WHISTLEBLOWING

REPORT MANAGEMENT AND WHISTLEBLOWER PROTECTION POLICY

Amer Group

| 2023

amergroup.com

REPORT MANAGEMENT AND WHISTLEBLOWER PROTECTION POLICY

AMER GROUP

Rev.	Prepared by	Dated
01	I Issued by the General Counsel Department	03/11/2023
02	I Reviewed by the Human Resources Department	10/11/2023
03	II Reviewed by the IT Department	17/11/2023
04	III Reviewed by the Executive Management	30/11/2023

Process	Assessed by	Approved by
01	– Directors / Auditors	B.o.D. Amer S.p.A.
02	– Directors / Auditors	B.o.D. Italsea Ltd.
03	- Directors / Auditors	B.o.D. SIR S.r.l.
04	- Directors / Auditors	B.o.D. NSM S.r.l.
05	– Directors / Auditors	B.o.D. B&S GmbH

TABLE OF CONTENT

TABLE OF CONTENT

TITLE I - GENERAL PROVISIONS

1. PURPOSE

Amer S.p.A. and the other Companies belonging to the Amer Group (hereinafter also only "**Group**" or "**AG**") conduct their business with loyalty, fairness, transparency, honesty, integrity and in compliance with laws, regulations and rules as well as standards and guidelines applicable to their business.

Therefore, AG – in order to foster a culture of good communication and corporate social responsibility within the organizations – adopts tools aimed at preventing, discovering and reporting unlawful conducts put in place in breach of binding and internal regulations, as well as of the ethical principles promoted by the Group, and encourages its employees, shareholders, as well as individuals who – in any capacity – perform or have performed work for the Group or hold administrative, management, control, supervisory or representative positions to report any relevant conduct, act or omission under this procedure and of which they become aware.

The purpose of this Policy – pursuant to the Legislative Decree implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 – is to regulate the channels for reporting unlawful breaches or irregularities and to remove factors that may hinder or discourage reporting, as well as to regulate measures to protect whistleblowers and the disciplinary system.

2. DEFINITIONS

NATIONAL ANTI-CORRUPTION AUTHORITY (ANAC): pursuant to Legislative Decree no. 24/2023, it is the authority in charge of managing external reporting channels.

AG or **GROUP:** it includes Amer S.p.A., the companies in which Amer has significant holdings and the Companies subject to Amer's management and control.

ACCESS CODE: it means the access code – unique for all Recipients of this Policy – provided to access the Reporting System.

ETHICAL CODE: document outlining the values and reference principles that govern the business and relations towards all parties the Group establishes relations with for the achievement of its corporate purpose.

REPORTING COMMITTEE: (hereinafter also just "R.C.") the Reporting Committee is appointed by the administrative body of the holding company and is the collegial Body responsible for the reporting management process. It is composed of one person from the Group's HR Department (who also acts as Reporting Manager), as well as a male or female Director of AG's holding company, delegated to control the regularity of the Group's conduct with regard to transparency, anti-corruption and protection of confidentiality, and a male or female Director of each subsidiary company to which this Policy applies. The total number of members of the Committee will always be odd. The Group's General Counsel Department also joins in the works of the Committee as Administrative Secretary and support for the correct application of the procedures governed by law. However, the Committee Secretary does not take part in the decision-making phase of the body. The names of the persons holding the above-mentioned offices are made known to the Recipients in the same ways of communication as adopted for the dissemination of this Policy.

The Committee oversees the assessment of reports and their processing, also distinguishing between non-relevant reports or those that should simply be reallocated to internal functions as they do not fully qualify as significant reports for the purposes of the whistleblowing legislation.

RECIPIENTS: it shall mean AG's People, as well as third parties, natural or legal persons, (including, without limitation, suppliers, self-employed and freelance professionals, consultants or customers, and other persons who have contractual relations with one of the Companies belonging to the Group as collaborators, business partners, joint venturers and/or - in any case - of anyone acting in the name, on behalf or in the interest of the Group). Specifically, this includes all the individuals under art. 3 of Legislative Decree no. 24/2023.

FACILITATORS: it shall mean those individuals, natural persons, working in the same work environment as the Reporting Person and who have provided/are providing assistance to the Reporting Person in the reporting process.

ALTERNATIVE MANAGER: it is also a collegial body responsible for carrying out the same activities as the R.C. and is involved whenever a report directly or indirectly concerns a Committee member. The Manager members are appointed by the holding company and their number will also always be odd.

AG PEOPLE: all legal representatives, partners, directors, managers, employees (whatever the legal and contractual classification of the work performed, including trainees and volunteers) and members of supervisory bodies of Group companies.

INTERNAL PROCEDURES: all the procedures, policies, operating instructions and all the other documents that are part of the company's regulatory system.

REPORTING MANAGEMENT DEPARTMENT: it is the Department composed of the male and/or female HR Managers of the Group which is entrusted with the task of ensuring the performance of the reporting process in accordance with the regulations in force.

EXTERNAL REPORTING: reporting carried out through the channels managed by ANAC and to which private entities can resort under the conditions provided for by Legislative Decree 24/2023.

RELEVANT INTERNAL REPORTING: any communication - made through the reporting channels arranged pursuant to this Policy - having to do with the reasonable and legitimate suspicion or awareness of unlawful conduct, acts or omissions laid down in the following paragraph "*Subject and content of reports*", carried out by AG People, and which harm the public interest or integrity of the Group Companies.

UNLAWFUL REPORTING: a report that, from the results of the preliminary verification and on the basis of objective elements, is found to be unfounded and with respect to which the established circumstances permit to believe that it was made in bad faith or wilful misconduct or gross negligence.

