PROCEDURE TO PROTECT PERSONS REPORTING VIOLATIONS AT COMPANY LEVEL (SO-CALLED WHISTLEBLOWING)

1. Purpose of the procedure.

This procedure is adopted by O.M.G. S.r.l. (hereinafter also referred to as the "Company") in compliance with the provisions of Legislative Decree no. 24 of 10 March 2023 (in the text: Decree or d. l.vo 24/2023), which implements EU Directive no. 2019/1937 of the European Parliament and of the Council of 23 October 2019, concerning the protection of persons who report violations of national or European Union regulatory provisions (so-called whistleblowing directive) that have come to their attention in the context of their work, which are detrimental to the public interest or the Company.

This procedure was approved by the Board of Directors on 11 December 2023 together with the identification of the organisational roles involved in the reporting process and the related responsibilities. This procedure comes into force on the date of its approval by the Board of Directors of the Company.

This procedure is also available on the company website at: www.omgsrl.com and will be posted on thecompany notice board.

On 15 December 2023, specific information on this procedure was provided to the trade unions, pursuant to Article 4, paragraph 1 of the Decree.

2. Scope of application.

This procedure applies to any report of information on violations (as better specified in paragraph 4) knownwithin the work context (to be understood as an employment relationship with the Company, or a professional/self-employed/collaboration relationship, present or past), if detrimental to the public interestor to the integrity of the public administration or of the Company, made through the appropriate reportingchannels made available by the Company itself.

They are excluded from the scope of this procedure:

- disputes, claims or demands of a personal nature that relate exclusively to individual employment relationships, i.e. employment relationships with hierarchically superior persons;
- violations mandatorily regulated by European Union or national acts that already guarantee specific reporting procedures.
- national security breaches, as well as procurement relating to defence or national security aspects

3. Normative references

- Legislative Decree No. 24 of 10 March 2023;
- EU Directive No. 2019/1937;
- Organisation, management and control model adopted by the Company pursuant to Legislative Decree No. 231/2001;
- European Regulation No. 2016/679 (GDPR);
- Privacy Code (Legislative Decree No. 196/2003);
- ANAC guidelines on the protection of persons who report breaches of Union law and the protection of persons who report breaches of national laws - procedures for the submission and handling of external reports.

4. Definitions.

For the purposes of the decree, the following are defined as:

- **reports**: any written, oral or displayed communication in an interview, provided it is not anonymous,containing information on violations;
- **violations:**
  - unlawful conduct pursuant to Legislative Decree No. 231/2001 or violations of the Organisation andManagement Model adopted by the Company;
  - offences within the scope of European Union or national acts 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 protection of personal data and security of networks and information systems;
  - infringements (acts or omissions) detrimental to the financial interests of the European Union (referred to in Article 325 of the Treaty on the Functioning of the European Union);
  - violations (acts or omissions) of European Union competition and state aid rules; violations of corporate tax rules;
  - acts and conduct that frustrate the object or purpose of the above provisions;
  - misdemeanours, accounting, administrative and criminal offences not covered by the above lists.

- **information on breaches:** all information, including reasonable suspicions, concerning breaches committed or which, on the basis of concrete elements, could be committed within the Company with which the reporting person or the person lodging the complaint with the authority legal/accounting relationship, as well as information on conduct aimed at concealing such violations;
- **internal reporting:** communication of information, submitted through the designated internal reporting channel;
- **external reporting:** communication of information, submitted through the external reporting channel;
- **public disclosure:** the placing in the public domain of information on infringements through the press, electronic media or, in any case, through means of dissemination capable of reaching a large number of people;
- **Reporting person**: an individual who makes a report or public disclosure of information on violations acquired in the context of his/her work context;
- **manager:** a natural person, or internal department, or external professional to whom the Company entrusts the management of the internal reporting channel, endowed with autonomy and specifically trained to carry out this task;
- **facilitator:** a person who assists a reporting person in the reporting process, operating within the same work context and whose assistance is to be kept confidential;
- **work context:** current or past work or professional activities through which, regardless 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 public disclosure or reporting to the judicial or accounting authorities;
- **person involved:** natural or legal person mentioned in the report as the person to whom the breach is attributed, or as a person otherwise implicated in the reported or publicly disclosed breach;
- **retaliation:** any conduct, act or omission, even if only attempted or threatened, occurring as a result of the report, judicial or accounting authority report or public disclosure and which causes

  or is likely to cause the reporting person or the person making the report, directly or indirectly, unjust damage;
- **follow-up**: the action, i.e. the actions taken by the person entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the

- investigation and any measures taken;
- **acknowledgement**: the communication to the reporting person of information on the follow-up given or intended to be given to the report;
- **Supervisory Board (SB):** Supervisory Board appointed pursuant to Legislative Decree No. 231/2001 by the Company;
- **Model 231:** Organisation, Management and Control Model adopted pursuant to Legislative Decree No. 231/2001 by the Company.

