-

WHISTLEBLOWING

applied by

VISOTTICA
GROUP

Visottica Industrie S.p.A.
Ookii S.r.l.
Matrix S.r.l.
Eurodecori S.r.l.
Ideal S.r.l.

Visottica Industrie S.p.A.
Via Vecchia Trevigiana, 11 – 31058 Susegana (TV), Italy
VAT Reg. No. 03486160264 - LEI: 815600A7F976E768590

VISOTTICA
GROUP

Table of contents

1. INTRODUCTION

1.1. Why this Policy?

The Italian Legislative Decree No. 24 of March 10, 2023 (hereinafter the "Decree"; see attachments for full document), implementing the Directive (EU) 2019/1937 and concerning "*the protection of persons who report breaches of Union law, and containing provisions with regard to the protection of persons who report breaches of national law*", introduced a new framework for whistleblowing in Italy by collecting, within a single norm of reference, all of the rules and provisions concerning reporting channels and the protection of the reporting persons both in the public and private sectors.

Whistleblowing is originally an Anglo-Saxon instrument through which the employees of a public or private organization can contact specific individuals or bodies and report a possible violation, crime, wrongful action or irregular conduct committed by other individuals belonging to the same organization.

The purpose of whistleblowing is to enable organizations to address the reported issue as soon as possible, disclosing situations of risk or harm, and contributing to prevent and combat wrongdoings.

This procedure (hereinafter the "***Policy***") aims to protect those who report breaches or unlawful actions of which they have become aware in the context of their work; it also aims to spread a culture of ethics and legality in the workplace, as well as to create a climate characterized by transparency and a sense of participation and belonging, associated to the overcoming of the fear of retaliation by corporate bodies or colleagues or the risk of seeing one's report unheeded.

This Policy plays a major role in discovering and preventing a variety of breaches and violations; it also makes it possible to take appropriate steps against the persons being reported on, ensuring the highest degree of protection and safeguard of employees who, in good faith, report breaches of applicable laws and regulations, violations of the ethical and moral principles embraced by the Group, or non-compliance with specific internal procedures.

By adopting this Policy, the Visottica Group pursues the following objectives:

- ✓ To encourage employees, as well as third parties whom the Group works with, to report internally and as promptly as possible any breaches of laws and regulations, any violations of the ethical and moral principles embraced by the Group, and any instances of non-compliance with specific internal procedures, as defined in greater detail in section 2.3, while being aware that their reports will only be followed up if internal investigations prove they are grounded;
- ✓ To provide employees and other concerned parties with information about how to submit a report and how such report will be handled;

- ✓ To create a safe environment in which employees and other concerned parties may in good faith report misconduct in a confidential way and without fear of retaliation, even in the event their suspicions should later prove to be unfounded.

In order to ensure the effectiveness of this Policy, the Group has implemented dedicated reporting channels, as defined in greater detail below.

This Policy does not supplement the employment agreements of the Group's employees and may be amended at any time subject to the procedures for informing and consulting with employee representatives, where applicable. Implementation of this Policy shall be subject to information or consultation with employee representatives where required by law.

1.2 Terms and Definitions

Reporting person	The person (whistleblower) who has submitted a report through the dedicated reporting channels in compliance with this Policy (and, where required by law, the natural persons and/or – subject to applicable local laws – the legal persons who assisted the reporting person in the reporting process pursuant to Article 5 of Directive (EU) 2019/1937, hereinafter the "***Facilitators***").
Other concerned persons	Any persons involved in the reporting who, pursuant to applicable law, have information on the alleged breaches and violations, which they have acquired during work-related activities.
Reporting channels	All reporting instruments available at the time of the reporting: - The reporting platform (website) accessible at www.visotticagroup.com, under the "Whistleblowing" section (which also offers the possibility of submitting an anonymous report and/or leaving a vocal message); - In-person reporting subject to compliance with the requirements set out in section 3.1 of this Policy.
Directive	Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law.
Personal data	Information related to an individual that allows them to be identified, either directly or indirectly.
Investigation	The process to verify the reported facts and events; the research, analysis and conclusion documented in a report.