SENSITIVE INDIVIDUALS RELATED TO THE REPORTING PERSON: pursuant to Legislative Decree 24/2023, these are defined as facilitators of the Reporting Person, persons related to the Reporting Person by a stable emotional relationship or relatives within the fourth degree of kin and operating in the same work context, colleagues of the Reporting Person, entities owned by the Reporting Person or operating in the same work context. The same protection measures provided for the Reporting Person extend to these individuals.

REPORTING SYSTEM OR SYSTEM: The multichannel system for receiving and handling the reports covered by this Policy.

REPORTING PERSON (hereinafter Whistleblower): the person who, because of a relationship of interest with AG, witnesses or has reasonable cause to believe that an offence or irregularity has been committed in the workplace and proceeds to report it. Eligible subjects for reporting are top management[1], employees (of

[1] "Top management" shall mean: the members of the Board of Directors, the Board of Statutory Auditors, the Chief Executive Officer, as well as any other person in a senior position who holds representative, administrative, or managerial positions in a Company belonging to AG Group.

any category: fixed-term, permanent, executives, interns etc.), collaborators, consultants, business partners, and all persons referred to in art. 3 of Legislative Decree No. 24/2023 implementing EU Directive 2019/1937 (by virtue of which employees of public administrations or independent administrative authorities of guarantee, supervision or regulation may also be included in the notion of Whistleblower).

3. SCOPE

This Policy applies to the following AG Group Companies: Amer S.p.A., Italsea Ltd., SIR S.r.l., NSM S.r.l., Baumeister & Shack GmbH & Co. KG.
Within these Companies, the Policy applies to all directors, members of supervisory bodies, employees and collaborators of Group Companies, non-subsidiaries in which a Group Company holds significant shareholdings, joint ventures and/or - in any case - anyone acting in the name of, on behalf of or in the interest of AG (by way of example: consultants, suppliers, agents etc.), as specified in the definition of "Recipients".

4. MAIN REGULATORY REFERENCES

Binding Legislation

- Italian Civil Code;
- Italian Criminal Code;
- Law no. 287/1990 "*Rules for the Protection of Competition and the Market*";
- Legislative Decree no. 231/2001 "*Rules governing the administrative liability of legal persons, companies and associations, including those without legal personality*";
- Law 179/2107 "*Provisions for the protection of people reporting crimes or irregularities of which they have become aware in the context of a public or private employment relationship*";
- Legislative Decree No. 101/2018 "*Provisions for the adaptation of national legislation to the provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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)*";
- Legislative Decree no. 196/2003 "*Personal Data Protection Code*" - Supplementing Legislative Decree 101/18;
- EU Regulation 679/2019 "*General Data Protection Regulation*";
- EU Directive 2016/680 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA;
- Law no. 179/2017 "*Provisions for the protection of the people reporting crimes or irregularities of which they have become aware in the context of a public or private employment relationship*";
- Legislative Decree no. 24/2023 "*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*";
- *ANAC Guidelines approved by resolution no. 311 of 12 July 2023 "On the protection of persons who report breaches of Union law and protection of persons who report breaches of national regulatory provisions. Procedures for the submission and management of external reports".*

Internal regulations

- Group-wide Ethical Code;
- Organizational documents (e.g., internal proxies, power of attorney, power map etc.) in force in AG Group Companies.

5. POLICY ADOPTION AND DISSEMINATION

This Policy is granted the widest possible dissemination.

To this end, it is in fact published on the Group's website, on the corporate intranet and made available in various formats on additional corporate management systems, as well as at corporate offices.

The AG Group HR Department ensures that this Policy is made known to all employees at the time of hiring and with periodic communications; the same also discloses information on the details and contact information of the members of the Reporting Committee and those of the Alternative Manager.

6. GENERAL PRINCIPLES

The activities regulated by this Policy must be carried out in accordance with the principles and contents of the Ethical Code and the binding regulations, with which everyone involved in the process must comply.

Special attention should be paid in the prevention of conflicts of interest and in the transparency of operations. Therefore, each employee is committed to ensuring the Group's interest and operating without conflict of interest between the corporate role held and personal business activities.

In accordance with the binding regulations, any communication having as its object the reasonable and legitimate suspicion or awareness of unlawful conduct, acts or omissions carried out by employees or representatives of the Company that may cause damage, including reputational damage, to the Company itself as well as to third parties may be the subject of a report.

The operation of the Reporting System is also based on the following fundamental principles:

- **Free access:** all AG Group Persons and third parties referred to in art. 3 of Legislative Decree No. 24/2023 who interact with the Group are entitled to make reports through the System described in this Policy.
- **Independence and professionalism of the Departments involved in managing reports:** all departments involved in the management of the reports carry out their activities ensuring the maintenance of the necessary conditions of independence and due objectivity, competence and professional diligence.
- **Training:** the provision to employees and senior management of specific training on the applicable regulations and the contents of this Policy is part of the management process and is scheduled on a regular basis.
- **Protection of the Whistleblower and related sensitive individuals:** in accordance with the provisions of Legislative Decree 24/2023, the Whistleblower and its related sensitive persons are guaranteed the following protections. Namely:

  a. **Duty of confidentiality**, referred to in the section "*Protection of the identity of the Whistleblower and confidentiality of information*" of this procedure.

  The AG Group Companies provide for and apply appropriate criteria and communication methods to protect the identity, as well as the anonymity of the identifying data of whistleblowers and related sensitive individuals (so-called "*principle of confidentiality of the Whistleblower*"), avoiding in any case the disclosure of the acquired data to parties unrelated to the process of investigating and dealing with reports. Individuals assigned to receive and manage reports, as well as any additional employees or individuals who, in any capacity, even accidentally, become aware of

a report, are required to ensure strict confidentiality about the subjects and facts reported.

b. **No retaliation,** referred to in paragraph "*Prohibition of retaliatory, harassing or discriminatory acts*" of this procedure.