5. Obligations and responsibilities.

The company

- makes available, also through this procedure, clear information on the channel, procedures and prerequisites for making internal reports;
- issues the reporting person with an acknowledgement of receipt of the report within the deadline;
- assesses the criteria for instructing the alert;
- shares the report with the Supervisory Board (if relevant for the purposes of Legislative Decree No. 231/2001), with any further internal interlocutors, defined within the scope of this procedure, and coordinates, together with the Supervisory Board, if the report is relevant for the purposes of Legislative Decree No. 231/2001, any investigations, their outcome and the feedback to be provided to the reporter;
- sends feedback to the reporter on the closure of the handling of the report;
- maintains contact with the reporting person, carrying out any interviews with the latter who has requested it; if necessary, manages in-depth investigations, additions and the performance of investigative acts to assess the merits and scope of the report;
- files and stores the reporting documentation within the regulatory timeframe;
- ensures respect for the principle of confidentiality;
- provides the head of the internal channel with feedback on the decisions taken by the Company to investigate the matter;
- monitors the investigation phase with any internal functions involved or with any external professionals entrusted with the investigation activities;
- identifies improvement plans to avoid the recurrence of reportable events;
- makes available on company channels all the information provided on the channel, procedures and prerequisites for internal reporting;
- manages the activities resulting from any public disclosures in the cases provided for;

- ensures respect for the principle of confidentiality.

The Signalman:

- transmits reports in accordance with this procedure;
- is obliged to provide circumstantial information on the matter reported.

The Supervisory Board:

- cooperates, in the areas falling within its competences, with the Manager of the reporting channel, ensuring support to the Manager and to any internal functions/external professionals involved; is informed by the Manager and the Corporate Bodies of the final determinations of the investigations; finally, adopts any consequent measures in the case of relevant reports pursuant to Legislative Decree No. 231/2001;
- ensures respect for the principle of confidentiality.

The Manager:

- It is the person, identified as the Chairman of the Supervisory Board, who carries out the task of managing the internal reporting channel set up by the Company, strictly complying with the provisions of Article 5 of the Decree.

The Legal Representative:

- liaises with ANAC in the event of any external reporting or activation of inspection activities by ANAC.

The Board of Directors / Managing Director:

- ensures that any measures are taken in accordance with the provisions of the penalty system set out in the Organisational Model;
- approves this procedure together with the associated organisational role structure;
- ensures compliance with the measures for the protection of the reporting person.

6. Persons who may make a report (so-called reporter).

They may proceed with the reporting:

- employees;
- self-employed workers and collaborators working for the Company;
- freelancers;
- consultants;

- volunteers and trainees, including unpaid ones;
- shareholders;
- administrators;
- Providers of services for third parties in any capacity whatsoever (irrespective of the nature of such activities) even without consideration;
- persons exercising functions of administration, management, control, supervision or representation, even if the relevant activities are performed in a de facto and not in a de jure capacity.
- Also included in this category are all those persons who, for whatever reason, become aware of offences in the context of the Company's working environment, i.e:
- when the employment relationship has not yet begun;
- during the probationary period;
- upon termination of the relationship.

7. Internal reporting channel. Manager.

The Company has provided for an internal reporting channel to be used by whistleblowers to transmit information on violations. The use of this channel allows for more effective prevention and detection of violations. This choice responds to the principle of fostering a culture of good communication and corporate social responsibility, as well as improving the internal organisation of the Company.
The management of the internal reporting channel is entrusted to the Manager, who is identified as the Chairman of the Company's Supervisory Board.
The internal signalling channel involves only the use of analogue written or oral mode.
The internal reporting channel guarantees the confidentiality of the identity of the whistleblower, the facilitator (if any), the persons involved and in any case mentioned in the report, as well as the content of the report, the attached documentation, and any supplementary documentation.