Visottica Group or the Group	The Italian legal entities with more than 50 workers owned and/or controlled by Visottica Industrie S.p.A., a company with its registered office in Susegana (TV), Italy, via Vecchia Trevigiana, 11, VAT Reg. No. 03486160264.
Visottica Industrie S.p.a.	Visottica Industrie S.p.A., a company with its registered office in Susegana (TV), Italy, via Vecchia Trevigiana, 11, VAT Reg. No. 03486160264.
Ookii S.r.l.	Ookii S.r.l., a company belonging to the Visottica Group with its registered office in Seren del Grappa (BL), Italy, Via Industrie, 3, VAT Reg. No. 00829730258.
Matrix S.r.l.	Matrix S.r.l., a company belonging to the Visottica Group with its registered office in Seren del Grappa (BL), Italy, Via Industrie, 13, VAT Reg. No. 0082643025.
Eurodecori S.r.l.	Eurodecori S.r.l., a company belonging to the Visottica Group with its registered office in Quero Vas (BL), Italy, Zona Artigianale, 11, VAT Reg. No. 00963640255.
Ideal S.r.l.	Ideal S.r.l., a company belonging to the Visottica Group with its registered office in Quero Vas (BL), Italy, via A. Redusio, 6/8/10, VAT Reg. No. 00843530254.
Whistleblowing Committee or Committee	A body specifically established by the Visottica Group and entrusted with the following tasks: i) to provide support in the analysis and evaluation of reports; ii) to make the final decision with regard to reports. The Committee is subject to strict confidentiality requirements and must be independent and impartial. If deemed necessary, the Committee may avail itself of an Inspector (either internal or external) to conduct targeted investigations. One Committee is established for the entire Group.
Confidential Information	Within the scope of the applicable law, all confidential information, including all personal data that can be recovered through the report and, specifically, information about the identity of the Reporting person, the identity of the persons concerned by the report, and all information related to a report and disclosed or collected during the investigation of the report, regardless of its format (written, oral, digital, or any other format).

Inspector	"Internal inspector" means an employee of the Group who has been specifically appointed, trained, and authorized to conduct investigations following a report. The Inspector is subject to strict confidentiality requirements and must be independent and impartial. "External inspector" means a third party who has been specifically appointed by the Group and is trained and authorized to conduct investigations following a report. External investigators are subject to strict confidentiality requirements and must be independent and impartial.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data.
DPIA	Data Protection Impact Assessment, which is a special procedure set out in Article 35 and Recitals 90 and 93 of the GDPR, aimed at identifying, evaluating, and managing risks connected to specific types of data processing.
Employee	A person who has entered an employment agreement with one of the companies belonging to the Visottica Group, even if the agreement has not become effective yet.
Breach	See the definition set out in section 2.3 below.
Policy	This document and all the obligations and rights contained herein.
Report	The reporting of breaches of laws, regulations, or internal policies (as defined in section 2.3) by Visottica employees, other concerned parties connected to Visottica or, if applicable, third parties, through the available reporting channels.
Attachment	Any document mentioned in this Policy.
Anonymous report	Any report which does not include details that make it possible, or may make it possible, to directly or indirectly identify the Reporting person.
Work-related context	The current or past work-related activities at or for the Group, through which the Reporting person, regardless of the nature of their employment, has acquired information on alleged breaches that fall within the scope of this Policy.

2. SCOPE OF THIS POLICY

2.1 Whom does this Policy apply to?

This Policy applies to and is binding for the entire Visottica Group.

The Board of Directors, directors, managers, and heads of corporate functions shall ensure that this Policy is implemented. All the Group's employees and other parties concerned undertake to comply with this Policy.

The scope of this Policy does not include the Group's customers, whose reports should be directly submitted to the sales office.

