WHISTLEBLOWING POLICY

adopted by

MAGIS S.p.A

INDEX

Definitions

- ***Report*:** written or oral communications concerning information on Breaches.
- ***Breaches***: conduct, acts or omissions that harm the public interest or the integrity of the public administration or private entity.
- ***Whistleblower***: the natural person who reports or publicly discloses information on Breaches acquired in the context of their work activities.
- ***Information on breaches***: information, including well-founded suspicions, regarding breaches committed or which, on the basis of concrete elements, could be committed in the organization with which the Whistleblower or the person who files a complaint with the judicial or accounting authority maintains a legal relationship in the public or private sector, as well as the elements concerning conduct aimed at concealing such breaches.
- ***Facilitator***: the natural person who assists a Whistleblower in the reporting process, who operates within the same work context and whose assistance must be kept confidential.
- ***Person Involved***: the natural or legal person mentioned in the report as the person to whom the Breach is attributed or as a person otherwise involved in the Breach.
- ***Public disclosure***: making public information about breaches through the press or electronic means or otherwise through means of dissemination capable of reaching a large number of people.
- ***Retaliation***: any conduct, act or omission, whether attempted or threatened, carried out by reason of the whistleblowing report, the complaint to the judicial or accounting authority or the public disclosure and which causes or may cause unfair damage to the Whistleblower or to the person who made the complaint, directly or indirectly.
- ***Whistleblowing manager:*** the subject entrusted with the management of the reporting channel to assess the existence of the facts reported, the outcome of the investigations and any measures taken.
- ***Follow-up***: the action taken by the Whistleblowing manager to assess the existence of the reported facts, the outcome of the investigations and any measures taken.
- ***Feedback***: communication to the Whistleblower of information relating to the follow-up that is being given or intended to be given to the whistleblowing report.

1. What is Whistleblowing

The "*Whistleblowing*" is an institution of Anglo-Saxon origin, aimed at regulating and facilitating the process of reporting offenses or other irregularities of which the reporting subject (hereinafter the "Whistleblower") has become aware and which provides, for the latter, significant forms of protection.

The protection of employees who report offenses was regulated for the first time in the public sector by art. 54-bis of Legislative Decree no. 165 of 2001. The institution of whistleblowing as a system for the prevention of corruption was introduced by Law no. 190 of 6 November 2012 on "*Provisions for the prevention and repression of corruption and illegality in the Public Administration*".

Law no. 179/2017, containing "*Provisions for the protection of authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship*", consolidated the existing legislation in the public and private sectors, strengthening the tools to protect whistleblowers and intervened on the regulation of the liability of entities, going to integrate the Art. 6 of Legislative Decree 231/2001.

At the end, Legislative Decree no. 24 of 10 March 2023 as amended from time to time (hereinafter also "Whistleblowing Decree") implemented 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 laying down provisions concerning the protection of persons who report breaches of national legal provisions.

2. Purpose of the Policy

This Whistleblowing Policy (hereinafter "Policy") aims to govern the process of sending, receiving, analyzing and processing, including archiving and cancellation, of Whistleblowing reports, by anyone coming from or transmitted, even confidentially or anonymously, as well as the protection of the Whistleblower and the Persons Involved.

In compliance with the legislation, **MAGIS S.p.A.** (hereinafter "the Company"), promotes the dissemination and use of whistleblowing as a fundamental measure to prevent and fight corruption and illegal conduct, as well as to protect the Whistleblowers with the provisions and principles set out in the following documents:

- Legislative Decree no. 24 of 10 March 2023 as amended from time to time;
- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019;
- European Regulation no. 679/2016 and Legislative Decree 196/2003 and subsequent amendments and additions;
- ANAC Guidelines on the protection of persons reporting violations of Union law and protection of persons reporting violations of national regulatory provisions, adopted by Resolution no. 311 of 12 July 2023;
- ANAC Guidelines on internal reporting channels, Resolution No. 478 of 26 November 2025;
- Organizational Model pursuant to Legislative Decree 231/2001 (hereinafter also referred to as "Model") and Code of Ethics.

3. The Whistleblower - subjective scope of application

The protection measures provided for in this Policy apply to the **Whistleblower** that is the person who reports the breaches of which he has become aware in his work context.

Pursuant to this Policy, the subjects entitled to report breaches are:

a) **subjects within the Company** and Group companies (e.g. but not limited to, persons with administrative, management, control and supervision or representation functions, employees and workers employed under temporary employment contracts, interns and trainees; volunteers, para-subordinate workers and collaborators without VAT status, even occasional);

b) **subjects external to the Company** and Group companies (e.g., but not limited to, self-employed workers, external collaborators, freelancers and consultants holding an independent VAT position, those whose employment relationship has ended or has not yet begun, such as former employees or candidates, shareholders and persons with administrative functions, management, control, supervision or representation, even if these functions are exercised by way of mere fact).

The protection measures shall also apply to:
- facilitators, i.e. those who assist the Whistleblower in the reporting process, operating within the same work context;
- persons linked to the Whistleblower by a stable emotional or kinship bond within the fourth degree, who operate in the same work context;
- work colleagues of the Whistleblower;
- Entities owned by the Whistleblower or operating in the same working context;
- Anonymous whistleblower, if subsequently identified and subject to retaliation.