8. Procedure for handling internal reports.

8.1 Features of the internal signalling channel.

The Company's internal reporting channel is based on analogue written reports to be made exclusively byregistered letter of the postal service.
The notification must be made using three sealed envelopes, the first two of which must bear the followingnumbers:

- The first one (1) must contain the identification data of the reporter (name, surname, address and telephone number, if any), together with a photocopy of his/her identity document;
- the second (2) must contain the alert;
- the third one must contain the two envelopes described above.

- This third envelope must be marked, in addition to the address of the Company, as follows: Reserved for the reporting manager.

The report may be opened, viewed and managed by the reporting channel manager alone, or by any other person authorised by him/her if the in-depth investigation of the matter reported makes this necessary.
The processing of personal data must always take into account and comply with the obligations set out in the GDPR and in Legislative Decree No. 196/2003 et seq. The Company, as data controller, through the internal reporting channel is required to carry out a prior analysis of the organisational design including the fundamental assessment of the possible impact on data protection (Article 35 of the GDPR).

8.2 Written reports.

It is necessary that the report be as detailed as possible in order to allow the analysis of the facts by the Manager designated to receive and handle reports. In particular, it must be clear:

- the circumstances of time and place in which the event reported occurred;
- description of the fact;
- personal details or other elements enabling identification of the person to whom the reported facts can be attributed.

Information on reported violations must be truthful. This does not include mere suppositions, unreliable indiscretions (so-called "rumours"), news in the public domain, incorrect information (with the exception of that which is the result of an innocent error), manifestly unfounded or misleading, or merely defamatory information. On the other hand, it is not necessary for the reporter to be certain of the actual occurrence of the reported facts and the identity of the author thereof.
It is desirable for the reporter to provide documents that provide evidence of the facts being reported, as well as an indication of other persons potentially aware of the facts.

8.3 Anonymous reports.

Anonymous reports, however circumstantiated, will in no way be taken into account.
Nevertheless, they will be kept on file with the others, solely for the purpose of protecting the reporter, should he or she be subsequently identified.

8.4 Oral reporting.

In addition to an analogue written report, the reporter may also make an oral report by requesting a meeting with the Reporting Manager.

This meeting must take place in a suitable place to ensure the confidentiality of the reporter within 15 working days of the request, unless it takes place during the Company's holiday closing period, in which case the time limit will be postponed to the first day of reopening.
With the reporter's consent, a recording of the meeting is recorded on a device suitable for storage and voice reproduction; in the event of lack of consent or unavailability of recording devices, minutes are drawn up and read out to the reporter, who may check and correct the text, finally signing it together with the person(s) who drew it up and took part in the meeting.

8.5 Transmission of alerts with wrong addressee.

If the report is transmitted to a person other than the person receiving it, the person receiving the report is obliged to transmit it within seven days to the Manager, notifying the reporting person of the transmission.

8.6 Preliminary verification procedure of the alert.

Upon receipt of the written report, the Company shall, without opening it, forward it to the Manager.
In the event of prior opening of the report by the Company's reception staff, either because it was not marked 'Confidential to the Reporting Manager', or by mistake, the Manager, upon receipt of the report, shall draw up a report describing the conditions in which the document is found and indicating the name(s) of the person(s) who opened it, to whom he shall emphasise the obligation of confidentiality with regard to the information of which he accidentally came to know.

Upon receipt of the report, the Manager shall, within seven days, notify the reporting party of its receipt. In the event of failure to provide the reporting party's address, where the same is not otherwise known or knowable by the Manager, the report shall be filed without further action.
The Managing Director proceeds with an initial check on the admissibility of the report, in particular by ascertaining that the procedural rules set out in paragraph 8.1 above have been complied with, that the person making the report falls within the scope of the persons entitled to make it, and that it does not concern matters excluded from the scope of the legislation
If the report concerns violations of the Organisation, Management and Control Model adopted by the Company or other relevant elements for the purposes of Legislative Decree No. 231/2001, the Manager necessarily involves the other members of the Supervisory Board to assess the report.
Having successfully completed the check on the admissibility of the report, the Manager then proceeds to a subsequent check on the admissibility of the report, ascertaining in particular that

- The data constituting the essential elements of the alert. In particular:

    - the circumstances of time and place in which the event reported occurred;
    - description of the fact;

- personal details or other elements enabling identification of the person to whom the reported fact can be attributed.

- It does not appear to be manifestly unfounded that the facts are attributable to the infringements envisaged by the legislature;
- The statement of facts is not made in such a general manner that it is not comprehensible to the Manager;
- The report does not merely consist of the enclosing of documents from which the commission of any infringement cannot be deduced.

