

Viabizzuno

POLICY
WHISTLEBLOWING

<i>N° Rev.</i>	<i>Date rev.</i>	<i>Note</i>
00	20/12/2023	First issue

Sommaro

INTRODUCTION

Viabizzuno S.p.A. (hereinafter also referred to as the "Company" or "Viabizzuno") aims to promote a corporate culture characterized by virtuous behavior and a Corporate Governance system that prevents the commission of unlawful acts, while ensuring a working environment where employees can confidently report any illicit behaviors and promote a virtuous path of transparency and adherence to appropriate ethical standards.

With the goal of endorsing and reinforcing these standards, the Company, recognizing the importance of having a specific procedure governing the Reporting of Unlawful Behaviors by employees and third parties, has decided to adopt this Whistleblowing Policy (hereinafter also the "Policy") – which also constitutes an integral part of its Organizational, Management, and Control Model pursuant to Legislative Decree 231/2001¹ (hereinafter also "Model 231" or "Organizational Model") – for reporting any conduct, including omissions, that constitutes or may constitute a violation or inducement to a violation of (i) national or European Union regulatory provisions, (ii) values and principles set forth in the Company's Code of Ethics, (iii) unlawful conduct relevant under Legislative Decree 231/2001 or a violation of the Organizational Model; and (iv) Internal Procedures adopted by the Company.

For this purpose, the Company has defined specific communication channels for the management of Reports in order to comply with Legislative Decree 24/2023. This legislation has incorporated into our legal system the content of EU Directive 2019/1937, harmonizing the regulation concerning whistleblowing within the European Union and prescribing minimum standards of protection that each Member State is required to adopt.

Therefore, the Recipients of this Policy are invited to promptly report such conduct through the methods described below, refraining from undertaking independent analysis and/or investigation initiatives.

1. DEFINITIONS AND ABBREVIATIONS

Case Manager / Manager: The collegial body, with a non-fixed composition, responsible for receiving and managing internal Reports for the purposes of this Policy, appointed in accordance with Article 4, paragraph 2, of Legislative Decree 24/2023. If the subject of the Report concerns unlawful conduct relevant under Legislative Decree 231/2001 or Violations of the Organizational Model 231, a representative of the Supervisory Body is involved in the Case Manager.

Code of Ethics: A document that outlines the values and principles governing the activities and relationships towards all parties with whom the Company engages to achieve its corporate objectives.

Disciplinary System: Set of punitive measures established against those who violate the provisions of this Policy.

EU Regulation No. 679/2016 (GDPR): Legislation concerning the protection of natural persons regarding the processing of personal data and the free movement of such data.

External Report: Written or oral communication of Information on Violations submitted through the External Reporting Channel as outlined in Section 6.2 of the Policy.

Facilitator: Denotes an individual, a natural person, operating within the same Work Environment as the Whistleblower, who has provided or provides assistance to the latter in the Reporting process. The assistance of the facilitator must be kept confidential.

Information Notice: Refers to the privacy notice provided pursuant to Article 13 of the GDPR to the individuals concerned, namely, the Reported Party and the Whistleblower.

Information on Violations: Refers to written/oral information, including well-founded suspicions, concerning committed or potential Violations, as well as circumstantial evidence of conduct aimed at concealing them².

Internal Procedures: Refers to the set of procedures, policies, operational instructions, and all other documents that are part of the company's regulatory system.

Internal Report: Written or oral communication of Information on Violations submitted through the Internal Reporting Channels as outlined in Section 6.1 of the Policy.

Model 231 or Organizational Model: Denotes the comprehensive set of principles, rules, provisions, methods, and operational procedures aimed at preventing the offenses specified in Legislative Decree 231/2001.

National Anti-Corruption Authority (ANAC): According to Legislative Decree 24/2023, it is the authority responsible for managing external Reporting Channels.

National Collective Labor Agreement (CCNL): The national collective labor agreement applicable to the Company.

Public Disclosure: Refers to the activity through which information about violations is made publicly available, either through the press, electronic means, or any other dissemination methods capable of reaching a large number of people.

Recipients: Refers to individuals within Viabizzuno, as well as third-party individuals or entities, such as suppliers, freelancers, consultants, clients, collaborators, or business partners, among others.

Report(s): Communication(s) from the Whistleblower containing information related to Unlawful Conduct.