4. Breaches – objective scope

The "**Breaches**" for which it is possible to report are identified in behaviors, acts or omissions that damage the public interest or the integrity of the public administration or the Company of which the Whistleblower has become aware in his or her work context and consist of:
1) administrative, accounting, civil or criminal offences;
2) significant unlawful conduct pursuant to Legislative Decree 231/2001, or breaches of the organization and management models provided for therein;
3) offences falling 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; protection of privacy and protection of personal data and security of network and information systems;
4) acts or omissions affecting the financial interests of the Union;
5) acts or omissions concerning the internal market;
6) acts or behaviour which defeat the object or purpose of the provisions contained in Union acts.

Discriminatory or harassing behaviors that undermine personal dignity and compromise the healthiness of the work environment are also considered breaches under Legislative Decree 231/2001, as they constitute violations of workplace health and safety regulations (Legislative Decree 81/2008). Such conduct, in addition to conflicting with the principles of equal opportunity, may constitute offenses relevant for the administrative liability of entities pursuant to Article *25-septies* of Legislative Decree 231/2001.

Please refer to **Annex A** for details of the breaches that can be reported.

They are not considered Breaches and therefore the protection measures provided for in this Policy do not apply:
- disputes, claims or requests related to a personal interest of the Whistleblower or of the person who has filed a complaint with the judicial or accounting authority that relate exclusively to their individual employment relationships, or inherent to their employment relationships with hierarchically superordinate figures;
- complaints relating to commercial activities (e.g. complaints);
- reports of breaches where already regulated on a mandatory basis by European Union or national acts (see: Annex to the Whistleblowing Decree, Part II; Annex to the EU Directive, Part II – Financial services, products and markets; prevention of money laundering and terrorist financing; transport safety; environmental protection);

- reports of national security breaches, as well as procurement relating to defence or national security aspects, unless such aspects fall within the relevant secondary Union law.

5. Subject and content of reports

Reports are written or oral communications concerning **information on Breaches** attributable to the Company's personnel or third parties.

Reports must be made in good faith and identifiable, i.e. adequately substantiated and based on precise and consistent elements.

Attempts at breaches, or conduct aimed at concealing breaches, as well as illegal activities not yet carried out but that the whistleblower reasonably believes may occur in the presence of precise and consistent elements are also reportable whistleblowing.

The content of each report can be as follows:

- type of Whistleblower in relation to the employment relationship with the Company, for example:
  - employee;
  - self-employed;
  - collaborator / Consultant / freelancer;
  - voluntary;
  - trainee;
  - other (to be specified in the report);
- name and surname of the Whistleblower (if he wishes), company to which he belongs and contact details;
- name of the Company in which the Infringement took place and the location of the Company;
- type of illegal conduct: corruption, conflicts of interest, illegitimate contracts, etc.;
- clear and complete description of the facts reported and how it became aware of them;
- where available, circumstances of time and place where the reported acts were committed;
- general information or other elements which allow the identification of the «Person Involved» or otherwise implicated in the Breach (such as, for example, the company he belongs to, qualification and function in which he carries out the activity);
- period and place in which the unlawful conduct was carried out or if the conduct is still ongoing;
- indication whether the illegal conduct has already been reported. If yes, to whom, when and how;
- any documents which may confirm the validity of the facts reported and the possible transmission of their annexes;
- indication of any other persons who can inform on the facts reported.

Only situations of which a subject has become directly aware, and not through an intermediary, in the performance of their work activities, albeit randomly, should be reported.

5.1. Anonymous report

Anonymous whistleblowing, as they lack elements that allow the author to be uniquely identified, are taken into consideration for further study and verification only if they are adequately detailed and verifiable, made in great detail and in any case such as to bring out facts and situations related to clearly determined and identifiable contexts (eg: indication of names or particular qualifications, mention of specific offices, procedures or particular events, etc.).

In the absence of the aforementioned elements, the anonymous report is exclusively archived.

The protection measures, as provided for in par. 12 of this Policy, do not apply to the anonymous Whistleblower unless he has been subsequently identified and subject to retaliation.

6. Reporting Channels

The Company, in order to facilitate the receipt of whistleblowing reports, having previously heard the representatives or trade unions referred to in Article 51 of Legislative Decree no. 81 of 2015, has set up special reporting channels that guarantee, also through the use of encryption tools, the confidentiality of the identity of the Whistleblower, of the Person Involved or in any case mentioned in the report; as well as the confidentiality of the content of the whistleblowing and related documentation.

The following requirements must be complied with to submit reports:

1. to submit the report / communication and to carry out the subsequent integrations, a single channel must be used;
2. the use of the platform is the priority channel;
3. duplications of the same report should not be submitted.

The Company has the following internal channels to make Reports in **written form** through:

- ✓ IT platform accessible from the Company's website, **https://magis.integrityline.com**, by filling out the appropriate form;
- ✓ paper letter sent to the attention of the Whistleblowing Committee with the words PERSONAL CONFIDENTIAL to the following address: Via Ponte Cerretano, 24, 50050 Cerreto Guidi, (FI), registered office of the company.

Or **orally**, through**:**

- ✓ direct meeting with the Whistleblowing Committee, set within a reasonable time at the explicit request of the Whistleblower;
- ✓ voice messaging and morphing system, through the IT platform accessible from the Company's website, **https://magis.integrityline.com.**

7. Management of internal reporting channels

The Company has entrusted the management of the internal reporting channels to a dedicated office, the Whistleblowing Committee (hereinafter also the "whistleblowing manager"/" Committee"), specifically trained and equipped with the necessary skills, in order to follow up on the reports received.

The current composition of the Whistleblowing Committee is shown below:

- Dr. Francesca Marzi, CFO & HR Manager;
- Dr. Daniele Toci, Administrative Manager.