2.2 Who can submit a report?

Our reporting channels are made available to any person who has a contractual relationship with the Group, specifically:

(i) The Group's employees, officers, managers, and internal stakeholders;

(ii) Self-employed persons, freelancers, consultants, and collaborators who work for the Group;

(iii) Volunteers and trainees (either remunerated or unremunerated);

(iv) All members of Visottica executive, management, and supervisory bodies;

(v) Any third party who acts on behalf of or interacts with the Group (including, but not limited to, suppliers and contractors), except for customers;

(vi) All shareholders and persons performing functions in the areas of administration, management, control, supervision, or representation, including when such functions are performed on a purely *de facto* basis.

Reports may also be submitted by:

(i) Persons who are in the recruitment or pre-contractual stage (with reference to information acquired during the recruitment process or other pre-contractual negotiations);

(ii) Employees or collaborators during the trial period;

(iii) Employees and collaborators after the termination of their employment (only if the information being reported has been acquired during employment).

In compliance with the applicable laws, all reports must be made without any direct compensation.

2.3 What are the breaches that should be reported?

The Visottica Group's reporting system is a confidential, protected channel made available to make it possible to report (in an anonymous form or otherwise), in good faith and to the best of one's direct

knowledge, substantiated facts and events based on reasonable suspicions and accurate and consistent information acquired in the work-related context. The Reporting persons may report breaches, or attempted breaches, that occurred (or are suspected to have occurred) with regard to the provisions of Article 2, paragraph 1 of the Decree, and specifically to the following ("Breaches"):

(a) Offenses, crimes and misdemeanours including but not limited to those related to the following areas:
- Corruption or influence peddling;
- Money laundering and finance, tax, and accounting-related offenses;
- Conflicts of interest;
- Protection of privacy and protection of personal data;
- Anti-competitive practices;
- Economic sanctions, trade embargoes, and export controls;
- Safety and compliance of products;
- Public health;
- Security of networks and information systems;
- Environment protection;
- Consumer protection;
- Tax evasion by enterprises;
- Fraud.

(b) Threats or harm to the public interest;

(c) Unlawful conduct that is relevant pursuant to the Italian Legislative Decree No. 231/2001, or severe violations of Visottica's 231 Organizational Model and Code of Ethics which are not covered by the Directive or the applicable local laws;

(d) Breaches of applicable laws concerning sexual or psychological harassment (e.g., related to gender, race, disability, or religion), as well as discrimination and violence in the workplace;

(e) Non-respect of human rights;

(f) Violation of the non-retaliation principle;

(g) Violation of any of the Group's policies, guidelines, and procedures;

(h) Breaches of applicable laws and regulations;

(i) Behaviour that might be detrimental to the Group's assets or reputation.

The Reporting persons may submit reports either on breaches that have already occurred or, where reasonable suspicion exists, breaches that are highly likely to occur.

2.4 What is not covered by this Policy?

In compliance with the Directive, the following information is completely excluded from the scope of this Policy and may not be reported or investigated:

- Breaches that do not harm the public interest;
- Any information protected by obligations of professional secrecy or medical privacy;
- Any information covered by the secrecy of judicial rulings or the secrecy of inquiries and investigations.

This Policy may not be used to report facts or events concerning one's personal situation or related to one's subjective work-related experience (e.g., to challenge the evaluation of one's work by a superior), with the exception of instances of discrimination or harassment.

The reporting system can only and exclusively be used for reports that fall within the scope of this Policy.

3. REPORTING A VIOLATION

3.1 Reporting method

The use of the Visottica Group's reporting system is voluntary and complementary to the other channels established within the Group's companies.

The Human Resources department and the heads of corporate functions remain available to receive and handle any reports; however, if for any reason the Reporting person deems it preferable not to contact them, they can use the reporting channels currently available, as outlined below.

3.1.1 Online reporting platform

The Reporting person is encouraged to submit their report through the Visottica Group's platform.