Reported Party/Person: Individual to whom the Whistleblower attributes the Unlawful Conduct subject to the Report.

Reporting Channels: Communication channels identified by Viabizzuno, whether internal or external to the Company, for conveying Reports.

Reporting Platform (so-called Tool): An information system that ensures, also through the use of encryption tools, the confidentiality of the identity of the Whistleblower, the Reported Party, any person mentioned in the Report, as well as the content of the Report and its related documentation.

Retaliation: Acts of retaliation or discrimination, whether direct or indirect, carried out by the Company against the Whistleblower for reasons connected, directly or indirectly, to the Report.

Supervisory Body (SB): Supervisory Body pursuant to Legislative Decree 231/2001 for the Company.

Unlawful Conduct: Any action or omission that constitutes or could constitute a violation or inducement to a violation regarding the behaviors outlined in Section 4 of the Policy.

Violation: Encompasses all behaviors, acts, or omissions identified in the subsequent Section 4.

Whistleblower: Individual belonging to the categories indicated in Section 4 of the Policy who makes the Report, or their Facilitator(s).

Work Environment: Refers to work-related professional activities, whether present or past, carried out within the scope of relationships with the Company. During these activities, an individual acquires information about violations and may face retaliation in the event of reporting, public disclosure, or reporting to authorities.

It is specified that terms defined in the singular also apply to the plural, where the context requires, and vice versa.

2. TERMS OF VALIDITY AND DISSEMINATION

This Policy takes effect from the date of its issuance as indicated on the cover.

Any subsequent updates supersede and replace, from the date of their issuance, all previously issued versions. This Policy is ensured the broadest possible dissemination.

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

3. PURPOSE

The purpose of the Policy is to regulate the Reporting Channels for reporting violations or irregularities and to remove factors that may hinder or discourage reports. Additionally, it aims to regulate measures to protect reporters and the disciplinary system.

4. CONTEN OF THE REPORT

This Policy describes the process and communication channels to be used for the submission, receipt, analysis, and handling of reports of unlawful behavior, including omissions, that constitute or may constitute:

- a violation, or inducement to a violation, of laws and regulations within the scope of the acts of the European Union or national laws specified in the Annex to Legislative Decree 24/2023 or, even if not included in said Annex, related to the following areas:
 - a. public procurement;
 - b. services, products, and financial markets, and prevention of money laundering and financing of terrorism;
 - c. product safety and compliance;
 - d. transportation safety;
 - e. radiation protection and nuclear safety;
 - f. food and feed safety and animal health and welfare;
 - g. consumer protection;
 - h. privacy protection and personal data protection, and network and information systems security;
 - i. public health;
 - j. environmental protection;
 - k. violation of competition rules and state aid;
 - l. violation of corporate tax rules;
 - m. financial interests of the European Union;
 - n. administrative, accounting, civil, or criminal offenses not covered by the letters above:
- a violation, or inducement to a violation, of internal regulations, such as:
 - a. values and principles set forth in the Viabizzuno Code of Ethics;
 - b. values, principles, and controls identified in the Viabizzuno Model 231;
 - c. operational procedures governed by the Company's internal policies.

The Report, sufficiently detailed and based on precise and consistent factual elements, must be made by providing the following information, along with any supporting documentation:

- a detailed description of the events and the methods by which they became known;
- date and place where the event occurred;
- names and roles of the individuals involved or elements that may allow their identification;

- names of any other individuals who can report on the reported events or elements that may allow their identification;
- reference to any documents that can confirm the validity of the reported facts.

The Whistleblower must take care not to report irrelevant or unnecessary information in relation to the Report.

The submission of Reports made solely for the purpose of retaliation or intimidation, or, in any case, unfounded and made with intent or gross negligence, is subject to penalties.

In particular, the submission of any communication that proves to be unfounded based on objective elements and that, always based on objective elements, is made solely for the purpose of causing unjust harm to the Reported Party is subject to sanctions.

The Company ensures the utmost confidentiality regarding the individuals and events reported, using appropriate criteria and communication methods to protect the identity and reputation of the persons mentioned in the Reports. This is done to ensure that the Whistleblower is not subject to any form of retaliation, avoiding, in any case, the disclosure of acquired data to third parties not involved in the Report management process, as governed by this Policy.

Whistleblowers acting in good faith will be protected against any form of retaliation, discrimination, or penalization.