Any person other than the Committee who receives a "whistleblowing report"[1] must transmit it, within 72 working hours of its receipt, to the competent internal office, giving simultaneous notice of the transmission to the Whistleblower.

7.1. Duties of the Whistleblowing Committee

The Whistleblowing Committee carries out the following activities:

a) issues the Whistleblower with acknowledgment of receipt of the report within seven days of the date of receipt;
b) maintain discussions with the Whistleblower and can request additions from the latter if necessary;
c) diligently following up on the reports received;

[1] In such cases, if the whistleblower does not expressly declare that he or she wishes to benefit from the protections provided, or this intention is not inferred from the report, the same is not considered as a whistleblowing report, but rather as ordinary as the protections provided for by Legislative Decree 24/2023 do not apply.

d) provides feedback to the report within three months from the date of the acknowledgment of receipt or, in the absence of such notice, within three months from the expiry of the seven-day period from the submission of the report;
e) makes clear information available on the channel, procedures and conditions for making internal reports, as well as on the channel, procedures and conditions for making external reports. The aforementioned information is displayed and made easily visible in the workplace, as well as accessible to people who, although not frequenting the workplace, have a legal relationship with the Company. If they have their own website, public sector and private sector entities also publish the information referred to in this letter in a dedicated section of the aforementioned website.

The Committee establishes a register of reports, containing details of the reports received, the investigations carried out, and their outcomes.

Each year, the Committee reports on its activities to the Company's Administrative Body.

7.2. Role of the Whistleblowing Committee

The role assigned to the Whistleblowing Committee relates to the mere management of internal reporting channels, including the drafting of an opinion on the admissibility of the report, excluding any possible decision-making activity regarding the follow-up to be given to the reports deemed admissible, the latter activity being the responsibility of the Company's Administrative Body and/or Control Body.

The meetings of the Committee are convened upon request and are validly constituted with the presence of at least two members of the Committee; in cases of conflict of interest, the member who is the subject of the report must refrain from participating in the management activities of the report.

All meetings of the Committee are specifically recorded, the minutes of the meetings are kept by the Committee itself, together with the paper documentation relating to the reports. The documentation in electronic/digital format relating to the reports is kept in the specific digital area reserved for the Committee.

The whistleblowing process consists of the following steps:

a) preliminary assessment of the report;
b) internal investigations;
c) conclusion of the investigation.

7.3. Preliminary assessment of the report

To give proper follow up on the reports received, the whistleblowing manager carries out a preliminary assessment of the contents of the report received, to verify the validity of the facts and/or circumstances indicated, as well as to assess their relevance, scope and potential risks.

Where deemed appropriate, the whistleblowing manager has the right to maintain discussions with the Whistleblower and can ask the latter, if necessary, for documentary or informative additions.

In carrying out the aforesaid analysis, the whistleblowing manager can rely on the support of the company functions competent from time to time on the matter reported and, where deemed appropriate, of specialized external consultants, ensuring, in any case, the confidentiality of the whistleblower's data, except as provided by par. 12.1.

7.4. Report received via EQS platform – IT tool

The report and its subsequent management take place according to the following steps:

1. The whistleblower enters the report through the web platform which at the same time sends an e-mail notification to the Committee;

2. The platform automatically assigns a protocol number and transmits this number to the Whistleblower at the same time as the Report is opened. This protocol number allows the Committee to start a dialogue with the whistleblower and to the latter to verify, again via the platform, the status of his report;
3. The Committee must evaluate every possible case of conflict of interest of one of its members with respect to the report excluding this one from the whistleblowing report management and declaring any situation of conflict, even if only apparent or potential;
4. The Committee starts with the preliminary analysis;
5. The Preliminary assessment is limited to verifying the existence of the minimum requirements necessary for reporting (by way of non-exhaustive example: presence of specific and non-generic objective elements of complaint; belonging to the categories of whistleblowers provided for by the decree);
6. Within **7 days of receipt of the report,** the the Committee, proceeds to issue the Whistleblower with an acknowledgement of receipt of the report, according to the above protocol number;
7. If the whistleblower requests a meeting with the Committee via the platform, the necessary actions are taken to follow up on the request within a reasonable time;
8. Based on the preliminary assessment, the report will be classified into one of the following categories:
   a. not verifiable (it is not possible to proceed with further analysis due to lack of evidence or information);
   b. manifestly unfounded, it will therefore not be necessary to carry out further analyses except for what is potentially attributable to potential disciplinary action;
   c. well-founded and verifiable; It is therefore necessary, as well as possible, to deepen its analysis through internal investigations.
9. If case 8.a or 8.b is confirmed, the Committee, closes the report on the platform, thus simultaneously sending the communication of the outcome to the Whistleblower (as required within three months from the date of the acknowledgment of receipt); if deemed appropriate, the Committee informs the Administrative Body and/or the Control Body, for the purposes of any disciplinary actions as indicated in par. 15 and without prejudice to the conditions for protection referred to in par. 14.
10. If case 8.c is confirmed, the Committee informs the Administrative Body and/or the Control Body of the Company and initiates an internal investigation, also with the help of external professionals, which consists of:
    - internal investigations;
    - conclusion of the investigation.

In any case, the Committee must provide feedback on the report **within three months** from the date of the acknowledgment of receipt**, communicating to the Whistleblower the information relating to the follow-up that is given or intended to be given to the report**.

The EQS platform allows the export and saving of data on your PC or company network folder, the Committee undertake not to carry out these operations unless expressly authorized by the Administrative and/or Control Body and according to the agreed procedures.