All Group employees are strictly prohibited from engaging in direct or indirect acts of retaliation or discrimination for reasons related, directly or indirectly, to the report against the Whistleblower and its related sensitive persons. In the case of breaches of the measures for the protection of the Whistleblower, sanctions are provided for in the following paragraph "*Penalty System*".

- **Protection of the Reported Person:** the AG Group Companies provide for and apply criteria and methods of communication suitable for protecting the identity and honorability of the persons mentioned in the reports. The reported persons are, therefore, protected both with reference to the confidentiality of the reports concerning them and of any investigations carried out, and to the protection of the same from any retaliatory and/or defamatory reports. In the case of unlawful reports, in order to protect the image and reputation of the unjustly reported persons, the listed protective measures are not applied to the Whistleblower, and AG Group ensures the adoption of the disciplinary sanctions provided for by the system and the applicable regulations also against the Whistleblower. In addition, the individuals / Departments involved in the unlawful report are informed of the content of the illicit unlawful report and of the identity of the Whistleblower to enable them to consider possible actions for their own protection.
- **Duty to report:** Recipients have a duty to report breaches of which they become aware or of which they have reasonable suspicion.
- **No making manifestly unfounded and / or defamatory reports:** it is prohibited to submit reports that are manifestly unfounded and/or made with malicious intent for defamatory purposes; in the case of manifestly unfounded and/or defamatory reports, disciplinary action may be taken for the protection of AG and the Reported Person.
- **Duty of independence and professionalism in managing reports:** all persons involved, in whatever capacity, in the process of managing reports must carry out the relevant tasks in accordance with the duties of independence, ensuring the accurate and efficient management of all reports and without making any deviation from the provisions of this Policy.
- **Protection of the integrity of reports:** the Reporting System ensures that no report (from the notification stage to the decision stage) can be deleted and/or altered.

7. SYSTEMS SUPPORTING THE PROCESS

The process is supported by a dedicated information system, the details and methods of use of which are described in Annex I.

TITLE II - REPORTING PROCEDURES AND MANAGEMENT OF REPORTS

In order to enable the recipients of this Policy to fulfil their duty of reporting, the AG Group Companies have prepared – in compliance with the provisions set forth in Legislative Decree 24/2023, implementing EU Directive 2019/1937 –different channels through which the recipients can make reports and regulated the process of managing reports as described below.

8. REPORTING CHANNELS

Private individuals can make their reports through internal AG and external channels, the latter of which can be used when the conditions provided by law are met, as explained in the following paragraphs.

8.1 INTERNAL REPORTING CHANNEL: IT REPORTING SYSTEM

The internal reporting channel adopted by AG Group Companies, described in more detail below, allows reports to be made in both written and oral form, including anonymously.

AG adopts, in particular, an IT Reporting System, consisting of an advanced web-based platform, separate from the Group's IT systems as it is hosted by independent servers, which meets all the requirements of the applicable regulations.

In keeping with the principle of proximity to the Whistleblower, the platform is structured to ensure the segregation of reporting channels for individual Companies.

The System can be reached at the link **https://segnalazioni.amergroup.it** and its access mode does not identify the individual user accessing it. Specifically, access is possible in two distinct ways:

(i) **without registration**, using the **access key** provided by the System itself when entering the report (and in such a case, the non-identification of the Whistleblower is guaranteed as this access key does not allow the identification of the individual user accessing the System);

(ii) **with registration, email** and a **password** entered by the Whistleblower him/herself (and in this case, non-identification is guaranteed as the registration email is known only to the platform and the Whistleblower while no person in AG will have access this data).

a) Written reports

After logging in, in the case of anonymous reporting, the Whistleblower enters the breach detcted (filling in all the fields required therein) on the "compilation" page of the Reporting System, attaching supporting documentation if necessary.

In the case of a named report, the Whistleblower enters his or her identifying information in the appropriate fields on the Reporting System compilation page and reports the breach detected (filling in all the fields required therein), attaching supporting documentation if necessary.

Through the platform, both the anonymous whistleblower and the named whistleblower can interact with the Reporting Committee.

The Reporting System allows the Whistleblower to enter the report by indicating the Group Company to which the report relates and selecting the type of misconduct.

Upon receipt of the report, the Reporting System anonymizes the data of the Whistleblower and automatically enters it into a separate file managed – by computer – by the Reporting Manager and accessible only to the latter, in which such data will be stored. Personal data contained in each archive is encrypted through the use of dedicated and different encryption keys.

The System then displays an initial information confirming that the report has been received and dealt with by providing its **unique identification code** which is communicated to all those who have intended to use the System, whether or not they have registered within it. Through this code and access key, for

example, the unregistered Whistleblower will always be able to access the System to check any requests for clarification and the evaluation status of his or her report. Otherwise, the registered Whistleblower will be able to access the System directly using his or her email and password and employing the unique identification code exclusively to identify his or her reports. In any case, the unique identification code does not allow the Whistleblower to be identified in any way, who can therefore remain anonymous and, at the same time, access the report, check its status and respond to any requests for clarification.

It is the duty of each Whistleblower to diligently guard the unique identification code of the report and/or access credentials, not to release them to others, and not to allow third parties to access information about the report.

b) Oral reports

By means of the IT channel described in the previous point, an oral report can be made, including anonymously, in one of the following ways:

i. **through the special feature on the platform** that allows the recording of an audio, in which the voice of the Whistleblower is altered to prevent his or her recognition and ensure that the Whistleblower himself or herself is not identified in the course of managing the report;
ii. **submitting a request through the platform for a direct meeting with the R.C.** within a reasonable deadline, set no later than 7 days after the respective request is advanced. In this case, it is ensured, with the express consent of the Whistleblower, that complete and accurate documentation of this meeting is kept in a durable medium that allows access to the information.