In accordance with applicable regulations, the Company ensures the possibility of making reports anonymously, provided that they are adequately detailed and contain sufficient information to make them verifiable.

In the case of an anonymous report, the Case Manager reserves the right to consider it based on the severity of the reported facts and in relation to the level of detail and precision of its content.

5. RECIPIENTS OF THE POLICY

The Policy applies to the following individuals:

- Subordinate workers of the Company (employees, volunteers, paid and unpaid interns, former employees³, job applicants⁴), as well as self-employed workers;
- Shareholders and members of the Company's administrative, management, supervisory, or representative body, including non-executive members, volunteers, and unpaid interns;
- Any person working under the supervision and direction of contractors, subcontractors, and suppliers, clients, partners, consultants, and, more generally, stakeholders of the Company.

6. PROCEDURE FOR REPORTING UNLAWFUL BEHAVIOR AND RECIPIENTS OF REPORTS

In order to comply with current regulatory provisions, the following Reporting Channels have been identified through which the recipients of the Policy can provide evidence of the commission or potential commission of Unlawful Behaviors.

1. "INTERNAL" REPORTING CHANNELS ("Internal Channels")

If Whistleblower has a reasonable suspicion that Unlawful Conduct has occurred or may occur, he or she may report it to the Company through the following Internal Channels (also, the "Internal Channels"):

- using the appropriate whistleblowing IT platform (the "Platform"), which can be reached at the following link <https://viabizzunowhistleblowing.integrityline.com/frontpage> ;
- by paper mail to the address Corso di Porta Nuova, 46, 20121, Milan (MI) to the c/a of the Case Manager. It is advisable for the Internal Reporting to be placed inside two sealed envelopes: the first with the identifying data of the Reporting Party, together with a photocopy of the identification document; the second containing the

description of the facts constituting the subject of Reporting. Both should be placed inside an additional sealed envelope marked ("Reserved for the Case Manager");

- ii. by means of a direct meeting with the Case Manager - to be requested through the use of the paper mail channel referred to in the preceding paragraph - set within a period of 7 (seven) days from receipt of the Reporting. The Reports issued through face-to-face meeting, subject to the consent of the Reporting Party, may be documented by drawing up special minutes, supported, where appropriate, by recording on a computer device suitable for listening, by the Case Manager. The minutes are then submitted to the Case Manager for his or her review and signature.

All Reports are received by the Case Manager, as the person designated to receive the Internal Report as well as, except as indicated below, the only person designated to access the Internal Channels and view the contents of it, subject to written authorization from the Company, pursuant to Articles 29 and 32 par. 4 of Regulation (EU) 2016/679 and Article 2-quaterdecies of Legislative Decree 196 of 2003.

The Case Manager shall take care to prepare suitable ways to prevent the loss and destruction of Internal Reporting as well as undue access to it.

Although Anonymous Reports are allowed, Viabizzuno recommends that they be named, to allow the Managers a more efficient investigation activity, applying in any case the protections provided against possible Retaliation.

If the Internal Report concerns unlawful conduct relevant pursuant to Legislative Decree 231/2001, or Violations of the Organizational Model, the Reporting Manager forwards the Internal Report to the SB which, assuming the role of Whistleblowing Manager, coordinates with the former in order to carry out the assessments of completeness and substantiation indicated below. If the Internal Whistleblowing Report refers to one or more members of the SB, it will be forwarded to the Managing Director or to another person appropriately identified.

Anyone who receives a Report transited outside the prescribed channels must transmit it to the Managers, in original and with any attachments, within 7 (seven) days of receipt.

The transmission must be made in accordance with the criteria of maximum confidentiality and in a manner appropriate to protect the Reporting Party and the identity of the Reported Persons, without prejudice to the effectiveness of the subsequent investigation activities.

No copies of the Report received and forwarded to the Managers shall be made.

1.

1. REPORT MANAGEMENT: PRELIMINARY EXAMINATION

Reports are subject to preliminary analysis by the Case Manager.

The Manager checks for the presence of useful data and information to enable an initial assessment of the Report itself.

Within 7 (seven) days of receipt of the Report, the Manager shall send the Reporting Officer an acknowledgement of receipt of the Report, using the communication methods adopted by the Reporting Officer.

The Manager shall take all necessary measures to treat the Reports confidentially, including in order to protect the identity of the Reporting Person, the Reporting Person, and other persons mentioned in the Report.