7.5. Report received via paper letter.

Upon receipt of the report, the Committee proceeds to register it with a progressive number and relative date in a specially dedicated register.

Within **7 days of receipt of the report, the** Committee shall proceed to issue the Whistleblower with an acknowledgement of receipt of the report, according to the contacts indicated by the Whistleblower.

In this phase the Committee also proceeds:
- examining the elements contained in the report to verify whether it is properly a "whistleblowing" or an "anonymous whistleblowing";

- identifying the Whistleblower, in terms of identity, qualification and role, as the subject from whom it is possible to receive further information deemed useful for the purpose of assessing the report;
- to anonymize the personal data being reported or the contents of the report where it is necessary to share it with other company functions and/or external consultants[2];
- adopting all appropriate security measures to prevent third parties from tracing the identity of the Whistleblower as well as the conservation of the report and supporting documentation in a confidential place.

The Committee must evaluate every possible case of conflict of interest of a member with respect to the report excluding this one from the whistleblowing report management and declaring any situation of conflict, even if only apparent or potential.

7.6. Reports received via face-to-face meeting

When, at the request of the Whistleblower, the report is made orally during a meeting with the Committee, the same, subject to the Whistleblower's consent, is documented by the Committee by means of a minute of the meeting, which the Whistleblower may verify and confirm by signing it.

7.7. Internal investigations

Where, following the preliminary analysis activity, useful and sufficient elements emerge or are in any case inferable to evaluate the report as founded, the whistleblowing manager will initiate any specific in-depth activities within the Company to:

- verify information regarding possible breaches of the law or corporate policies and, in general, to ascertain - and when possible, prevent - facts that may compromise the Company or its employees, and which could give rise to civil, administrative, or criminal liability, or damages reputational;
- guaranteeing the Company the preparation of an adequate defensive strategy and promptly implementing any remedial actions.

Specifically, the whistleblowing manager will be able to:

a) initiate specific analysis activities making use, if deemed appropriate, of the competent functions of the Company and/or of the Group and/or of consultants external to the Company itself;
b) interact with the Whistleblower, requesting, if necessary, additions;
c) interviewing with people/functions who may be able to report useful circumstances on the facts reported and acquire documents;
d) evaluate which type of Breaches are reported among those indicated in par. 4., involving the Supervisory Body where they integrate one or more types of crime from which liability may derive pursuant to Legislative Decree 231/2001; or, while not integrating any type of crime, pertain to conducts committed in contravention of regulations, procedures, protocols or provisions contained within the Model or the documents attached to it;
e) if the report refers a crime, evaluate the opportunity to carry out internal investigations with the formalities of the defensive investigations provided for by the Code of Criminal Procedure, giving a mandate to a defender[3];
f) formulate recommendations regarding the adoption of urgent corrective actions to be implemented in the areas/functions of the Company in which the Breaches were committed or implicated in the report;

[2] For example, by separating personal data of the Whistleblower (where communicated) from the content of the report, providing for the use of replacement codes so that the report can be processed anonymously and make it possible to subsequently associate it with the identity of the author only in cases where this is strictly necessary.

[3] Unlike internal investigations, defensive investigations, including preventive ones, are governed by articles 327bis and 391bis ss. Code of Criminal Procedure; are conducted by a defender provided with a specific mandate or by his substitutes and technical consultants; they can be used in the context of a trial at the discretion of the defender, in compliance with the code of procedure; ensure maximum protection of procedural secrecy and the application of the defense guarantees pursuant to art. 103 Code of Criminal Procedure.

g) conclude the internal investigation at any time if the groundlessness of the report is established and, if the report demonstrated to be knowingly false, with willful misconduct or gross negligence, informing the Management Body and/or the Controlling Body, suggesting any disciplinary actions, as described in par. 15 and without prejudice to the conditions for the protection referred to in par. 14.

It is not up to the whistleblowing manager to ascertain individual responsibilities of whatever nature they may be, nor to carry out legitimacy or merit checks on acts and measures adopted by the entity/administration subject to the report, under penalty of encroaching on the competences of the persons responsible for this within each body or administration or the judiciary.

In any case, the whistleblowing manager must respond to the report **within three months** from the date of the acknowledgment of receipt or, in the absence of such notice, within three months from the expiry of the term of seven days from the report, communicating to the Whistleblower the follow-up that is given or intended to be given to the report.

7.8. Conclusion of the investigation

At the conclusion of the internal investigations, the whistleblowing manager communicates the final results of the assessment, so that the most appropriate measures are taken, therefore:

- ✓ will inform the Management Body and/or the Controlling Body and the Supervisory Body about the activity carried out and any corrective actions that can be recommended to the Company to strengthen the internal control system. It will be the responsibility of the Management Body and/or the Controlling Body to appoint the competent functions for the definition and implementation of the initiatives to be undertaken to protect the interests of the Company and/or of the Group (such as, by way of example and not limited to: legal actions, adoption of disciplinary measures, suspension/cancellation from the supplier register, etc.);
- ✓ will communicate to the whistleblower the reasoned final outcome of the investigation, which may also consist of:
  - archiving (e.g. minor extent of the Breach);
  - transmission to the competent authorities;
  - notification of the corrective actions initiated by the Company and of the measures taken against the Person Involved;
  - disciplinary sanction against the whistleblower;
- ✓ will close the report, archiving all the documentation relating to the investigation, including the final report, in such a way as to avoid access by unauthorized third parties.

In all phases, the whistleblowing manager ensures the protection of the identity of the Whistleblower and the Person Involved.