The platform is managed by a certified external provider that ensures information confidentiality and does not alter the content in any way. As such, the provider guarantees impartiality in the reception and processing of reports.

The reporting platform is available 24 hours a day, 7 days a week (except during maintenance) to those who wish to submit a report.

The platform includes two reporting channels:

- Reporting by manually filling in the fields on the online platform; or
- The recording of a vocal message (the voice will be made unrecognizable) on the online platform.

3.1.2 In-person reporting

The Reporting person may choose to make their report in person, during a video conference or an in-person meeting attended by at least one member of the Committee.

The meeting can be arranged by calling the Committee's dedicated phone number +39 348-8585307, from Monday to Friday, from 10:00 a.m. to 12:00 p.m. (noon).

In case of vocal messages and/or in-person reporting, subject to the Reporting person's consent, the report may be documented by the personnel in charge who will either record it on a device suitable for storage and playback or see to a verbatim transcription of it (as provided for in Article 14, paragraphs 2 and 4 of Italian Legislative Decree No. 24/2003).

3.2 Content of reports

Reports must describe facts and events in an objective way, be relevant to the Policy's scope, and be limited to representing only the elements strictly necessary to verify the reported facts or events.

A report shall contain at least the following elements:

- The Reporting person's personal details, including their job title or function performed in the company, unless the Reporting person intends to make an Anonymous report by selecting the "*Segnalazione Anonima*" (Anonymous Report) option available on the platform;
- A clear, exhaustive description of the facts or events being reported;
- If known, the time and place in which the facts or events being reported have been committed or have taken placed;
- The indication of other persons, if any, who could provide information on the facts or events being reported;
- The indication of documents, if any, which could confirm that the facts or events being reported are grounded;
- Any other piece of information that could provide useful insight regarding the substantiation of the facts or events being reported.

The reporting platform makes it possible to upload documents together with the report.

It is recommended that the Reporting person be as specific as possible to enable a better understanding and faster handling of the problem by the Committee.

The Reporting person may choose to submit an Anonymous report. However, the following should be noted:

- An Anonymous report might be more likely to be rejected if it does not include sufficient information to conduct a meaningful investigation.

- Communicating the Reporting person's identity will facilitate the investigation and the search for further information concerning the reporting; moreover, it will enable the organization to protect the Reporting person more effectively.

An Anonymous report might make it more difficult for the Reporting person to obtain legal protection.

If the Reporting person chooses to use the dedicated phone number (see section 3.1), the member of the Committee taking the call will take note of the report and handle it as outlined in greater detail in section 3.3.

The reporting channels must be used in good faith.

3.3 Submitting a report

3.3.1. Submitting a report through the online platform

When accessing the online platform, the Reporting person will have to select the Group's company that the report refers to, fill in the mandatory fields, and then provide the information to be reported. Even when choosing to remain anonymous, the Reporting person will be given an access code to check the status of the report. The access code must be stored securely. If lost, the code cannot be retrieved in any way, and it will be no longer possible to contact the Reporting person if the report has been submitted anonymously.

If the Reporting person chooses to remain anonymous, it is recommended that they do not use a device provided by the Group and/or connected to the company network/intranet, that they access the system directly by copying and pasting or typing the URL address in an Internet browser instead of clicking on the corresponding link, and that they do not include any information that might make it possible to directly or indirectly identify them.

Upon submitting the report through the platform, the Reporting person will receive an acknowledgement of receipt together with the assigned code (key code). From this moment on, the Reporting person will have the right to be informed of the actions taken concerning the report and the decisions made with regard to it.

3.3.2. Submitting a report in person

When calling the Committee's phone number, the Reporting person should start the phone call by saying: "I have to make a report" and then ask to arrange a video conference or in-person meeting attended by at least one member of the Committee.

It is the responsibility of the Committee to arrange the video conference or in-person meeting no later than twenty (20) working days after the Reporting person has made their request.

Subsequently, the Committee will open a new reporting case.

