has/have carried out the reported facts (e.g. job title, place of employment where he/she carries out the activity);

(iv) any documents supporting the report;

(v) an indication of any other persons who may report on the facts being reported;

(vi) any other information that may provide useful feedback on the existence of the reported facts.

Through the IT channel and thus through the software, the reporting person is guided through each stage of the reporting process and will be asked, in order to better substantiate the report, to fill in a series of fields that must be completed in accordance with the requirements.

It is indispensable that the elements indicated are known directly to the reporter and not reported or referred to by others.

B. The **written report in paper format (letter)** should be sent to the following address

"Whistleblowing Manager
at SAIB S.p.A.
Via Caorsana 5/A - 29012 Caorso (PC)

The '**Whistleblowing Manager**' is a multi-subjective body composed of:

- SAIB's Supervisory Board;
- Head of SAIB's Prevention and Protection Service;
- HR Manager of SAIB. It

should be noted that:

- the Report must be placed in a **sealed envelope**[2] **marked** on the outside **"confidential to the** Whistleblower**"** so as to expressly indicate the wish to benefit from the Whistleblowing protections;
- the recording of the report is reserved exclusively, also by means of an independent register, for the Reporting Manager.

[1] It should be pointed out that in the event of a Report that does not indicate the identity of the reporter, the identity of the reporter could possibly be inferred from the circumstances set out in the Report.

[2] As provided for in the ANAC Guidelines, if the Report is not anonymous, it must be submitted in two sealed envelopes: the first, with the identification data of the Reporting Party (together with a photocopy of the identification document), the second, with the

Report (so as to separate the identification data of the Reporting Party from the Report). Both envelopes should then be placed in a third sealed envelope marked 'reserved for the Reporting Manager' on the outside.

ORAL REPORT

(A. COMPUTER PLATFORM AND B. MEETING WITH THE MANAGER)

It is also possible to make **oral reports** to the Manager. Specifically, it is possible:

A. submit an **oral report via the platform**

The system allows the management of voice alerts. By means of this module, the signaller is enabled to **record a voice message** with **a** maximum duration of 5 minutes **on the system**. The voice message is then processed by the system functions in such a way that a transformation is performed on the recorded voice, altering its characteristics so that it is not recognisable.

The message is then transmitted to the manager, who, after listening to it, will complete the report with the data necessary for storing the new report.

The new alert is highlighted in the system interface with a specific graphic sign.

B. request a **direct meeting with the Reporting Manager**. In that case, please note that:

1. The meeting must take place in a suitable place to ensure the confidentiality of the reporter and within a reasonable time (within 15 working days);

2. the Whistleblower must expressly state that he/she wishes to benefit from the Whistleblowing protections;

3. the Manager must provide the Reporting Officer with the information on the processing of personal data and the necessary indications to find the full text of this information online;

4. the Manager must record the content of the Report in a report (which the Reporting Party may verify, rectify and confirm by its own signature).

In the event of a **conflict of interest** (i.e. where the Reporting Manager coincides with the Reporting Party, with the reported person or is in any case a person involved in or affected by the Reporting), the Report may be addressed to senior management or to another person/office that can guarantee its effective, independent and autonomous management, always in compliance with the confidentiality obligation laid down by the rules.

Where an internal Whistleblowing **Report is submitted to a person other than the "Manager"** and it is clear that it is a Whistleblowing Report, within the meaning of this Policy (e.g. because the words "Confidential to the Whistleblowing Manager" are explicitly stated), it must be forwarded (without retaining a copy), within seven days of its receipt to the Whistleblowing Manager.

In any case, the Reporting Manager must:

a) issue the **Reporting** Officer with **an acknowledgement of receipt of the Report within seven days of** its receipt;

b) liaise with the reporter and request additions from him/her, if necessary;

c) diligently follow up on Reports received;

d) **provide a reply to the Report within three months from the date of the acknowledgement of receipt** or, in the absence of such notice, within three months from the expiry of the period of seven days from the submission of the Report[3].

4.2 Examination and investigation

Once the Report has been received, the Manager must verify the **admissibility of** the report in the light of the subjective scope of application (whether the Reporting Party is among the persons entitled, pursuant to Legislative Decree 24/2023) and the objective scope of the Decree (whether the breach falls within those provided for by Legislative Decree 24/2023).

After verifying that the report meets the subjective and objective requirements defined by the legislator, it is necessary to assess its **admissibility** as a whistleblowing report. For instance, a whistleblowing report cannot be considered admissible for the following reasons:

- lack of data constituting the essential elements of the alert;
- manifest groundlessness of the facts attributable to the infringements typified by the legislator;
- presentation of facts of such general content that they cannot be understood;
- production of documentation only without the actual reporting of violations.