Upon the outcome of the investigation, the company function or competent corporate body evaluates whether to take the disciplinary measure deemed most appropriate pursuant to the provisions of par. 15.

8. Reporting activities of the Supervisory Body

Pursuant to the Model, specific information flows are established between the whistleblowing manager and the Supervisory Body (also "SB") and by the latter and towards the Management Body of the Company, in particular the SB:

- periodically, at least annually, sends a report on the activity carried out in the previous period, which summarizes, among other things, the results of the investigations on reports received through the reporting channels, including the possible adoption of disciplinary and/or legal actions. The SB evaluates the data relating to the reports within its competence in order to:

- identify the areas of possible criticality for which it is advisable a strengthening of the internal control system;
- suggest to the Management Body the adoption of possible further prevention and/or updating measures of the Model.

- by event, following the checks carried out on the reports, transmits a written reporting regarding ascertained Breaches which may involve liability for the Company or facts of particular relevance which suggest immediate corrective actions, for the purposes of appropriate measures.

9. Retention of documentation relating to Reports

The whistleblowing manager ensures, also through the IT systems used, the traceability of data and information and ensures the retention and archiving of the documentation produced, paper and / or electronic, to allow the reconstruction of the different phases of the reporting management process.

The Reports, internal and external, and the related documentation, paper, electronic and digital, are kept, by the whistleblowing manager, after adopting every appropriate precaution in order to guarantee maximum confidentiality.

When, at the request of the Whistleblower, the report is made orally during a meeting with the whistleblowing manager, the same, subject to the consent of the Whistleblower, is documented by the whistleblowing manager by means of a minute, which the Whistleblower can verify, confirming and signing it.

Except as provided for by specific provisions of law, access to data relating to Reports is allowed only to the whistleblowing manager.

The original documentation of the Reports is kept in special archives with appropriate security and confidentiality standards.

Internal reports and related documentation, paper, electronic and digital, are maintained for the time necessary to process the report and in any case no later than **five years** from the date of communication of the final outcome of the reporting procedure in compliance with the confidentiality obligations referred to in Article 12 of the Whistleblowing Decree and the principles established by art. 5, paragraph 1, letter e) of Regulation (EU) 2016/679[4] and art. 3, paragraph 1, letter e) of Legislative Decree no. 51 of 2018,[5] unless other legal obligations.

10. External reports via ANAC

Pursuant to the Whistleblowing Decree, the National Anti-Corruption Authority (ANAC) has activated an external reporting channel that guarantees, also through the use of encryption tools, the confidentiality of the identity of the Whistleblower, the Person Involved and the person mentioned in the report, as well as the confidentiality of the content of the report and related documentation.

The Whistleblower can make an external report ONLY if, at the time of its submission, one of the following conditions is met:

- there is no mandatory activation of the internal reporting channel, i.e. this, although mandatory, is not active or, even if activated, does not comply with the Whistleblowing Decree;

[4] Art. 5, paragraph 1, letter e) Regulation (EU) 2016/679: "Personal data are maintained in a form that allows identification of data subjects for a period of time not exceeding the achievement of the purposes for which they are processed ; personal data may be retained for longer periods provided that they are processed exclusively for archiving purposes in the public interest, scientific or historical research or statistical purposes, in accordance with Article 89(1) ("processing for archiving purposes in the public interest, scientific or historical research or for statistical purposes is subject to adequate safeguards for the rights and freedoms of the data subject. These safeguards ensure that technical and organizational measures have been put in place, in particular to ensure compliance with the principle of minimization data. These measures may include pseudonymisation, provided that the purposes in question can be achieved in this way") without prejudice to the implementation of adequate technical and organizational measures required by the Regulation to protect the rights and freedoms of the data subject ("retention limitation»)"

[5] Art. 3, paragraph 1, letter e) Legislative Decree no. 51 of 2018: "Personal data are stored in ways that allow the identification of data subjects for the time necessary to achieve the purposes for which they are processed, subjected to periodic examination to verify the persistent need for conservation, canceled or anonymized once this period is expired.

- the Whistleblower has already made an internal report and the same has not been followed up
- the Whistleblower has reasonable grounds to believe that, if he made an internal report, it would not be effectively followed up or that it could determine the risk of retaliation;
- the Whistleblower has reasonable grounds to believe that the Breach may constitute an imminent or manifest danger to the public interest.

The Whistleblower must assess the occurrence of the above conditions.

Reports at ANAC can be made:

✓ **in writing** via an IT platform accessible from the ANAC website: https: //www.anticorruzione.it/-/whistleblowing, by filling the Form for reporting illicit conduct pursuant to Legislative Decree no. 24/2023;
✓ or **orally** through telephone lines or dedicated voice messaging systems or direct meeting set within a reasonable time, at the request of the Whistleblower.

ANAC publishes on its website a dedicated section that includes, inter alia, its contacts, such as, in particular, the telephone number, indicating whether or not telephone conversations are recorded, the postal address and the e-mail address, ordinary and certified.

In particular, ANAC designates personnel specifically trained for the management of the external reporting channel and provides:
✓ provide data subjects with information on the use of the external reporting channel and the internal reporting channel, as well as on protection measures;
✓ give notice to the Whistleblower of the receipt of the external report within seven days from the date of its receipt, unless explicitly requested otherwise by the Whistleblower or unless ANAC considers that the notice would jeopardize the protection of the confidentiality of the identity of the Whistleblower;
✓ interact with the Whistleblower, requesting additions, if necessary;
✓ diligently follow up on the reports received;
✓ carry out the investigation necessary to follow up on the report, including through hearings and acquisition of documents;
✓ give feedback to the Whistleblower within 3 months or, if justified reasons occur, 6 months from the date of acknowledgment of receipt of the external report or, in the absence of such notice, from the expiry of 7 days from receipt;
✓ communicate to the Whistleblower the result, which may also consist of:
  - archiving (e.g. minor extent of the Breach);
  - transmission to the competent authorities;
  - recommendation;
  - administrative sanction.