The Committee must ensure the protection of the Reporting person and facilitators, if any, as outlined in section 4 below.

In the event the report is submitted to an entity other than the Committee, such entity is required to transmit the report to the Committee within 7 days after receipt, while at the same time notifying the Reporting person that such a transmission has been made.

3.3.3. Managing the report

The Reporting person will receive acknowledgement of receipt within 7 days after the date of report submission.

When a report is submitted through the platform, the Committee receives an e-mail notification addressed to comitatowb@visotticacomotec.com. For security reasons, this notification will not include any information on the case file (information is limited to the file number and, if relevant, the category of the breach reported), nor any information revealing the identity of the Reporting person.

The Committee will need to access the platform to view the content of the report.

The preliminary review of the report by the Committee can have the three following outcomes:

1 Request for further information	If the details included are not sufficient to determine the admissibility of the report (e.g., if the facts or events being reported, even though featuring a certain degree of severity, are described in an inaccurate or unsubstantiated way, or if their description suggests the Reporting person does not have direct knowledge of what has been reported), the Committee will send a message to the person who made the report (provided that their identity has been disclosed) asking to be contacted again. In this message, the Committee will ask the Reporting person to provide additional information. If the Reporting person fails to reply within 7 days, the case file will be closed.
2 Inadmissible report	Any report that does not fall within the scope of this Policy (e.g., the reporting of facts or events that do not constitute a breach or violation; allegations that cannot be verified or are vague or unsubstantiated) will be deemed inadmissible and will be destroyed or archived according to the retention period set out by law.

3 Management of the report on the part of the Committee	A report is deemed admissible if i) the situation described therein corresponds to facts and events that fall within the scope of this Policy; ii) the description appears to be sufficiently accurate; iii) a preliminary review of the report shows that the Reporting person is acting in good faith. If these three conditions are all met, the Committee will proceed to handle the report and, if able to do so, will also see to its resolution.
4 Appointment of an inspector	If unable to resolve the situation, the Committee may submit the case file to an internal and/or external Inspector; the Inspector will be selected based on the importance of the case, the people involved in the reporting, the severity of the reported facts or events, the type of reporting, and the place in which the reported facts or events occurred.

The Committee may decide to close the case file at any stage of its processing. Regardless of when such a decision is made, the Reporting person who has disclosed their identity will be informed that the reporting case has been closed and be given the general reasons for the decision.

3.4 Follow-up to the report

The Committee and the Internal inspector, if appointed, shall perform their tasks in such a way to ensure confidentiality and impartiality at all stages of the investigation, as well as when drafting the investigation report. If any member of the Committee has a conflict of interest with respect to the report, they shall immediately notify the other members of the Committee. The members of the Committee who have a conflict of interest will be exonerated from the investigation.

The Committee reserves the right to appoint an External inspector at its own discretion (except for matters related to Human Resources).

If appointed, the Inspector will contact the Reporting person to communicate their contact information, as well as how they can be contacted; the Inspector will also provide information on the follow-up actions that have been planned.

The follow-up to the report by the Committee or the Internal or External inspector, if appointed, might include, without limitation:

a) Starting an internal investigation and adopting the necessary measures to resolve the reported issue;
b) Referring the case to the competent authority for further investigation;
c) Closing the proceeding due to insufficient evidence or for other reasons.

As part of the Committee's supervision and planning responsibilities, the Inspector is responsible for the following actions:

- Performing checks and investigations on the report;
- Interviewing people, including the Reporting person, as necessary. Upon request of the person being questioned, the interview may be conducted in the presence of a witness;
- Collecting documents and evidence, if deemed appropriate, by interviewing individuals and from open-source data banks;
- Ensuring communication with the Reporting person;
- Preparing an investigation report which should include a detailed description of the facts or events, the checks performed, the reasons underlying the breach or violation (if possible); the report should also include the Inspector's conclusions and the recommended actions aimed at a resolution;
- Protecting the rights of the persons concerned by the report or involved in the subsequent investigation;
- Drafting an action plan and suggesting recommendations;
- Proposing disciplinary sanctions, where appropriate, and/or recommending legal actions;
- Closing any ungrounded case files.