In the course of the verifications, the Manager may avail itself of the support of the relevant corporate functions from time to time and, where deemed appropriate, of external consultants specialized in the field of the Report received and whose involvement is functional to the investigation of the Report, ensuring the confidentiality and anonymization of any personal data contained in the Report.

All those involved in the inspections must maintain strict confidentiality regarding the information received in the course of the inspections.

Upon completion of the preliminary analysis, the Manager may:

- (a) dismiss the Report as manifestly unfounded or relating to conduct or facts not relevant to this Policy;
- b) request additions/clarifications if the Report is well-founded but not sufficiently detailed. In the absence of the requested integrations, the Manager shall proceed to dismiss.
- (c) open the investigation phase.

The Manager will inform the Reporting Officer about the outcome of the investigations carried out within a reasonable period of time, in any case not exceeding 3 (three) months⁵.

2. REPORT MANAGEMENT: INVESTIGATION AND ASSESMENT

With respect to each Report, where, as a result of the preliminary analysis, useful and sufficient elements emerge or are otherwise inferable to make an assessment of the merits of the Report, the Manager will:

- acquire from the Reporting Party additional Information and/or documentation in support of the reported facts;
- proceed to the hearing of the Reported Person and other subjects possibly involved in the facts that are the subject of the Report;
- in the event that the reported conduct continues, consider suggesting to the Managing Director, or to another person appropriately identified, the adoption of suitable preliminary measures to contain any risks (e.g. suspension of the reported person);
- make use of the support of other internal Company Functions or third parties (e.g., consultants) if, due to the nature and complexity of the checks, their involvement is necessary;
- conclude the investigation at any time, if, in the course of the investigation, it is established that the Report is unfounded;
- verify the possible legal implications against the Company;
- assess whether there is an obligation to inform the competent Authorities in relation to the nature of the offence that is the subject of the Report.

In addition, Case Manager must:

- ensure that the investigation is accurate, fair, impartial, and protects the confidentiality of the identity of the Whistleblower and the persons involved, including the Whistleblower;
- ensure that appropriate measures are taken for the collection, processing and storage of personal information, ensuring that the needs of the investigation are balanced with those of privacy protection. On this point, the onus is on the Manager to consider informing the Reported Person about the investigation. The Whistleblower shall, however, always be informed by the Manager in the event that disciplinary proceedings are initiated;
- ensure that the investigative activity is carried out in compliance with the deadlines set out in §7.1.

3. REPORT MANAGEMENT: INVESTIGATION RESULT

Upon the outcome of the investigative findings, the Case Manager shall, in each case, issue a report addressed to the Board of Directors (the "Report"), which shall:

- summarize the course of the investigation;

- set out the conclusions reached, providing any supporting documentation;
- provide recommendations and suggest actions to be put in place to remedy the Violations found and ensure that they do not occur in the future.

If, at the end investigation results, the following emerges:

- a. the absence of sufficiently substantiated facts, i.e., the unfoundedness of the Internal Report, the Case Manager will dismiss the Internal Report, informing the Reporting Person ("dismissal without remark"), so-called "Report without sufficient and relevant indications" or "Report unfounded";
- b. (b) the final substantiation of the Internal Reporting, so-called "Well-founded Reporting," the Reporting Manager will:
 - i. inform the hierarchical manager of the perpetrator of the Violation as well as the Chief Executive Officer or other appropriately identified person, recommending corrective action;
 - ii. propose disciplinary measures by written notice, in accordance with the Disciplinary System referred to in §9.

Where at the outcome of the investigation proceedings are initiated against a specific reported person, an Ad Hoc Disclosure shall be made to the latter.

If the Violation is particularly serious or concerns one or more members of the Board of Directors, the Case Manager shall inform the other members of the management body and/or the Board of Statutory Auditors, where appointed, if appropriate, also informing the shareholders.

It is understood that, in all cases, upon completion of the verification of the merits of the Report received, the Reporter will be provided with feedback within a reasonable period of time, in any case not exceeding 3 (three) months.

4. CORRECTIV ACTIONS MANAGEMENT AND ANNUAL PERIODIC REPORTING

The hierarchical manager and the Chief Executive Officer, or other appropriately identified person, supervise the implementation of compliance with the identified corrective actions.