11. Public disclosure

The Whistleblower may make information on Breaches public through:
- the press;
- electronic means;
- other means of diffusion capable of reaching a large number of people (e.g. TV, social networks).

The Whistleblower who makes a public disclosure, benefits from the protection provided by the Whistleblowing Decree ONLY AND EXCLUSIVELY if, at the time of public disclosure, one of the following conditions is met:
- the Whistleblower has previously made an internal and external report or directly an external report, and has not received a response within the terms provided for, in this Policy;
- the Whistleblower has reasonable grounds to believe that the Breach may constitute an imminent or manifest danger to the public interest;

- the Whistleblower has reasonable grounds to believe that the external report may involve the risk of retaliation or may not be followed up effectively due to the specific circumstances of the concrete case (e.g. concealment or destruction of evidence; well-founded fear that the person receiving the report may be colluded with the perpetrator of the Breach or involved in the Breach itself).

12. Protection of the whistleblower

12.1. Confidentiality

The Company guarantees the absolute confidentiality of the identity of the Whistleblower, using for this purpose criteria and methods of communication suitable to protect both the integrity of the persons mentioned in the Reports and the anonymity of the Whistleblower. The Company censures any conduct that violates the measures envisaged to protect the Whistleblower through the application of the provisions of this Whistleblowing Policy.

The identity of the Whistleblower and any other information from which it can be deduced, directly or indirectly, this identity **cannot be revealed,** without his express consent**, to persons other than those competent to receive or follow up on reports, expressly authorized to process such data in accordance with privacy legislation.**

The whistleblowing manager may reveal the identity of the Whistleblower to external consultants (e.g. legal advisors) **only with the express and formal consent of the Whistleblower.**

In the context of criminal proceedings, the identity of the Whistleblower is covered by secrecy in the manner and within the limits established by art. 329 Code of Criminal Procedure until the accused can have knowledge of it and, in any case, no later than the closure of the preliminary investigations.

As part of the disciplinary procedure:
- if the disciplinary dispute is based on separate and additional assessments with respect to the report, the identity of the Whistleblower cannot be disclosed;
- if the dispute is based, in whole or in part, on the reporting and knowledge of the identity of the whistleblower is essential for the defense of the accused, the whistleblowing can only be used in the presence of the whistleblower's express consent to the disclosure of his identity.

If the disclosure of the whistleblower's identity (or of the information from which this identity can be deduced, directly or indirectly) is essential for the purpose of defending the Person Involved or mentioned in the report, the whistleblowing manager must notify the Whistleblower, indicating of the reasons why it would be necessary to reveal his identity.

12.2. Prohibition of retaliation

The Company prohibits any form of retaliatory, discriminatory, or otherwise penalizing action, carried out both directly and indirectly against the Whistleblower and reminds all its personnel that any dismissal, demotion, or other retaliatory or discriminatory measure is null by law.

The Whistleblower who believes he has suffered retaliation can report it to the ANAC, which can entrust the Labor Inspectorate with carrying out the related investigations and checks.

For further protection of the Whistleblower, it is envisaged that the adoption of discriminatory measures against the Whistleblower can be reported to the National Labor Inspectorate, not only by the Whistleblower, but also by any trade union organization indicated by the same.

Furthermore, the retaliatory or discriminatory dismissal of the Whistleblower, the change of duties, as well as any other retaliatory or discriminatory measure adopted against the Whistleblower are punishable under this Policy.

The position of the Whistleblower is also guaranteed by the burden placed on the employer to demonstrate that the measures taken against the Whistleblower are based on reasons unrelated to the reporting. For example in the case of disputes related to the imposition of disciplinary sanctions, or demotion, dismissal, transfer, or subjection of the Whistleblower to another organizational measure having direct or indirect negative effects on working conditions, subsequent to the submission of the report.

Below are the conducts that fall under direct or indirect retaliation:

- dismissal, suspension (also from training) or equivalent measures;
- demotion (relegation) or lack of promotion;
- change of duties, transfer, salary reduction, changes to working hours;
- negative merit notes (for variable payment);
- negative references;
- disciplinary measures;
- coercion, intimidation, harassment or ostracism;
- discrimination or any unfavorable treatment;
- non-conversion or non-renewal of a fixed-term employment contract into an open-ended employment contract (in the event of a legitimate expectation of conversion);
- 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 opportunity and loss of income;
- inclusion in the black list;
- early conclusion or cancellation of the contract for the supply of goods or services;
- cancellation of a license or permit;
- request to undergo psychiatric or medical tests.

12.3. Support measures

The list of Third Sector bodies that provide the Whistleblower with support measures such as information, assistance and advice free of charge has been established at the ANAC regarding:

- ✓ methods of reporting and protection from retaliation offered by national and EU regulatory provisions;
- ✓ rights of the Person Involved;
- ✓ methods and conditions of access to legal aid at the expense of the State.

12.4. Limitation di liability

It is not punishable who, through his report:

- reveals or disseminates information on violations covered by the obligation of secrecy other than that referred to in art. 1, paragraph 3, of the Whistleblowing Decree (for example forensic and medical professional secrecy), or relating to the protection of copyright or to the protection of personal data
- reveals or disseminates information about violations that offend the reputation of the Person Involved or mentioned in the report

<u>WHEN</u>

- at the time of disclosure or dissemination, there were reasonable grounds to believe that disclosure or dissemination of the same information was necessary to reveal the violation;

<u>AND</u>

- the report was made pursuant to the Whistleblowing Decree.