Reports issued through in-person meetings, subject to the consent of the Whistleblower, may be documented by staff by recording on a device suitable to storage and listening or by minutes. In case of minutes, the Whistleblower may verify, correct and confirm the minutes of the meeting by his or her own signature.

In addition, regardless of the manner (oral or written) in which the report is made, where the Whistleblower has indicated its reference, an acknowledgement of receipt of the report is sent within 7 days of receipt.

In order to ensure traceability, all reports submitted outside the IT platform are entered, by the Committee, within 48 working hours of receipt on the dedicated IT platform, taking care to highlight the origin of the reports.

Similarly, the parties of the Group Companies, other than the Committee, who mistakenly receive reports, in whatever form, are required to keep the information acquired absolutely confidential and ensure the timely forwarding, no later than 3 days after receipt, of the report without retaining a copy and attaching any supporting documentation to the Committee, which then uploads it on the dedicated IT platform also informing the Whistleblower, if known, of the transmission of the report to the competent party.

8.1.1 ANONYMOUS REPORTING

As mentioned in the point above, AG Group, in compliance with applicable legislation, contemplates the possibility of anonymous reporting. Anonymous reporting can be taken up and managed provided it is adequately substantiated and its content sufficiently detailed to make it verifiable.

Therefore, in view also of the extensive protection provided by the law in favour of the Whistleblower, AG Group Companies encourage and foster non-anonymous reports since they are more effective and, in any case, recommend that any anonymous Whistleblower, where possible, makes a report supported by evidence or, in any case, as substantiated as possible.

8.2 EXTERNAL REPORTING CHANNELS

As provided for in Legislative Decree 24/2023, ANAC implements a so-called external reporting channel that guarantees the confidentiality of the Whistleblower, the person involved and the person mentioned in the report, as well as the content of the report and the related communication.

Private sector entities may make a report, using the above external channel, **where one of the following mandatory conditions is met**:

- the Whistleblower has already made an internal report, through the means referred to in the previous paragraphs, but this has not been followed up;
- the Whistleblower has reasonable grounds to believe that by making an internal report, it would not be effectively followed up or that the report may entail the risk of retaliation;
- the Whistleblower has good reason to believe that the breach may pose an imminent or obvious danger to the public interest.

9. SUBJECT AND CONTENT OF REPORTS

a) Subject of reports

This Policy is applicable to reports of breaches that may have an impact on AG Group companies and their business.

In particular, through the Reporting System it is possible to report acts or facts involving legal representatives, directors, executives and/or Employees of AG Group, non-controlling companies in which a Group company has significant shareholdings, joint ventures and/or-in any case-anyone acting in the name, on behalf or in the interest of AG (by way of example: consultants, suppliers, agents etc.).

The acts or facts being reported may involve the following conduct:

- legally relevant and/or pertaining to administrative, accounting, civil or criminal offences;
- put in place in breach of the Group-wide Ethical Code;
- acts or omissions concerning the European internal market, including breaches of competition and state aid rules and corporate taxes;
- likely to cause financial and/or reputational damage to the Group;
- likely to cause harm to AG's employees;
- likely to cause harm to the health or safety of employees, citizens or users;
- likely to constitute environmental breaches or generally cause harm to the environment;
- specific discriminatory conduct and/or breaches of behavioural norms, breach of personal rights, breach of internal control principles and other internal procedures or company regulations that can be sanctioned by disciplinary action;
- involving one of the members of the Reporting Committee;
- potentially suitable for breaching the compliance system adopted by the Group;
- offences that fall within the scope of EU or national acts including, without limitation: public procurement; transport security; environmental protection; public health; privacy and data protection and network and information system security.

Reports taken into consideration are only those that concern facts encountered directly acquired in the context of the Whistleblower's own work environment and must not represent claims / instances of a personal nature[2].

[2] "Claims/requests of a personal nature" means requests made by an employee or a third-party supplier of goods or services that

The above breaches should not be reported through the System in the event that they have come to light as part of audits, or any further investigative activity.

b) Content of the reports

Reports shall:

- relate to situations of which the Whistleblower has become directly aware by reason of the work relationship with AG Group. Therefore, they include all those illegal conducts or omissions of which one has become aware by virtue of one's role and during the performance of one's work activities, even in a casual manner (including relevant breaches under Legislative Decree 231/2001);
- be truthful, circumstantial and based on precise and concordant elements, concerning facts that are verifiable and known directly to the whistleblower him/herself.
- contain information, including well-founded suspicions, regarding actual or potential breaches that have occurred or are very likely to occur in the organization at which the Whistleblower works or has worked, or in another organization with which the Reporting Person is or has been in contact in the course of his or her professional activities, as well as attempts to conceal such breaches.

In order for reports to meet the above requirements, it is useful for them to contain sufficient information to provide a complete and comprehensive representation of the unlawful event, and specifically, it is useful to include:

- except in the case of anonymous reporting, the identifying elements of the Whistleblower (e.g., general details, contact details, job title or position);
  - a description of the facts being reported, including the known circumstances (of manner, time and place) relating to the reported facts, the persons involved and the manner in which one became aware of them;
- identifying elements of the Reported Person(s) when known and of any other persons in a position to report on the reported facts;
- any other information that may provide useful support for the investigation and verification of the existence of the reported facts;
- any documentation supporting the reported fact, using the appropriate document uploading function.