The Case Manager, at least annually, prepares a report on the Reports filed and the findings of the activities carried out in relation to the Reports under investigation (the "Annual Report"). The Annual Report is forwarded to the Board of Directors and/or the Board of Auditors and, where appropriate, to the Company's Supervisory Body.

5. PROCESSING AND MANAGEMENT OF PERSONAL DATA

Personal data-including special categories of data and judicial data-disclosed as part of Internal Reporting will be processed in compliance with the provisions of the GDPR as better described in the Whistleblower disclosure ([Attachment 1](#)) and the Involved person disclosure ([Attachment 2](#)) made available on the Viabizzuno S.p.A. website.

Internal Reports may not be used beyond what is necessary to adequately follow up on them.

The identity of the Whistleblower and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the Reporting Person himself/herself:

- a. to people other than the Case Manager and other persons specifically authorized by the Data Controller. The Case Manager shall request such consent before proceeding with disclosure to each person other than the persons authorized to handle the reports.

The Reporting Manager shall request consent using the following wording and notify the data recipient:

I consent I do not consent

to the disclosure of my identity, and any other information from which such identity may be directly or indirectly inferred, to persons other than those authorized to receive or act upon Reports;

- b. in disciplinary proceedings where the charge is based, in whole or in part, on the Report and knowledge of the identity of the Reporting Officer is essential for the defense of the accused. The Case Manager shall:
- o in case of a Report received by paper mail or by face-to-face meeting, request such consent prior to the disciplinary process;
 - o in case of a Report received through an IT platform where already at the time of the transmission of the Report such consent is requested, prior to the disciplinary procedure ask for confirmation of any consent already received or denied.

The Case Manager should request consent using the following wording:

I consent I do not consent

to the disclosure of my identity in disciplinary proceedings where the charge is based, in whole or in part, on the Report and the knowledge of my identity is indispensable for the defense of the accused.

In the case of Oral Reporting by face-to-face meeting, in addition to the consents in (a) and (b) above, the Case Manager shall also acquire the following consent:

- c. to the documentation of the Report.

The Case Manager should request consent using the following wording and notify the data recipient of the data:

I consent I do not consent the Authorized Persons to document the Report by recording it on a device suitable for storage and listening or by report

In the event that the Case Manager has received consent to the documentation of the Reporting referred to in (c) above, he/she shall document the Reporting by recording on a device suitable for storage and listening or by minutes. The Reporting Party may verify, correct and confirm the minutes of the meeting by its own signature.

The protection of the identity of the Whistleblower and Involved Persons is guaranteed until the conclusion of the proceedings initiated on account of the Internal Reporting.

Personal data that are manifestly not useful for the processing of a specific Internal Reporting, where possible, shall not be collected or, if accidentally collected, shall be deleted immediately.

The Involved Person may not exercise the rights set forth in Articles 15-22 of the GDPR if actual and concrete prejudice to the confidentiality of the identity of the Whistleblower may result from the exercise thereof.

2. "EXTERNAL" REPORTING CHANNEL ("External Channels")

The Reporter of Unlawful Behavior may make a Report through External Channels (the "External Report") if, at the time of its submission, one of the following conditions applies:

- a. the Company has not adopted the mandatory Internal Channel, or, even if active, it does not comply with the art. 4 of Legislative Decree 24/2023;
- b. the Whistleblower has already made an Internal Report, through the methods set out in this Policy, without it having been followed up;
- c. the Whistleblower has reasonable grounds to believe that, if he/she made an Internal Report, it would not be followed up effectively or could lead to the risk of retaliation;
- d. the Reporter has reasonable grounds to believe that the Violation may constitute an imminent or obvious danger to the public interest;
- e. is himself the Case Manager.

In the cases above, the Reporter carries out the External Report using the methods prepared and implemented by the ANAC, both in written form, through the IT platforms or other means implemented by the Authority itself, and in oral form, through the telephone line and /or the recorded voice messaging system implemented.

In detail, ANAC has activated an IT channel for the reception and management of External Reports - which can be reached in a specific section of the relevant website link <https://whistleblowing.anticorruzione.it/#/> - which guarantees, also through the use of encryption tools, the confidentiality of the identity of the Whistleblower, the Reported Party, any further subjects involved in the Report, as well as the content of the Report and the related supporting documentation produced.

The same confidentiality is also guaranteed when the External Report is carried out through channels other than those indicated on the ANAC website or reaches personnel other than those responsible for processing External Reports, to whom it is in any case transmitted without delay.