In all cases, the Inspector shall adopt all reasonable measures to guarantee that the investigation can be completed quickly.

Subject to the provisions of applicable laws and regulations, the Internal and/or External inspector will provide feedback to the Reporting person within 3 (three) months of the report's receipt, except for the following cases:

- Communication is prohibited by the applicable law; or
- The Reporting person has not disclosed their identity; or
- The complexity of the investigation prevented it from being completed within three months; under such circumstances, the Reporting person shall be notified of the need for an extension to complete and close the investigation.

The investigation of reports is not disciplinary in nature. Unless otherwise provided for by law, the "interviews" or conversations held with the Reporting person, the persons mentioned in the reports, and any witnesses, shall be solely aimed at verifying the facts or events as part of an internal investigation.

3.5 Results of the investigation

The Committee (or the Inspector, if appointed) shall communicate the outcome of the report to the Reporting person. The Reporting person may ask to be kept informed of the progress and outcome of the investigation.

The Reporting person may also provide further information during the investigation.

The investigation will end with a report written by either the Committee or the Inspector (if appointed). Subsequently, the investigation report will be transmitted to the Board of Directors and the Human Resources department, and /or to the office in charge of implementing any recommended measures.

Should the Human Resources corporate function or the Board of Directors decide not to follow through with the measures recommended by the Committee or Inspector, they are required to document in writing the reasons why they did not implement them and forward such documentation to the Committee.

3.6 Other means of reporting

The purpose of this Policy is to implement an effective, reliable, and trusted internal system for the reporting, investigation and sanctioning of wrongful conduct in the workplace, while ensuring that the reports received are followed up in the most rigorous and timely manner.

If:

- a report has not been followed up in any way within 3 months after submission;
- a report has not been taken on within 7 days, as stipulated;
- a person believes that they have suffered retaliation;
- a person has a well-founded reason to believe that the breach or violation may pose immediate or evident danger to the public interest;

the report may be forwarded to the National Anti-Corruption Agency (ANAC) through the digital platform available at https://www.anticorruzione.it/-/whistleblowing, following the instructions included therein.

Said platform guarantees all of the rights of the Reporting person as specified below in section 4 of this Policy.

4 PROTECTION OF REPORTING PERSONS AND FACILITATORS

4.1 Confidentiality of reports

The identity of the Reporting person and of the person(s) concerned by the report, as well as all information collected, are deemed to be confidential and shall not be disclosed. Information and data submitted through the system are automatically encrypted and shall be always treated as strictly confidential.

Such confidentiality obligation also applies to the Reporting person (who is required to maintain strict confidentiality about the report and all people involved) in order to ensure that the investigation is conducted with peace of mind, and all people involved (the Reporting person, any witnesses, facilitators, as well as the persons being reported on) are protected.

During the investigation, information regarding the report – including the Reporting person's identity – may only be shared for the purpose of implementing this Policy, and only with the following persons:

- the members of the Committee;
- the Inspector.

These persons have an obligation to protect the identity of the Reporting person. They may not disclose to anyone the Reporting person's identity or any information that might lead to the identification of the Reporting person. Furthermore, they shall adopt all reasonable measures to reduce the risk of identifying the Reporting person.

Exceptionally, and only if the Reporting person grants their consent in writing, or if an obligation exists to supply the information to local law enforcement authorities, the Reporting person's identity may be shared for the sole purpose of facilitating the investigation. The Reporting person has the right to determine whom their identity may or may not be disclosed to. Even when the Reporting person has granted their consent, extreme caution should be applied to prevent the Reporting person's identity from being disclosed to the persons being reported on, thus avoiding the risk of retaliation.