Please note that the absence of one or more of the above-mentioned pieces of information does not invalidate the receipt of the report.

10. REPORT MANAGEMENT PROCESS

10.1 ACCEPTANCE AND PRELIMINARY ASSESSMENT

Following the entry of a new report in the portal, the system sends a notification email – devoid of any reference to the content of the report itself – to the Committee members – who are thus made aware of its receipt.

concern the ordinary administration of the contractual relationships they have established with the AG Group Companies and that as a consequence do not require additional scrutiny in light of this reporting procedure, unless the reported conduct relating to one's personal position falls within the hypotheses of acts characterized by purposes external to the relationship itself and therefore deserving of attention due to their potentially discriminatory, harassing, retaliatory nature or overshadowing hypotheses of corruption between private parties within the meaning of art. 2635 of the Italian Civil Code.

Within **7 days** from when the report was made, the Reporting Committee will issue to the Whistleblower an acknowledgement of receipt – including, if necessary, through the appropriate features of the IT platform. It is the responsibility of the Committee to keep in touch with the Whistleblower to request any additions and diligently follow up on reports received.

Upon taking charge of the report, the R.C. proceeds to conduct a preliminary verification of its subject identification, as well as the substantiation of the circumstances and events represented. To this end, the Committee, in accordance with the principles of impartiality and confidentiality, is empowered to carry out any activity deemed adequate to the ascertainment of the truthfulness of the facts.

Where the report results:

- **manifestly unfounded**, the R.C. proceeds to dismiss the case substantiated by accompanying note;
- **lacking sufficient circumstantial elements or not sufficiently detailed**, the R.C. may dismiss the report, ensuring, however, the traceability of the supporting reasons, or send to the Whistleblower – if known – the appropriate requests for supplements/clarifications;
- **related to different issues than those identified in par. 9** (e.g., communications relating to activities of a commercial nature, complaints etc.), the Head of the Reporting Committee shall forward the report to the Relevant Functions and inform the Committee thereof at the first useful meeting;
- **well-founded**, the R.C. shall initiate the next preliminary investigative stage, taking care to promptly inform the Board of Auditors in cases of alleged accounting irregularities and/or deficiencies in the Company's auditing system.

In the event that, in the course of the analysis, situations of potential conflict of interest with any of the members of the Committee emerge, the Committee is required to refrain from any further activity and the Reporting Manager will forward the report to the Alternative Manager who takes over responsibility for all subsequent activities.

10.2 PRELIMINARY INVESTIGATION

The preliminary investigative phase is aimed at ascertaining the reported facts. The Committee, therefore, carries out the appropriate investigative assessments, if necessary, with the support of an external advisor, ensuring, where possible and necessary, talks with the Whistleblower.

In the latter case, the Reporting Committee defines a specific path of investigation, in which the following are identified:

- the manner of conducting the assessment (requests for supplements/clarifications to the Whistleblower, conduct of verifications deemed necessary etc.);
- the possible Group companies and/or corporate functions responsible for the matter; and
- the deadlines within which to conclude the assessment.

In addition to the above, the Reporting Committee may:

- verify the existence of further disciplinary proceedings against the Reported Person;
- request a personal hearing of the Whistleblower and/or any other individuals who may report on the facts;
- make use of other AG Functions and/or third parties (e.g., consultants), when due to the nature and complexity of the verifications, their involvement is necessary.

The bodies of the Group companies and/or the corporate functions involved in the "path of investigation" shall guarantee full cooperation with the Reporting Committee to the extent necessary to carry out the investigation, in accordance with the principles and guarantees set forth in this Policy.

Fact-finding activities are conducted in compliance with all applicable regulations for the protection of both the Whistleblower and the Reported Person.

Within three months after sending the acknowledgement of receipt of the report, or, after the expiration of the seven-day period from the receipt of the report (when the acknowledgement of receipt could not be forwarded to the Whistleblower), the Whistleblower shall be informed, where possible, of the status of the report – also through the appropriate features of the IT platform.

Reporting Persons can monitor the progress of the management of their reports by accessing the dedicated information portal, if the report was made through that system.

10.3 DECISION AND MEASURES IN RESPONSE TO THE REPORT

In light of the preliminary findings, the R.C.:

- dismisses the report stating the reasons;
- qualifies the report as a report made with wilful misconduct or gross negligence and, in such cases, decides on any action to be taken against the Whistleblower (such as, for example, the imposition of disciplinary measures and/or further action in compliance with current regulations and without prejudice to the provisions of art. 16 (Conditions for the protection of the Whistleblower) and 20 (Limitations of liability) of Legislative Decree 24/2023);
- classifies the report in its reports;
    - prepares a report on the results of the investigation in which it outlines: i) the results of preliminary investigations; ii) its decision on the facts that are the subject of the report; iii) any disciplinary measures and corrective actions to be proposed to the relevant corporate function/body.

The report shall be forwarded to the Managing Directors – or to the Board of Directors if the conduct is attributable to the Managing Director – for the purpose of taking, if necessary, the actions that may be required in accordance with this Policy.

In the event of ascertained significant breaches, the outcome of the investigation as well as disciplinary measures, corrective actions and any further measures and/or actions that may be necessary in the actual case to protect the AG Group Companies are communicated to the H&R Department, so that it may take the measures within its competence, and information is provided to the Area Manager of the Department in which the author of the ascertained breach works.

Disciplinary measures must be appropriate and proportionate to the ascertained breach, also taking into account the possible criminal relevance[3] of the conduct engaged in, and must comply with the provisions of the applicable national labour law.

Information on the sanctions and corrective actions taken is given by the relevant function to the Reporting Committee, which updates the file on the report of interest.