Following such further scrutiny, the Manager, if he deems it necessary, may request clarifications from the reporting party in order to carry out any further investigation, as specified in paragraph 8.8 below. At the outcome of the check on the admissibility and admissibility of the report, the Manager adopts a measure declaring the report admissible and admissible, or orders the report to be closed, stating the reasons, in the latter case notifying the reporter within three months of receipt of the report.

8.7 Conflict of Interest.

It is specified that, from the receipt of the report until the closure of the investigation, any person who finds himself in a situation of conflict of interest must declare this condition, refraining from taking decisions, in order to ensure compliance with the principle of impartiality.

In the event that the report concerns the Manager himself, it should be addressed directly to the Chairman of the Board of Directors of the Company/Managing Director, who shall carry out all the activities attributed to the Manager himself referred to above, possibly availing himself of the support of specialised external consultants for investigation activities.

8.8 Instruction.

If it is necessary to obtain additional information, the Management Company contacts the reporting person at the address indicated by the latter. If the reporting agent does not provide the additional information requested within three months of the request for supplementation, the Management Authority shall consider whether to proceed with the filing of the report, notifying the reporting agent accordingly.

After verifying the merits of the report and acquiring all the necessary supplementary elements from the reporter, the Manager may decide to initiate all the investigations necessary to further investigate the matter reported.

In particular, also for the purpose of making any recommendations on the adoption of the necessary corrective actions on the areas and business processes concerned, with a view to strengthening the internal control system, the Manager may, by way of example

- examine the documentation received from the reporter and that obtained from internal functions or external stakeholders;
- obtain information from the reporting person himself, while guaranteeing the confidentiality of his identity, and/or from other persons belonging to the corporate structures or from external persons involved in any way, who are aware of the facts or circumstances relating to the report, by means of hearings, which should, if necessary, be minuted;
- make use of external expertise.

The person concerned shall in any case be heard by the Manager also by means of a cartel procedure, through the acquisition of written observations and documents.
In any case, the Manager shall proceed to the obscuring of data and any information from which the identification of the reporter could be derived.
In respect of all internal and external parties involved in the preliminary activity, the Manager will acquire specific commitments to maintain the confidentiality of the data processed and the identity of the parties involved.
In the event of information of relevant breaches pursuant to Legislative Decree No. 231/2001, the Manager shall coordinate with the other members of the Supervisory Board in order to assess how to initiate the investigation phase, without prejudice to compliance with the principle of autonomy and independence of the Supervisory Board.
The Manager shall assess, on a case-by-case basis, with the Company whether and which corporate function should be appropriately involved for the relevant analysis, to be carried out in any case in compliance with the principle of confidentiality, and for the adoption of any consequent measures.
The Manager shall prepare a final written report upon completion of the investigation.The report may include:

- dismissal of the report on the ground that it was unfounded;
- the declaration of the merits of the report, with transmission of the documents to the competent corporate functions or bodies for the relevant measures or steps to be taken.

No final action shall be taken, nor shall any disciplinary proceedings be brought by the Manager.
In the sole case of reports of violations relating to Legislative Decree No. 231/2001 and to the Organisation, Management and Control Model adopted by the Company, the Manager's report must be shared with the other members of the Supervisory Board.
The Supervisory Body, within the scope of its operational autonomy, if the report proves to be well-founded, assesses any consequent measures and adopts any measures deemed necessary for the purposes of adapting the Model, taking the necessary steps to ensure that the Company proceeds with the application of any sanctions.
Any consequent measures are applied in accordance with the provisions of the sanctions system set out in the Company's Organisational and Management Model.

The reporter must be informed of the outcome of the investigation within three months from the date of receipt of the report, i.e. after the expiry of seven days from its submission.
Only in exceptional cases, where the complexity of the report so requires, or in view of the time required to reply to the reporter, the Manager, having promptly informed the latter before the deadline, may continue the investigation phase for as long as necessary, giving the reporter periodic updates and informing him/her of the final outcome.
In the event of defamation or slander, ascertained by a conviction even at first instance, the Company shall proceed with a sanctioning procedure against the whistleblower.

8.9 Retention of documentation on internal reporting.

Internal reports and all the documentation attached thereto, or acquired as a result of additions ordered by the Manager, are kept for the time strictly necessary to process the report itself, and in any case only for a maximum period of five years from the date of communication of the final outcome of the reporting procedure.