Information about the report, including the Reporting person's identity, may be disclosed to judicial and/or administrative authorities and law enforcement agencies.

Non-confidential information (e.g., the report's reference number, its progress status, etc.) may be disclosed, for instance, in internal reports concerning the implementation and circulation of this policy (e.g., in the annual report addressed to the company's board). However, when a report is being processed, such disclosure may only occur after confirming that it does not risk jeopardizing the investigation.

The violation of the confidentiality obligation is subject to the application of the Disciplinary System (pursuant to Italian Legislative Decree No. 231/2001) currently in force at Visottica Industrie S.p.a. and the Group's companies which have an Organizational Model pursuant to Italian Legislative Decree No. 231/2001, as well as of any applicable civil or criminal sanctions. In the Group's companies which do not have an Organizational Model pursuant to Italian Legislative Decree No. 231/2001, the sanctions provided for by the relevant national collective labour agreement (CCNL), as well any applicable civil or criminal sanctions, shall apply.

4.2 Prohibition against retaliation

For reports within the scope of this Policy, the Visottica Group is strongly committed to protecting the Reporting person who acts in good faith from intimidation, harassment, reputational damage, unfavourable treatment, discrimination, and retaliation (in any form, including, but not limited to dismissal, unjustified disciplinary actions, demotion, transfer, isolation), without prejudice to the Group's right to initiate disciplinary proceedings against any Reporting person found to have knowingly and with intent or gross negligence submitted a false and/or defamatory and/or misleading report.

If the Reporting person believes that they have suffered retaliation or discrimination following the submission of a report, they shall immediately notify the Committee or submit a specific report.

This provision applies to the following persons:

a) The Reporting person;
b) An anonymous Reporting person whose identity has been subsequently disclosed;
c) The facilitator;
d) Third parties connected to the Reporting person, such as their colleagues or family members;
e) Any legal entities owned by the Reporting person, or which the Reporting person works for, or which the Reporting person is connected to in a work-related context.

4.3 Sanctions

The employees and other concerned parties who, for reasons directly or indirectly connected to the report, or to hinder or attempt to hinder the report, engage in retaliation and/or discrimination against the Reporting person and other persons identified in section 4.2 of this Policy, may be subject to the disciplinary sanctions defined in their employment agreement or in the 231 Organizational Model, where applicable (as well as to the termination of the contractual relationship).

In addition, the person committing retaliation and/or discrimination may be subject to civil or criminal sanctions in accordance with the applicable law.

4.4 Anonymous reports

The Reporting person may choose to submit an Anonymous report. However, the following should be kept in mind:

- An Anonymous report might be more likely to be rejected if it does not include sufficient information to conduct a meaningful investigation.
- Communicating the Reporting person's identity will facilitate the investigation and the search for further information concerning the reported content; moreover, it will enable the organization to protect the Reporting person more effectively.

An Anonymous report might make it more difficult for the Reporting person to obtain legal protection.

5 PERSONAL DATA PROTECTION

5.1 Personal data that may be collected

The following personal data may be collected through the reported channel used by the Reporting person and during subsequent investigation/fact-checking:

- The Reporting person's identity, job title and contact information;
- The identity, job title and contact information of the persons being reported on and of witnesses;
- The identity, job title and contact information of the persons involved in the reporting;
- The data under Articles 9 and 10 of the GDPR with reference to the Reporting person and/or the persons being reported on and/or the witnesses and/or the persons involved in the reporting.

Moreover, the following information may be collected:

- A description of the events;
- The elements gathered as part of the fact-checking connected to the reported facts or events;
- The report documenting the fact-checking;
- The measures adopted in connection with the reporting.

5.2 Rights of the reporting person

In compliance with all applicable privacy and data protection laws, the information provided under this Policy must be factual and directly related to the subject of the report.

Pursuant to the provisions of Article 13 of the GDPR, prior to entering the reported information, the Reporting person shall receive – through the online reporting platform or any other means – all required information concerning the processing of the personal data provided.