[3] Please note that: within the framework of criminal proceedings, the identity of the Whistleblower is covered by secrecy in the manner and to the extent provided for in article 329 of the Italian Code of Criminal Procedure; within the framework of proceedings before the Court of Accounts, for example, the identity of the Whistleblower may not be revealed until the preliminary investigation stage is over.

10.4 ALTERNATIVE MANAGER

In the event that the Reporting Manager or one of the other members of the Reporting Committee, in relation to a specific report, finds him/herself in one of the following situations:

i. be hierarchically or functionally subordinate to the Reported Person, if any;

ii. be the alleged perpetrator of the breach;

iii. have a potential interest in the report that would compromise his or her impartiality and independence of judgement;

there is a possibility for the Whistleblower to forward the report to an "Alternative Manager" through the platform described above by selecting the item "*Misconduct concerning reporting receivers*".

The name(s) of the persons constituting the "Alternative Manager" shall be made known to all recipients by the same forms of communication adopted for the dissemination of this Policy.

TITLE III - PROTECTIONS AND PENALTY SYSTEM

11. PROTECTION AND DUTIES OF THEWHISTLEBLOWER

Committee members involved in the management of reports are required to ensure confidentiality regarding the existence and content of the report, as well as the identity of the Reporting Persons (where disclosed) and Reported Persons.

Any communication regarding the existence and content of the report, as well as the identity of the Whistleblower (where disclosed) and Reported Persons, must strictly follow the "need to know" basis which limits access to only the information necessary for the purposes of the preliminary investigative activity of the report.

It should be noted that, in accordance with regulatory provisions, the protections provided for the Whistleblower are also extendedto parties related to the same[4].

11.1 PROTECTION OF THE WHISTLEBLOWER'S IDENTITY AND CONFIDENTIALITY

AG Group guarantees the confidentiality of the identity of the Whistleblower (where disclosed) and the confidentiality of the information contained in the reports at every stage of the report managing process, to the extent that anonymity and confidentiality are enforceable under the law.

In particular, it is the task of the Reporting Committee to ensure the secrecy of the identity of the Whistleblower (where disclosed) from the moment the report is taken in charge until the end of the investigation of the merits of the report, even in cases where it turns out to be erroneous or unfounded. Reports may not be used beyond what is necessary so that they can be adequately followed up.

The identity of the Whistleblower (where disclosed) – and any other information from which that identity may be inferred directly or indirectly – may not be disclosed – without his or her express consent – to persons other than those responsible for receiving or following up the reports, who are expressly authorized to process such data (Data Controller and Data Processor, pursuant to Regulation (EU) 2016/679 and the Personal Data Protection Code).

In the case of transmission of the report to other structures/organizations/third parties for the performance of preliminary investigative activities, the Reporting Committee shall separate the identification data of the Whistleblower (where disclosed) from the content of the report, so that the reported facts can be processed anonymously and that the association of the report with the identity of the Whistleblower (where disclosed) takes place only in those cases where this is strictly necessary.

For reports transmitted through the IT platform referred to in the previous paragraphs, the confidentiality of the Whistleblower is guaranteed in the following ways:

- the advanced **web platform** is separate and independent from the Group's IT systems, as it is hosted on independent servers that enable reporting from any device, in a highly confidential and facilitated

[4] These parties are:
- Facilitator, an individual who assists the Whistleblower in the reporting process, operating within the same work environment and whose assistance shall be kept confidential;
- persons from the same employment background as the Whistleblower, reporting person or the person making a public disclosure and who are related to them by a stable emotional relationship or relatives within the fourth degree of kin;
- colleagues of the Whistleblower, reporting person or person making a public disclosure, who work in the same work environment as that person and who have a usual and current relationship with said person;
- entities owned – exclusively or in majority third-party co-partnership – by the Whistleblower, reporting person, or person making a public disclosure;
- entities at which the Whistleblower, reporting person, or person making a public disclosure works (art. 3, par. 5(d).
- entities that operate in the same work environment as the Whistleblower, reporting person, or person making a public disclosure.

manner, guaranteeing the protection of the identification data of the Whistleblowers;

- ensures high standards of **security, non-traceability** and **integrity** of information and **confidentiality** of the identity of the Reported Person and the Whistleblower, allowing the Whistleblower to also enter the report anonymously;
- the platform does not make available to any AG person the information about the connection mode (e.g., server, IP address, MAC address), thus ensuring complete anonymity in access;
- the platform does not allow the registration of any Whistleblower who enters an e-mail address belonging to an AG person into the system in order to ensure that the Whistleblower is not identified, even indirectly; in addition, again in order to ensure the non-identification of AG persons who act as a Whistleblower, access to the Reporting System is denied to all company devices or to all devices found to be connected to AG's network thus preventing internal security systems from tracing the identity of the Whistleblower himself;
- the platform ensures high security standards, employing advanced encryption algorithms and other methods to protect against unauthorized access. Reports issued through verbal communication will not allow voice recognition;
- the platform assigns the report a unique identification code (so-called ID code) in order to protect the identity of the Whistleblower; in addition, if the Whistleblower registers on the platform, this data is never made available to AG persons;
- for access via the Internet on AG's website (available to anyone, including employees) no mandatory registration is required, and the Whistleblower can remain anonymous. The latter, if he or she deems so, may otherwise give his or her name by providing express consent for his or her personal details to be disclosed.

For reports transmitted through the other internal channels, the confidentiality of the identity of the Whistleblower and the content of the report are protected in the following ways:

- paper correspondence addressed to the Reporting Manager is delivered in a sealed envelope (as delivered by the postal service);
- mailboxes can only be accessed by the Reporting Committee. The administrator of the e-mail system of the Group Companies may only access the reference email box for technical needs, subject to a reasoned case-by-case request to be submitted in writing to the R.S. and access will be allowed only subject to prior written permission of the same.