The External Report, submitted to a party other than the ANAC, must be transmitted to the competent Authority within 7 (seven) days from the date of its receipt, giving simultaneous notice of the transmission to the Reporter.

Received the External Report, ANAC provides feedback to the Reporting Party within three months or, if there are justified and motivated reasons, within six months from the date of acknowledgment of receipt of the External Report or, in the absence of said notice, from the expiry of seven days from receipt.

3. PUBLIC DISCLOSURES ("Public Disclosures")

The Whistleblower of Illicit Behavior who makes a public disclosure - i.e. through the press or electronic means or in any case through means of dissemination capable of reaching a large number of people - benefits from the protection provided by the Policy if, at the time of the disclosure, there is a of the following conditions:

- a. the Whistleblower has previously made an Internal and External Report or has directly made an External Report, under the conditions and methods set out in the Policy, without however obtaining feedback within the terms set out in the Policy;
- b. the Whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest, such as in the case where there is an emergency situation or the risk of irreversible damage;
- c. the Whistleblower has reasonable grounds to believe that the External Report may involve the risk of Retaliation or may not have an effective follow-up due to the specific circumstances of the specific case, such as those in

which evidence may be hidden or destroyed or in which there is reason to believe that the person who received the Report may have colluded with the author of the Violation or was involved in the Violation itself.

7. PROTECTION OF THE WHISTLEBLOWER AND THE REPORTED PARTY

1. PROTECTION OF THE WHISTLEBLOWER

In order to protect the Reporter against any retaliatory and/or discriminatory acts, protection measures are envisaged, which apply when the following conditions are met:

- a. at the time of the Report or Public Disclosure, the Whistleblower or the complainant had reasonable grounds to believe that the Information on the Violations was true and fell within the objective scope of this Policy;*
- b. the Report or Public Disclosure was carried out in compliance with the methods set out in this Policy.*

In response to the Report, the protection and confidentiality of the Whistleblower's identity is always guaranteed, processing the data in accordance with the law and adopting every useful measure to prevent the dissemination of the Whistleblower's data and the content of the Report.

Retaliatory or discriminatory acts, direct or indirect, against the Whistleblower for reasons connected, directly or indirectly, to the Report are prohibited and are also sanctioned.

Viabizzuno guarantees the prohibition and removal of the effects of any form of Retaliation against the Whistleblower, including, in particular:

- dismissal, suspension or equivalent measures;*
- demotion or failure to promote;*
- change of functions, change of place of work, reduction of salary, modification of working hours;*
- the suspension of training or any restriction of access to it*
- notes of demerit or negative references;*
- the adoption of disciplinary measures or other sanctions, including pecuniary ones; coercion, intimidation, harassment or ostracism;*
- discrimination, disadvantageous or unfair treatment;*
- failure to convert a fixed-term employment contract into a permanent employment contract, where the worker had legitimate expectations of being offered permanent employment;*
- failure to renew or early termination of a fixed-term employment contract;*
- damage, including to the person's reputation, in particular on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income;*
- blacklisting on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;*
- the early termination or cancellation of the contract for goods or services;*
- the cancellation of a license or permit;*
- subjecting to psychiatric or medical tests.*

It is reiterated that the measures to protect whistleblowers also apply, where appropriate:

- a. to the Facilitators;*

- b. to third parties connected to the Whistleblower and who could risk Retaliation in the Work Context, such as colleagues or subjects linked to the Whistleblower by a stable emotional or kinship bond within the fourth degree;
- c. to legal entities that the Whistleblower owns, works for or is otherwise connected to in a Work Context.

The Whistleblower cannot be held liable for defamation, violation of copyright or secrecy obligations, with the exception of those required by the legal or medical profession, as well as for violation of data protection regulations if, at the time of the Report, had reasonable grounds to believe that the Information on Violations was true, fell within the scope of the legislation and conformed to the established procedures.

No responsibility can be attributed to the Whistleblower even in relation to the conduct adopted to access the information subject to the Report, unless the same constitutes a crime.

The exclusion of liability does not apply in the event that a conviction has been issued, even in first instance, for the crime of defamation or slander or liability for the same title for willful misconduct or gross negligence is established in civil court.