In all the above cases, the procedure for keeping internal reports and related documentation must comply with EU and national guarantees on the processing of personal data, as well as with the measures in place to protect the confidentiality of the reporter and other persons involved.

8.10 Information obligations.

Information on the channel, procedures and prerequisites for making reports is displayed in the workplace, by posting it on the company notice board. The same information is also posted in a special section of the corporate website.

9. External signalling.

If the following conditions are met, the whistleblower may proceed with a report through an external channel to ANAC:

- if in the relevant working context, the activation of the internal reporting channel is not mandatory, or the channel itself has not been activated, or does not comply with regulatory requirements;
- when the whistleblower has already submitted an internal report, if it has not been followed up;
- whether the whistleblower has reason to believe that, by submitting an internal report, the report will not be effectively followed up, or that the report, in itself, may give rise to the risk of retaliation against him/her;
- Where the reporter has a well-founded reason to believe that the reported breach may constitute an imminent or obvious danger to the public interest.
-

The external body entitled to receive external reports is ANAC according to the modalities and procedures it has duly adopted and which can be consulted at www.anticorruzione.it.

10. Public Disclosure.

On a residual and subordinate basis, the reporter may proceed with a public disclosure in the following cases:

- when it has already previously made an internal or external report, or has directly made an external report without having received a reply within the prescribed time limit;
- where it has reasonable grounds to believe that the breach constitutes an imminent or obvious danger to the public interest;
- where it has reasonable grounds to believe that the external report carries the 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 breach.

11. Duty of confidentiality.

All alerts and their annexes shall not be used beyond the time required to follow them up.

It is foreseen that the identity of the person making the report together with any other information from which such identity may be inferred, directly or indirectly, shall not be disclosed without the express consent of the person making the report to persons other than those competent to receive or follow up the reports,

expressly authorised to process such data pursuant to Articles 29 and 32(4) of Regulation (EU) No 2016/679 and Article 2 quaterdecies of the Personal Data Protection Code laid down in Legislative Decree No 196 of 30 June 2003.

The Company shall protect the identity of the persons involved, the facilitators and the persons mentioned in the report until the conclusion of the proceedings initiated on account of the report, in compliance with the same guarantees provided for in favour of the reporting person.

Mitigating circumstances for the protection of the right to privacy include:

- In the context of criminal proceedings, the identity of the reporter is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure: the obligation of secrecy is imposed on the acts of the preliminary investigation until such time as the suspect has the right to have knowledge of them and, in any case, no later than the closure of that phase;
- Within the framework of the proceedings established at the Court of Auditors, the identity of the reporter cannot be disclosed until the investigation phase is closed;

- within the framework of disciplinary proceedings, the identity of the whistleblower may not be disclosed where the allegation of the disciplinary charge is based on investigations that are separate from and additional to the report, even if consequent to it;
- where the accusation is based, in whole or in part, on the report and knowledge of the identity of theperson making the report is indispensable for the accused's defence, the report will only be usable forthe purposes of disciplinary proceedings if the person making the report expressly agrees to reveal his identity;
- in cases of disciplinary proceedings initiated against the alleged perpetrator of the reported conduct, written notice shall be given to the whistleblower of the reasons for the disclosure of confidential datawhen such disclosure is also indispensable for the defence of the person concerned.

The report and the documents attached to it are exempt from the right of access to administrative acts provided for by Articles 22 et seq. of Law No. 241/1990 and from generalised civic access provided for by Articles 5 et seq. of Legislative Decree No. 33/2013;
The administrations and bodies involved in the handling of reports guarantee confidentiality during all stages of the reporting process, including the possible transfer of reports to other competent authorities.

12. Protection of personal data.

All processing of personal data, including communication between the competent authorities, is carried out in accordance with the law:

- of Regulation (EU) 2016/679;
- of Legislative Decree No 196 of 30 June 2003, as amended and supplemented.

The disclosure of personal data by EU institutions, bodies or entities is made in accordance with Regulation (EU) No 2018/1725.
The processing of personal data relating to the receipt and handling of reports is carried out by the data controller, in compliance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679, by first providing appropriate information to the reporting subjects and the persons concerned and by taking appropriate measures to protect the rights and freedoms of the persons concerned.