Disclosure of the identity of the Whistleblower (where disclosed) and of any other information from which the identity of the Whistleblower can be directly or indirectly inferred is permissible only if this represents a necessary and proportionate obligation imposed by European Union or national law in the context of investigations by national authorities or judicial proceedings, including in order to safeguard the defence rights of the person involved.

In fact, the Reported Person will not be able to request to know the name of the Whistleblower, except in cases expressly provided for by law.

As part of the disciplinary proceedings implemented by Group Companies, the identity of the Whistleblower (if known) may not be disclosed where the allegation of the disciplinary charge is based on findings that are distinct and additional to the report, even if consequent to it.

If, on the other hand, the charge is based, in whole or in part, on the report and the knowledge of the identity of the Whistleblower is essential for the defence of the accused, the report can be used for the

purposes of the disciplinary proceedings only if there is the Whistleblower's consent to the disclosure of his or her identity. In such cases, written notice shall be given to the Whistleblower of the reasons for the disclosure of the confidential data.

A Whistleblower who makes a **public disclosure**, in the information media, shall benefit from the protection provided by this Policy, as well as by regulatory provisions, if one of the following conditions is met: a) the Whistleblower has previously made a report that has not been followed up; b) the Whistleblower has reasonable grounds to believe that the breach may pose an imminent or obvious danger to the public interest; c) the Whistleblower has a well-founded reason to believe that the internal report may carry the risk of retaliation or may not be effectively followed up due to the specific circumstances of the particular case, such as those where the Whistleblower's non-identification may be concealed or evidence destroyed or where there is a well-founded fear that the Whistleblower may be colluding with or involved in the breach.

11.2 PROHIBITION OF RETALIATORY, HARASSING OR DISCRIMINATORY ACTS

No form of retaliation, harassment, or discriminatory measures, whether direct or indirect, for reasons related directly or indirectly to the reporting, is permitted or tolerated against the Whistleblower. This protection is guaranteed even when the report, though unfounded, was made in good faith and reasonably.

By way of example, pursuant to Legislative Decree 24/2023, the following **constitute retaliation**: dismissal, suspension or equivalent measures; demotion or non-promotion; change of duties, change of workplace, reduction of salary, change of working hours; the suspension of training or any restriction of access to it; negative merit notes or negative references; the adoption of disciplinary measures or other penalty, including fines; coercion, intimidation, harassment or ostracism; discrimination or otherwise unfavourable treatment; the failure to convert a fixed-term employment contract to a permanent employment contract where the employee had a legitimate expectation of said conversion; the non-renewal or early termination of a fixed-term employment contract; damage, including to the person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income; inclusion in improper lists based on a formal or informal trade or industry agreement, which may result in the person being unable to find employment in the trade or industry in the future; early termination or cancellation of the contract for the supply of goods or services; the cancellation of a license or permit; the request to undergo psychiatric or medical examinations.

A Whistleblower who believes that he or she has suffered discriminatory acts must provide detailed notice to the Reporting Committee by submitting an appropriate report through the Internal Channels made available.

In such cases, the Reporting Committee ensures the timely conduct of investigations, with the support of the functions affected by the reported facts.

In particular, having assessed the existence of the elements, it reports the hypothesis of retaliatory, harassing or discriminatory acts to the HR Manager, who assesses the acts or measures required to remedy the negative effects of any ascertained retaliatory, harassing or discriminatory acts and the existence of the gounds for initiating disciplinary proceedings against the person who perpetrated the aforementioned acts.

In addition, if the Whistleblower is an employee, the Reporting Committee – availing itself of the competent Departments – monitors the performance of the employee's work life for a period of at least 2 years from the date of the report, to ascertain the absence of discriminatory actions or other forms of retaliation resulting from the report.

The above also applies to facilitators of the Whistleblower, persons related to the Whistleblower by a stable emotional relationship or relatives within the fourth degree of kin and operating in the same work context, colleagues of the Whistleblower, and entities owned by the Whistleblower or operating in the same work context.

11.3 PRIVATE INTEREST AND CO-RESPONSIBILITY OF THE WHISTLEBLOWER

The Whistleblower is required to declare the existence of any private interest of his or her own related to the report.

If the Whistleblower is co-responsible for the reported breaches, mitigation of disciplinary measures may be applied against him or her in proportion to the contribution made by the report to the discovery and/or prevention of the said breaches.

The Reporting System is therefore configured in such a way as to enable the Whistleblower to disclose *(i)* the existence of a private interest in relation to the report as well as *(ii)* his or her own possible co-responsibility in relation to the acts or facts that are the subject of the report.

12. PROTECTION OF THE REPORTED PERSON

The Group requires everyone to cooperate in maintaining a climate of mutual respect and prohibits and sanctions attitudes that may harm the dignity, honour and reputation of each person. The confidentiality guarantees established by this procedure also protect the Reported Person.

The Reported Employee has the right to be informed of the existence of the report and the outcome of the checks carried out. Such information may, however, be delayed, limited to the necessary time, in order to avoid the risk of prejudicing the needs of investigation, including those that may be requested by the Judicial Authority, if involved.

The Reported Person is not subject to penalty in the absence of objective findings of the reported breach, or without having investigated the reported facts and disputed the related charges as required by applicable regulations.

For the further protection of the Reported Person, the actions and power allowed to him or her by law remain unaffected.
Please note that the identity of the persons involved and the persons mentioned in the report is also protected until the conclusion of the proceedings initiated on account of the report, subject to the same guarantees provided in favour of the Whistleblower.