13. Protection of the Person Involved

During the preliminary analysis and/or preliminary investigation activities, the Person Involved and the one mentioned in the report could be notified of these activities, but, in no case, will a proceeding be initiated solely because of the mere report, in the absence of concrete evidence on its content.

Conversely, the Person Involved and the person mentioned in the report may not be informed regarding the recording of their data, if this is necessary to guarantee the correct management of the investigations and, in any case, in compliance with the provisions of current legislation and, where applicable, by the national collective labor agreement.

In any case, the identity of the Person Involved and the one mentioned in the report is protected until the conclusion of the proceedings initiated as a result of the report, in compliance with the same guarantees provided in favor of the Whistleblower, without prejudice to any further form of liability provided for by the law which imposes the obligation to communicate the name of the subject (for example in the case of requests from the Judicial Authority).

14. Conditions for protection

The protection measures provided for in this Policy apply only if:

- at the time of reporting or public disclosure, the Whistleblower had reasonable grounds to believe that the information on the reported Breaches were true and fell within the objective scope of this Policy pursuant to the Whistleblowing Decree;
- the reporting or public disclosure was made on the basis of the provisions of this Policy pursuant to the Whistleblowing Decree.

The protections are not guaranteed, and the Whistleblower is subject to a disciplinary sanction where it is ascertained:

- the criminal liability of the Whistleblower for the crimes of defamation or slander, even with a first instance sentence
- the civil liability of the Whistleblower, for the same reason, in cases of willful misconduct or gross negligence.

15. Sanctioning System

The Company will adopt the most appropriate disciplinary and/or legal measures to protect its rights, assets and image, against anyone who interferes with, or uses improperly, the reporting channels set up for reporting Breaches:

a) violating the measures to protect the Whistleblower or the Person Involved or otherwise mentioned in the report;
b) taking retaliatory or discriminatory actions against the Whistleblower consequent to the report;
c) making reports with willful misconduct or gross negligence that prove to be unfounded or opportunistic and/or for the sole purpose of slandering, defaming, or causing unjust damage and/or prejudice to the Person Involved or to other subjects mentioned in the report.

The Company will apply the most appropriate disciplinary and/or sanctioning measures, or judicial initiatives in the event that the Person Involved is held responsible for the Breaches indicated in the report, whether originating from internal or external reporting channels.

Disciplinary measures are applied in compliance with the provisions of art. 7 "Disciplinary sanctions" of Law 300 of 1970 (Workers' Statute). For further details on the disciplinary system adopted by the Company, please refer to the applicable CCNL (National Collective Labor Agreement) and/or to the General Part of the Model, in

which this Policy is expressly referred to and, in particular, to art. 8 dedicated to The disciplinary and civil sanctioning system.

16. Sanctions applied by ANAC

Failure to comply with the Whistleblowing Decree may result in the application by ANAC of the following pecuniary administrative sanctions:

- From 10,000 to 50,000 euros when it is ascertained that:
  - retaliation has been committed;
  - the report was obstructed, or an attempt was made to obstruct it;
  - the obligation of confidentiality has been violated.
- From 10,000 to 50,000 euros when it is ascertained that:
  - reporting channels have not been set up;
  - no procedures have been adopted for making and managing reports;
  - the adoption of these procedures does not comply with those envisaged by the Whistleblowing Decree;
  - the verification and analysis of the reports received was not carried out.
- From 500 to 2,500 euros, when it is ascertained that the whistleblower made the report with willful misconduct or gross negligence, unless he has been convicted, even in the first instance, of the crimes of defamation or slander or in any case for the same crimes committed with the complaint to the judicial or accounting authority.

17. Data Controller of personal data

The Data Controller of personal data relating to the reports and to the Whistleblowing Policy (hereinafter "Data Controller") is identified in the legal person of the Company **MAGIS S.p.A..**

The Data Controller is assisted, in relation to the management of reports, by the whistleblowing manager.

Company's activities related to the whistleblowing system involve the processing of the following data:

- personal data of the Person Involved and of the one mentioned in the report;
- personal data of the Whistleblower;
- other personal data that may be contained in the reports.

The Data Controller informs that personal data (including any sensitive, "particular" data, such as racial and ethnic origin, religious and philosophical beliefs, political opinions, membership of political parties, trade unions, as well as suitable personal data to reveal the state of health and sexual orientation) of the Whistleblower, of the Person Involved and of the one mentioned in the report, acquired during the management of the reports, will be treated in full compliance with the provisions of current personal data protection regulations and in any case in line with the provisions of the privacy information, and limited to those strictly necessary to verify the validity of the reports and their management.

18. Dissemination and Training

To ensure the dissemination, knowledge and application of this Policy, the whistleblowing manager provides clear information on the channel, on the procedures and on the conditions for making internal reports, as well as on the channel, on the procedures and on the conditions for carry out external reports, also through specific training activities.

This Policy is sent to:

- each member of the Board of Directors, the Board of Statutory Auditors and the Supervisory Body of the Company;
- each member of the Administrative Bodies, of the Boards of Statutory Auditors and of the Supervisory Bodies of the individual Italian subsidiaries;

- each employee of **MAGIS S.p.A.** and of its subsidiaries by posting in the spaces dedicated to company communications and in the IT portal reserved for communications to employees.