In the event that the report is inadmissible or inadmissible, the Reporting Manager may proceed to file it, while ensuring the traceability of the supporting reasons.

Once the admissibility and admissibility of the report has been verified, the Manager starts **the investigation**
on the facts and conduct reported in order to assess their justification.

The purpose of the preliminary investigation phase is to proceed with the specific checks, analyses and assessments as to whether or not the reported facts are well-founded, also in order to formulate any recommendations regarding the adoption of the necessary corrective actions on the corporate areas and processes concerned with a view to strengthening the internal control system.

Since the Reporting Manager is the Supervisory Board in monocratic composition, it may request the support of the corporate functions (in compliance with the confidentiality obligations required by law[4]) or of specialised external consultants, in view of the specific technical and professional skills required.

Once the investigation has been completed, the Reporting Manager may:

- file the report as unfounded, stating the reasons;
- declare the report well-founded and refer it to the competent internal bodies/functions for the relevant follow-up (e.g. company management, human resources, etc.). It should be noted, in fact, that the reporting manager is not responsible for any assessment of individual responsibilities and any subsequent measures or proceedings.

---

3 It should be noted that it is not necessary to conclude the assessment activity within the three-month period, considering that there may be cases that require a longer period of time for verification purposes. Therefore, it is a finding that, at the expiry of the time limit indicated, may be final if the investigation is completed or of an interlocutory nature on the progress of the investigation, which has not yet been completed.

4 To this end, any type of data that might allow the identification of the reporting person or of any other person involved must - for example - be obscured. In any case, the confidentiality obligations expressly provided for in this Policy and in the Organisational, Management and Control Model adopted by the Company pursuant to Legislative Decree No. 231/2001 shall also be extended to these persons.

After the expiry of three months from the date of the acknowledgement of receipt (or - in the absence of such notice - within three months from the date of expiry of the seven-day time limit for such notice), the Reporting Manager may notify the Reporting Officer:

- the filing of the report, stating the reasons;
- whether the report is well-founded and forwarded to the competent internal bodies;
- the activity carried out so far and/or the activity it intends to carry out.

5. EXTERNAL SIGNALLING CHANNEL

The Whistleblower may make an external report to the National Anti-Corruption Authority 'ANAC' if, at the time of its submission, one of the following conditions is met:

a) there is no provision for the mandatory activation of the internal reporting channel within the working context[5] , or this channel, even if mandatory, is not active or, even if activated, does not comply with the reference legislation;

b) the reporting person has already made an internal report under the relevant legislation and the report has not been followed up;

c) the reporting person has reasonable grounds to believe that, if he or she were to make an internal report, the report would not be effectively followed up or that the report might give rise to the risk of retaliation;

d) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest

6. PUBLIC DISCLOSURE

The whistleblower may make a public disclosure (i.e. make information about violations publicly available through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people) if one of the following conditions is met:

a) the reporting person has previously made an internal and an external report or has made an external report directly and no reply has been received within the prescribed time limits as to the measures envisaged or taken to follow up the reports;

b) the person issuing the alert has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;

c) the reporting person has reasonable grounds to believe that the external report may involve a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there is a well-founded fear that the recipient of the report may be colluding with or involved in the perpetrator of the violation.

7. CONFIDENTIALITY

[5] A work context refers to present or past work or professional activities through which, irrespective of the nature of such activities, a person acquires information about violations and in the context of which he or she could risk retaliation in the event of a public disclosure or report to a judicial or accounting authority.

Alerts may not be used beyond what is necessary to adequately follow them up.

The identity of the reporting person and any other information from which this identity may be inferred, directly or indirectly, cannot be disclosed, without the express consent of the reporting person himself/herself, to persons other than those competent to receive or follow up the reports and expressly authorised to process such data.

In criminal proceedings, the identity of the reporting person is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure.

In proceedings before the Court of Auditors, the identity of the reporting person may not be revealed until the investigation phase is closed.

In the context of disciplinary proceedings, the identity of the reporting person may not be disclosed, where the disciplinary charge is based on investigations that are separate from and additional to the report, even if consequent to it. Where the disciplinary charge is based, in whole or in part, on the report and knowledge of the identity of the person making the report is indispensable for the accused "s defence, the report shall be usable for the purposes of the disciplinary proceedings only if the person making the report expressly consents to the disclosure of his/her identity.

The reporting person shall be notified in writing of the reasons for the disclosure of confidential data, as well as in the reporting procedures when the disclosure of the identity of the reporting person and of the information is also indispensable for the defence of the person concerned.

The person concerned may be heard, or, at his or her request, shall be heard, also by means of a cartel procedure through the acquisition of written observations and documents.