12.1 DISCLOSURE TO THE REPORTED PERSON

As part of all phases of the managing reports, the Reporting Committee considers how to inform the Reported Person of the transmission of a report against him or her, the alleged breach, the conduct of the related proceedings, and the outcome of the proceedings.

In particular, the time at which the Reported Person is made aware of the report against him or her must be evaluated on a case-by-case basis, assessing whether sending such a report may prejudice the conduct of the investigation required to ascertain the facts that are subject to the report or whether, on the other hand, the Reported Person's involvement is necessary for the development of the investigation.

AG guarantees, in any case, the Reported Person's right to be able to defend himself or herself and to be informed (within a reasonable time) of the charges and any disciplinary measures against him or her.

13. PENALTY SYSTEM

AG Group shall take appropriate disciplinary or contractual measures against:

- anyone who is responsible for any act of retaliation or discrimination or otherwise unlawful prejudice, direct or indirect, against the Whistleblower (and/or anyone who collaborated in the investigation of the facts that are subject to a report and/or persons connected to the Whistleblower) for reasons related, directly or indirectly, to the report;

- the Reported Person, for the responsibilities ascertained;
- anyone who breaches the confidentiality obligations invoked by this Policy;
- the employees, as provided by law, who have made an unfounded report with wilful misconduct or gross negligence;
- those who abuse the reporting tool, such as by making reports for opportunistic purposes and/or for the purpose of harming the accused;
- the Reporting Manager, the members of the Reporting Committee and the Alternative Manager if they breach the duty of independence and professionalism in the management of reports or otherwise give rise to conduct that is unjustified and deviates from the provisions of this Policy.

The applicable penalties are those set forth in the applicable labour and contractual regulations.

TITLE IV - FINAL PROVISIONS

14. ANNUAL PERIODIC REPORTING

The Reporting Committee, at least annually, prepares a report on the reports filed and the findings of the activities carried out in connection with the reports under investigation. The report is forwarded to the competent administrative and supervisory bodies.

15. SUPPORT AND ASSISTANCE

For any doubts, clarifications or advice related to this Policy, Recipients should always turn to the Reporting Manager who is at their disposal to provide any necessary support.

Any request for assistance can be submitted by e-mail to whistleblowing@amergroup.it.

16. RESPONSIBILITY FOR UPDATING

The Functions involved, each to the extent of its competence, are responsible for the detection of operational business occurrences that entail the need to update this procedure and will be required to make a relevant request for implementation to the address of the boards of directors of the AG companies that will have to provide for the assessment of any risks of non-compliance and the execution of the changes and/or supplements deemed appropriate.

17. STORAGE, RECORD KEEPING AND TRACEABILITY

The Functions involved ensure, each to the extent of its competence and also by means of the IT systems used, the traceability of data, information and controls and provide for the storage and archiving of the documentation produced, on paper and/or electronically, so as to enable the different stages of the process itself to be retraced.

Reports received through the Reporting System (together with any attached documentation) are saved in the IT archive of the Reporting System, which does not allow for any form of deletion and/or alteration. The archive is protected with encryption measures, access restrictions and tracking of every activity. Such documentation must be retained for an appropriate period of time and in any case not more than 5 years from the date of the communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set forth in this Policy and the principle set forth in art. 5 par.1 letter e) of the GDPR and art. 3, par., letter a) of Legislative Decree 51/2019.

18. DATA PROCESSING

Personal data is processed in compliance with Regulation (EU) 2016/679 (GDPR), as well as any other applicable and compatible laws and/or regulations, and with the notice published on the Company's website (at https://amergroup.it/privacy-policy, hereinafter "Notice").

The management of reports involves the processing of personal data of the Whistleblower (where disclosed), the Reported Person (e.g: first name, last name, position held etc.), of any third party, as well as any additional information gathered as part of the investigation required to ascertain the merits of the report. The data collected is used exclusively for the processing of the report, and that is not useful for the purpose is immediately deleted.

The processing of personal data carried out by the Competent Functions and Control Bodies as part of the reporting management process falls under the responsibilities of "Data Processors" and persons authorized to process personal data for their respective competencies, in accordance with the provisions of the law and those of this Policy.

The process of managing reports is based on the principle of "*guarantee of confidentiality and anonimity*" and the "*principle of confidentiality of the Whistleblower*" and, therefore, while waiting for the internal verification process, strict confidentiality is guaranteed.

Where provided for by applicable legal provisions, data subjects may exercise their rights under the GDPR by sending an e-mail notice to the address of the Data Protection Officer (Mr. Giuseppe Mercanti, giuseppe.mercanti@amergroup.it). The right to appeal to the data protection authority, which has jurisdiction over unlawful data processing, is also guaranteed.

The confidentiality of the Whistleblower, whose identity may not be disclosed to the Reported Person except in the cases provided for by law, shall always be protected in order to avoid retaliation, threats, violence, discrimination etc., direct or indirect against him or her for reasons related directly or indirectly to the report. This principle is not guaranteed in the case of unlawful reporting.

The Group reserves the right to limit or delay the exercise of these rights, in accordance with the applicable provisions of the law, in the case of actual and concrete prejudice to the confidentiality of the identity of the Whistleblower and the impairment of the possibility of verifying the merits of the report and/or identifying evidence. Under no circumstances may the Reported Person, or third parties, exercise their access rights to obtain information about the identity of the Whistleblower unless the Whistleblower has made an unlawful report.

The Group reserves the right to assess the specific circumstances and conditions that make it appropriate to specifically inform the Reported Person about the conclusion of the proceedings, in order to avoid any abuse and ensure his or her protection as a data subject.


amer
group