This is without prejudice to cases in which the Report turns out to be false and made with malice or gross negligence or in the case in which the behavior, acts or omissions are not connected to the Report, to the report to the judicial or accounting authority or to the Public Disclosure, or which are not strictly necessary for the detection of the Violation.

Furthermore, the interested parties have the right to legal protection if the Whistleblower is found to be liable of a criminal or civil nature linked to the falsity of what was declared or reported.

Confidentiality and disclosure of the identity of the Whistleblower (where communicated) and of any other information from which the identity of the Reporting person can be deduced directly or indirectly, is permitted to the extent that anonymity and confidentiality are opposable on the basis to the provisions of the law.

In particular, it is the responsibility of the Case Manager to ensure the confidentiality of the identity of the Whistleblower (where communicated) from the moment of taking charge of the Report until the end of the checks on its validity, even in cases where it turns out to be incorrect or unfounded. Reports cannot be used beyond what is necessary to adequately follow up on them.

The identity of the Whistleblower (where communicated) and any other information from which the same can be deduced directly or indirectly, cannot be revealed - without his express consent - to persons other than those competent to receive or follow up on the Reports, expressly authorized to process such data.

In any case, personal data that is manifestly not useful for the processing of a specific Report are not collected or, if collected accidentally, are deleted immediately.

In the case of transmission of the Report to other structures/bodies/third parties for carrying out investigative activities, it is the obligation of the Reporting Manager to separate the identifying data of the Whistleblower (where known) from the content of the Report, so that the facts reported can be processed anonymously and that the association of the Report with the identity of the Whistleblower (where known) occurs only in cases where this is strictly necessary.

For Reports transmitted through the Platform referred to in the previous paragraphs, the confidentiality of the Whistleblower is guaranteed in the following ways:

- the Platform consists of a web application, separate and independent from the Company's IT systems, as it is hosted on an independent server which allows Reports to be made from any device, in a highly confidential and facilitated manner, guaranteeing the protection of the whistleblowers' identification data, also through the use of encryption tools;

- the Platform guarantees high standards of security, non-traceability, and integrity of the information, as well as confidentiality of the identity of the Reported Party and the Whistleblower, leaving the Whistleblower the possibility of entering the Report even anonymously. This protection is also guaranteed in the case of verbal communications;
- adoption of the "no-log" policy, which does not reveal in any way, direct or indirect, information on connection methods (for example, server, IP address, mac address, ...), thus guaranteeing complete anonymity in 'access. This means, in particular, that the IT systems are not able to identify the access point to the portal (IP address), even if access is made from a computer connected to the Company's network;
- assignment of an identification code to the Report in order to protect the identity of the Whistleblower;
- provision of internet access to the Company's website (available to anyone, including employees) in the absence of registration, as the Whistleblower can remain anonymous. The latter, if he deems it, can otherwise indicate his name by providing express consent for his personal details to be communicated.

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

As part of the disciplinary proceedings activated by the Company, the identity of the Reporter (where known) cannot be revealed where the dispute of the disciplinary charge is based on investigations distinct and additional to the Report, even if consequent thereto.

However, if the dispute is based, in whole or in part, on the Report and knowledge of the identity of the Whistleblower is indispensable for the defense of the accused, the Report will be usable for the purposes of disciplinary proceedings only in the presence of the Whistleblower's consent to the disclosure of his identity. In such cases, notice is given to the Whistleblower by written communication, containing the reasons for the disclosure of the confidential data.

Furthermore, those who believe they have suffered retaliation as a consequence of the Report or Public Disclosure must inform the Case Manager who, after having assessed the existence of the retaliatory or discriminatory elements, reports the hypothesis of discrimination to the CEO or to other appropriately identified subject.

2. PROTECTION OF REPORTED PARTY

In order to avoid prejudicial consequences within the Work Context, even if only of a reputational nature, the protection reserved for the Whistleblower, referred to in the previous paragraph, must also be granted to the Reported Person.

Following investigations into the validity of the Report, the Case Manager, if disciplinary proceedings are opened against the Reported Person:

- inform the latter;
- keeps him updated on the developments of the proceedings, compatibly with the carrying out of the verification and collection of necessary evidence activities, so as to allow him to exercise his right of defense.

The personal data of the Reported Person may be transmitted to the competent administrative or judicial authority and, more generally, to public entities, in compliance with legal formalities, also for the purpose of following up on requests received from them.