8. PROCESSING OF PERSONAL DATA

Any processing of personal data, including communication between competent authorities, must be carried out in accordance with Regulation (EU) 2016/679, Legislative Decree No 196 of 30 June 2003 and Legislative Decree No 51 of 18 May 2018. The communication of personal data by the institutions, bodies, offices or agencies of the European Union shall be made in accordance with Regulation (EU) 2018/1725.

Personal data that are clearly not useful for processing a specific alert are not collected or, if accidentally collected, are deleted immediately.

The processing of personal data relating to the receipt and handling of reports shall be carried out in compliance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679 or Articles 3 and 16 of Legislative Decree No 51 of 2018, providing appropriate information to the reporting persons and the persons concerned pursuant to Articles 13 and 14 of the same Regulation (EU) 2016/679 or Article 11 of the aforementioned Legislative Decree No 51 of 2018, as well as taking appropriate measures to protect the rights and freedoms of the persons concerned.

9. PROHIBITION OF RETALIATION AGAINST THE REPORTER

No **form of retaliation** or **discriminatory measure** directly or indirectly linked to the Whistleblowing is allowed or tolerated against the Whistleblower. Retaliation constitutes, for instance:

a) dismissal, suspension or equivalent measures;

b) relegation in grade or non-promotion;

c) change of duties, change of workplace, reduction of salary, change of working hours;

d) suspension of training or any restriction of access to it;

e) negative merit notes or negative references;

f) the adoption of disciplinary measures or other sanctions, including fines;

g) coercion, intimidation, harassment or ostracism;

h) discrimination or otherwise unfavourable treatment;

i) the failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion;

l) non-renewal or early termination of a fixed-term employment contract;

m) damage, including to a person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;

n) 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;

o) early termination or cancellation of the contract for the supply of goods or services;

p) cancellation of a licence or permit;

q) the request to undergo psychiatric or medical examinations.

10. RESPONSIBILITY OF THE REPORTER

The Policy is without prejudice to the **liability**, including disciplinary **liability**, of the **Whistleblower** in the event of a report made with malicious intent or gross negligence or in any event a report made for defamatory purposes.

Any abuse of this Policy, such as Reports that are manifestly opportunistic and/or made for the sole purpose of harming the Accused or other persons, and any other hypothesis of misuse or intentional exploitation of the institution covered by this Policy, shall also give rise to disciplinary liability.

Where the criminal liability of the reporting person for offences of defamation or slander or, in any case, for the same offences committed with the report to the judicial or accounting authorities or his civil liability, for the same reason, in cases of wilful misconduct or gross negligence, is established, even by a judgment of first instance, the protections provided for by this Policy are not guaranteed and a disciplinary sanction is imposed on the reporting or whistleblowing person.

11. TRACEABILITY AND ARCHIVING

The Reporting Manager is required to document the Reports received, in order to ensure full **traceability** of the actions taken to fulfil its institutional functions.

All documents collected and/or processed in the context of this Policy shall be retained for as long as necessary for the processing of the report and, in any event, no longer than five years from the date of the communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set out in Article 12 of Legislative Decree 24/2023 and the principle set out in Article 5(1)(e) of Regulation (EU) 2016/679 and Article 3(1)(e) of Legislative Decree No. 51 of 2018.

If the **recorded voice messaging system** is used **for** the report, the report, subject to the consent of the person making the report, is documented by the **Reporting Manager** either by recording it on a device suitable for storing and listening to it, or by means of a verbatim transcript. In the case of a transcript, the reporting person may verify, rectify or confirm the content of the transcript by signing it.

When, the report is made orally during a **meeting with** the **Reporting Manager,** it is, with the consent of the person making **the** report, documented by the **Reporting Manager** either by recording it on a device suitable for storing and listening to it, or by minutes. In the case of minutes, the person issuing the alert may verify, rectify and confirm the minutes of the meeting by signing them.

This Policy, drafted in compliance with the requirements set out in the legislation in force and the values set out in the Code of Ethics, forms an integral part of the Organisation, Management and Control Model adopted by the Company.

12. SANCTIONS

The Company shall impose appropriate sanctions (varying according to the person involved) on those who are responsible for the conduct set out below by way of example:

- retaliation or obstruction (including in the form of attempt) of reporting;
- breach of the obligation of confidentiality with regard to the identity of the reporter;
- adoption of procedures that do not comply with the applicable legislation;
- failure to verify and analyse reports received;

Lastly, the Company shall impose sanctions when the criminal liability of the reporting person for offences of defamation or slander or, in any case, for the same offences committed with the report to the judicial or accounting authorities or his civil liability, for the same reason, in cases of wilful misconduct or gross negligence, is established, even by a judgment of first instance.