13. Protection and support measures.

Appropriate measures are in place to protect whistleblowers from direct retaliation and indirect retaliation. The protective measures apply if at the time of the report the reporting person had

reasonable grounds to believe that the information on the reported violations was true, fell within the objective scope and the reporting procedure was followed.
In the case of defamation or slander, established by conviction even at first instance, protections are not guaranteed.
Protection measures also apply:

(a) to facilitators;
(b) persons in the same employment context as the reporting/whistleblowing person who are linked to him/her by a stable emotional or family relationship up to the fourth degree;
(c) co-workers of the reporting/whistleblower who work in the same work environment as the reporting/whistleblower and who have a regular and current relationship with the reporting/whistleblower;

(d) entities owned by the reporting/whistleblowing person or for which the same persons work, as well asentities operating in the same work environment as those persons.

13.1 Proibition of retaliation

The whistleblower and the persons referred to in the preceding paragraph may not suffer any retaliation. By way of information and without limitation, retaliation is considered to be

- dismissal, suspension or equivalent measures;
- relegation in grade, or non-promotion;
- the change of functions;
- the change of workplace;
- salary reduction;
- the modification of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes, or negative references;
- the adoption of disciplinary measures or other sanctions, including pecuniary ones;
- coercion;
- intimidation;
- harassment;
- ostracism;
- discrimination or otherwise unfavourable treatment;
- 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;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, particularly on social media,
- economic or financial harm, including loss of economic opportunities and loss of income;

- -inclusion in 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;
- the early termination or cancellation of a contract for the supply of goods or services;
- cancellation of a licence or permit;
- the request to undergo psychiatric or medical examinations.

Acts taken in violation of the prohibition of retaliation are null and void.
In the context of judicial or administrative proceedings, or in the case of out-of-court disputes concerning the ascertainment of the prohibited conduct, acts or omissions in respect of the reporting persons only, it is presumed that they were carried out as a result of the reporting. The burden of proving that such conduct or acts are motivated by reasons unrelated to the reporting is the responsibility of the person who carried out the retaliatory acts.
Whistleblowers may inform ANAC of retaliation they believe they have suffered, whether attempted or contemplated.
The ANAC informs the National Labour Inspectorate, for measures within its competence.

13.2 Support measures.

The reporting party may turn to Third Sector entities on the list published on the ANAC website. These are bodies that carry out activities of general interest for the pursuit, on a non-profit basis, of civic, solidarity and socially useful purposes ("promotion of the culture of legality, peace among peoples, non-violence and non-armed defence; promotion and protection of human, civil, social and political rights, as well as the rights of consumers and users of general interest activities, promotion of equal opportunities and mutual aid initiatives, including time banks and solidarity purchasing groups") and that have entered into agreements with ANAC.
The support measures provided consist of information, assistance and advice free of charge on how to report and on the protection from retaliation offered by national and EU legislation, on the rights of the person concerned and on the terms and conditions of access to legal aid.

13.3 Limitation of liability of the reporter.

There is no liability (including civil or administrative liability) for anyone who discloses or disseminates information about violations:

- covered by the obligation of secrecy,
- related to copyright protection,
- of the provisions on the protection of personal data,
- which offend the reputation of the person involved or denounced

whether, at the time of the disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of the same information was necessary to disclose the breach and the reporting was consistent with the conditions for protection.

In addition, protective measures include:

- The rights to make a report and the related protections cannot be restricted in a contractual manner;
- the exclusion of all other liability, including civil and administrative liability, for the acquisition of or access to information on violations, unless the conduct constitutes a criminal offence;
- the exclusion of any other liability with regard to conduct, acts, omissions carried out if connected to the report and strictly necessary to disclose the violation or, in any case, not connected to the report.

13.4 Penalty regime.

The disciplinary system adopted by the Company pursuant to Article 6(2)(e) of Legislative Decree No. 231/2001, and referred to in the General Section of the 231 Model, must be considered amended and supplemented with the provision of sanctions to be applied against those who are found to be responsible for the following conduct:

- commission of retaliation or proposed adoption, obstruction of reporting (even attempted), or breachof confidentiality obligations;
- Failure to set up reporting channels, failure to adopt procedures for handling them, adoption of procedures that do not comply with the requirements of the decree, or failure to verify and analyse reports;
- criminal liability of the person making the report, ascertained even by a judgment at first instance, for offences of defamation or slander, or civil liability for the same offence, in cases of wilful misconductor gross negligence;

as well as against anyone who violates this procedure.

For the same offences, ANAC may intervene with the application of pecuniary administrative sanctions (from EUR 500 up to EUR 50,000) in the event of a finding of the same offences.