The Company requires everyone to collaborate in maintaining a climate of mutual respect and prohibits and sanctions behaviors that may damage the dignity, honor and reputation of each individual. The confidentiality guarantees established by this Policy also protect the Reported Party or other subjects involved.

The Reported Party has the right to be informed of the existence of the Report and the outcome of the checks carried out. However, this information may be delayed, limited to the time necessary, in order to avoid the risk of jeopardizing the investigation needs, including those possibly requested by the Judicial Authority, if involved.

The Reported Person cannot be sanctioned in the absence of objective confirmation of the reported Violation, or without the facts covered by the Report having been investigated and the related charges contested, as required by the applicable regulations.

For further protection of the Reported Party, the actions and powers permitted by law remain unaffected.

It is specified that the identity of the people involved and mentioned in the Report is also protected until the conclusion of the proceedings initiated due to the Report, in compliance with the same guarantees provided in favor of the Whistleblower.

8. DISCIPLINARY SYSTEM

Disciplinary proceedings are expected to be initiated against the person responsible in the event of a violation of this Policy and when the Company ascertains that:

- a Violation has been committed;*
- Retaliation has occurred;*
- the Report was hindered, even in an attempted form;*
- the obligation of confidentiality referred to in art. 12 of Legislative Decree 24/2023;*
- the Whistleblower has made a Report, Public Disclosure or complaint to the Judicial Authority with malice or gross negligence;*
- the verification and analysis of the internal reports received was not carried out.*

The applicable sanctions are those referred to in the Organizational Model, as borrowed from the CCNL applicable to the Company.

The Company, through the relevant bodies and functions, takes steps to impose, with impartiality, uniformity and fairness, proportionate sanctions for violations of this Policy.

Failure to comply with and/or violate the rules of conduct indicated in this Policy by the Company's employees/administrators constitutes failure to fulfill the obligations deriving from the employment relationship, giving rise to the application of disciplinary sanctions; the same will be applied in compliance with the provisions of the law and collective bargaining and will be proportionate to the seriousness and nature of the facts.

Violations of this Policy by members of the Company's corporate bodies must be communicated to the Case Manager / the Board of Directors, who will take appropriate initiatives in accordance with the law.

Any behavior carried out by Third Parties in violation of the provisions of this Policy may also lead to the termination of the contractual relationship, without prejudice to any request for compensation by the Company if such behavior causes damages to it.

9. STORAGE OF DOCUMENTATION

The documentation used to carry out the activities (even in the case of irrelevant reports) must be kept in a specific archive, in order to guarantee the reconstruction of the different phases of the process.

The Reports, Internal and External, and the related documentation, are kept for the time necessary to process the Report and, in any case, no later than 5 (five) years from the date of communication of the final outcome of the reporting

procedure - in compliance of the confidentiality obligations referred to in Article 12 and of the principle referred to in Articles 5, paragraph 1, letter e) of Regulation (EU) 2016/679 and 3, paragraph 1, letter e) of Legislative Decree 18 May 2018, n . 51. Personal data that is clearly not useful for the processing of a specific Report will not be stored and, if collected accidentally, will be deleted immediately.

If a registered telephone line or another registered voice messaging system was used for the Report, the Report, with the consent of the Reporter, is documented by the personnel in charge by recording on a device suitable for storage and listening or by transcription whole wheat.

If an unregistered telephone line or another unregistered voice messaging system is used for the Report, the Report is documented in writing with a detailed report of the conversation by the relevant personnel.

When, at the request of the Whistleblower, the Report is made orally during a meeting with the relevant personnel, it, with the consent of the reported person, is documented by the relevant personnel by recording on a device suitable for storage and listening or by verbal means.

10. ATTACHMENTS

Attachment 1 – Whistleblower Disclosure;

Attachment 2 – Involved Person Disclosure.

WHISTLEBLOWING REPORT FORM

Identifying information of the Whistleblower:

Nome and Surname	
Tax Identification Number	
Address	
Role held within the Company	
Phone number for further contact	

Data and information on the reported Violation:

Area to which the misconduct can be referred (e.g. administration, service)	
Timeframe during which the misconduct occurred	
Location of the Violation	

Brief description of the Reported facts:

.....

.....

.....

.....

.....
.....
.....
.....
.....
.....

Other individuals to whom the same report has been presented:

<i>Authority</i>	<i>Date</i>

Sed, if possible, any documentation accompanying the Report.