This Policy is also published on the Company's website.

The Human Resources function ensures the delivery of this Policy to employees upon hiring to certify that they have been read.

Furthermore, in order to spread full knowledge of the importance of the Whistleblowing Policy, the whistleblowing manager carries out specific training and information activities involving every company level aimed at knowing and understanding the contents of the Whistleblowing Policy.

ANNEX A – BREACHES

- Relevant offenses pursuant to Legislative Decree 231/01:
  - undue receipt of disbursements, fraud to the detriment of the State, a public body or the European Union or for the achievement of public funds, IT fraud to the detriment of the State or a public body and fraud in public supplies (art. 24);
  - cybercrimes (art. 24-bis);
  - organised crime (Art. 24-ter);
  - embezzlement, misappropriation of funds or movable property, extortion, undue inducement to give or promise benefits, and corruption (Art. 25);
  - counterfeiting of currency, public credit instruments, revenue stamps, and identification instruments or marks (Art. 25-bis);
  - crimes against industry and commerce (Art. 25-bis.1);
  - corporate crimes (Art. 25-ter);
  - crimes with terrorist purposes or aimed at subverting the democratic order, as provided by the Criminal code and special laws (Art. 25-quater);
  - practices of female genital mutilation (Art. 25-quater.1);
  - crimes against individual personality (Art. 25-quinquies);
  - market abuse offenses (Art. 25-sexies) and related administrative violations (Law No. 62 of April 18, 2005, Art. 9);
  - manslaughter and serious or very serious negligent injuries committed in violation of accident prevention and workplace health and safety regulations (Art. 25-septies);
  - receiving, laundering, and use of money, goods, or benefits of illicit origin, as well as self-laundering (Art. 25-octies);
  - crimes related to non-cash payment instruments and fraudulent transfer of assets (Art. 25-octies.1);
  - offences relating to breaches of European Union restrictive measures (Art. 25-octies.2);
  - crimes concerning copyright infringement (Art. 25-novies);
  - inducing someone not to make statements or to make false statements to judicial authorities (Art. 25-decies);
  - environmental crimes (Art. 25-undecies);
  - employment of third-country nationals whose stay is irregular (Art. 25-duodecies);
  - racism and xenophobia (Art. 25-terdecies);
  - fraud in sports competitions, unlawful gambling or betting, and gambling using prohibited devices (Art. 25-quaterdecies);
  - tax crimes (Art. 25-quinquiesdecies);
  - smuggling offenses (Art. 25-sexiesdecies);
  - crimes against cultural heritage (Art. 25-septiesdecies);
  - laundering of cultural assets and devastation and looting of cultural and landscape assets (Art. 25-duodevicies);
  - crimes against animals (Art. 25-undevicies);
  - crimes referred to in Art. 12 of Law No. 9/2013, which constitute a prerequisite for entities operating in the virgin olive oil supply chain;
  - transnational crimes under Law No. 146/2006, which constitute a prerequisite for the administrative liability of entities when committed in a transnational manner;
  - crimes under Legislative Decree No. 129/2024 relating to unlawful management, market manipulation, insider trading, and money laundering through crypto-assets, which constitute a prerequisite for the administrative liability of entities when committed in the course of business activities.
- Breaches falling within the scope of the Union acts that concern the following areas: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii)

product safety and compliance; (iv) transport safety; (v) protection of the environment; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and welfare; (viii) public health; (ix) consumer protection; (x) protection of privacy and personal data, and security of network and information systems; L 305/34 EN Official Journal of the European Union 26.11.2019.

- Breaches affecting the financial interests of the Union as referred to in Article 325 TFEU and as further specified in relevant Union measures:
  - The Union and the Member States shall counter fraud and any other illegal activities affecting the financial interests of the Union through measures to be taken in accordance with this Article, which shall act as a deterrent and be such as to afford effective protection in the Member States, and in all the Union's institutions, bodies, offices and agencies.
  - Member States shall take the same measures to counter fraud affecting the financial interests of the Union as they take to counter fraud affecting their own financial interests.
  - Without prejudice to other provisions of the Treaties, the Member States shall coordinate their action aimed at protecting the financial interests of the Union against fraud. To this end they shall organise, together with the Commission, close and regular cooperation between the competent authorities. C 202/188 Official Journal of the European Union 7.6.2016 EN.
  - The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, after consulting the Court of Auditors, shall adopt the necessary measures in the fields of the prevention of and fight against fraud affecting the financial interests of the Union with a view to affording effective and equivalent protection in the Member States and in all the Union's institutions, bodies, offices and agencies.
  - The Commission, in cooperation with Member States, shall each year submit to the European Parliament and to the Council a report on the measures taken for the implementation of this Article.
- Breaches relating to the internal market, as referred to in Article 26 (par. 2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law:
  - The Union shall adopt measures with the aim of establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaties.
  - The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties.
  - The Council, on a proposal from the Commission, shall determine the guidelines and conditions necessary to ensure balanced progress in all the sectors concerned.
- Acts or omissions that: (i) are unlawful and relate to the Union acts and areas; or (ii) defeat the object or the purpose of the rules in the Union acts and areas falling within the material scope as below:
  - breaches falling within the scope of the Union acts in the areas of: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) protection of the environment; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and welfare; (viii) public health; (ix) consumer protection; (x) protection of privacy and personal data, and security of network and information systems;
  - breaches affecting the financial interests of the Union as referred to in Article 325 TFEU;
  - acts or omissions relating to the internal market, as referred to in Article 26 (par. 2) TFEU.