The Committee and the Inspector (if appointed) shall in no case disclose the identity of the Reporting person or any information that could lead to the Reporting person's identification by the persons being reported on, unless the Reporting person has granted their consent, except when the request comes from the judicial authority.

This is without prejudice to the right of limitation under Article 18 of the GDPR.

5.3 Rights of the person being reported on

Pursuant to Article 14 of the GDPR, following a reporting, the persons involved (e.g., witnesses, victims, or alleged perpetrators) will have the right to be informed of the report within a reasonable period of time.

However, pursuant to Article 14, paragraph 5, letter b) of the GDPR, disclosure of such information may be avoided if it "*is likely to render impossible or seriously impair the achievement of the purposes of such processing*." This may occur if disclosure of information to the data subject risks hindering the investigation (e.g., if the risk exists that evidence could be destroyed).

In such cases, information may be provided only if the risk has been eliminated but, in any case, it must not contain any clue to the identity of the Reporting person, or third parties involved.

5.4 Data retention

The data collected through the reporting channels and the related documentation may be retained for a period strictly limited to what is necessary for the processing of the data and, in all cases, for up to **five years** from the date on which the final outcome of the reporting procedure has been communicated, subject to confidentiality requirements.

5.5 Data security

Data security is ensured with reference to the personal data transmitted and processed in connection with all reports, either submitted through the platform or made in person, to prevent any unauthorized alteration, modification, or disclosure of such data.

The security and confidentiality of personal data are ensured at the time such data are collected, as well as during their transmission and storage, by adopting appropriate security measures covered by the DPIA.

Access to personal data shall be permitted only to the persons authorized to process them, subject to strict confidentiality requirements and limited to what is necessary for the purposes of the investigation.

During the retention period, the personal data stored on the reporting platform shall be archived and kept separate from the other elements on the reporting platform.

6 GOVERNANCE

6.1 Who is responsible for this Policy?

The Parent Company's Committee is responsible for this Policy and for evaluating the effectiveness of the measures adopted in response to this Policy.

The Committee has operational responsibility for this Policy and must ensure that all managers and other employees who may be assigned to deal with matters or investigations under this Policy receive appropriate, periodical training.

The Committee regularly reviews this Policy from a legal and operational perspective, ensuring compliance with the procedures for informing or consulting employee representatives.

6.2 Annual report

The Committee will draft a report on an annual basis regarding the implementation of this Policy and the key indicators (number of reports by category, number of Anonymous reports, number of reports made in person, number of justified reports, possible reasons underlying the change in the number of cases, etc.).

This report is addressed to the Board of Directors, as well as to Visottica management and the different governing bodies (Supervisory Body, Board of Statutory Auditors).

The identity of the Reporting persons and of the persons being reported on shall never be disclosed, and only aggregated/statistical data may be published in the annual report.

7 MISCELLANEOUS PROVISIONS

7.1 Previous policies

Effective 17 December 2023, this Policy supersedes the protocol for handling reports and complaints concerning violations of principles and rules defined and/or recognized by the Group in its Code of Ethics.

7.2 Language

This Policy was originally drafted in Italian. Any translation of this Policy into another language shall in no way affect its interpretation. In case of contradiction or discrepancy with any translation in other languages, the Italian text will prevail.

7.3 Publicity

The Group undertakes to share, display, and make easily accessible in the workplace and on the company website the relevant information about the platform and this Policy.

7.4 Disputes

Any dispute or controversy arising out of, relating to, or in connection with the interpretation or application of this Policy shall be governed by the law of the Italian Republic, and shall be under the exclusive jurisdiction of the Court of Treviso.

7.5 Contacts

For inquiries concerning this Policy, please send an e-mail to the Committee by addressing it to comitatowb@visotticacomotec.com.

8 ATTACHMENTS

The following documents are attachments to this Policy:

- Italian
- Legislative Degree No. 24/2023;
- EU Directive No. 2019/1937.