MUVIQ Srl
Stradale Torino 603 – Frazione San Bernardo d'Ivrea
10015 Ivrea (TO)
Cf: 12849500017 REA TO-1320586

WHISTLEBLOWING POLICY

Issue 2.0 of August 9, 2024

MUVIQ Srl
Stradale Torino 603 – Frazione San Bernardo d'Ivrea
10015 Ivrea (TO)
Cf: 12849500017 REA TO-1320586

TABLE OF CONTENTS

Premise

By Legislative Decree No. 24 of 8 March 2023 – on the "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and laying down provisions on the protection of persons who report breaches of national law." – the following were transposed into national law: Directive (EU) 2019/1937, which innovated the pre-existing reporting rules[1] , bringing together in a single regulatory text the entire regulation of reporting channels and the protections granted to whistleblowers, both in the public and private sectors. Legislative Decree No. 24/2023 brings together in a single regulatory text the entire regulation of reporting channels and the protections granted to whistleblowers in both the public and private sectors. The result is an organic and uniform discipline aimed at greater protection of the whistleblower, in this way, the latter can be more incentivized to report wrongdoing within the limits and in the manner indicated in the decree.

The relevance of the public interest recognized to the whistleblowing tool is such as to bend in its favour the impediment to the disclosure of information covered by the obligation of secrecy referred to in Articles 326, 622 and 623 of the Criminal Code and Article 2105 of the Civil Code.

In compliance with the provisions in force, it has defined its own internal institutional channel (hereinafter, for the sake of brevity, the "*WB Channel*") for reports concerning violations – as defined below – and represented, through the publication of this policy, the rules of transparency and the overall functioning of the organizational and procedural system used to oversee the management of reports.

The WB Channel, identified by this policy, has been created by Muviq Srl to be subservient to all the structures belonging to its entity. Therefore, all offices, establishments and branches wherever located in Italy or abroad are included in the scope of application of this policy. The WB Channel collects and centralizes all information flows aimed at reporting violations of mandatory or optional rules whose application derives from EU law, national law, internationally recognized standards applied by Muviq Srl, the Code of Ethics and the Organization, Management and Control Model adopted pursuant to Legislative Decree no. 231/2001.

This document is issued and updated, after consulting the Representatives and/or Trade Unions referred to in Article 51 of Legislative Decree No. 81 of 2015.

[1] Law no. 190/2012, containing provisions for the prevention and repression of corruption and illegality in the public administration. By amending Legislative Decree no. 165 of 30 March 2001, it introduced the protection of public employees who report wrongdoing (Article 54-bis of Legislative Decree 165/2001) but it is only with Law No. 179 of 30 November 2017 that the reporting tool acquires specific scope and dignity, expanding its strength and effectiveness in the public sector (further updating the aforementioned Article 54-bis of Legislative Decree 165/2001) and also intervening in employment relationships in the sector private.

Regulatory references

In addition to Legislative Decree No. 24/2023 mentioned in the **Premise**, the rules governing the whistleblowing management system represented herein are subject to and made compliant with the following additional rules – mandatory or optional – of main reference:

- Directive (EU) 2019/1937 [Directive];
- Legislative Decree No. 231 of 8 June 2001 [Decree No. 231];
- General Data Protection Regulation (EU) 2016/679 [GDPR]
- Legislative Decree no. 196 of 30 June 2003 [Privacy Code]
- ANAC Guidelines of 12 July 2023
- Confindustria Whistleblowing Operational Guide of October 2023
- ISO 37002:2021 Guidelines on Whistleblowing Management Systems

Definitions

Term	Description
Recipients of the policy	The recipients of this whistleblowing policy are all natural persons in any way related to the *work context* of Muviq Srl .
Work context of Muviq Srl	Present or past work or professional activities carried out in the context of the relationships referred to in paragraph 2, through which, regardless of the nature of those activities, a person acquires information about infringements and in the context of which he or she could face retaliation if reported or publicly disclosed or reported to a judicial or accounting authority
Public Disclosure	To make information about violations publicly available through the press or electronic means or otherwise through means of dissemination capable of reaching a large number of people
Facilitator	A natural person who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential;
Person involved	A natural or legal person named in the internal or external report or public disclosure as a person to whom the violation is attributed or as a person otherwise involved in the reported or publicly disclosed violation
Retaliation	Any behaviour, act or omission, even if only attempted or threatened, carried out by reason of the report, the complaint to the judicial or accounting authority, or public disclosure and which causes or may cause, to the reporting person or to the person who has filed the complaint, directly or indirectly, unjust damage, to be understood as unjustified damage.
Whistleblower	The natural person who makes the report or public disclosure of information about violations acquired in the context of his or her work context.

Term	Description
Signalling	Written or oral communication, separately: a) "internal reporting" means the communication, written or oral, of information on violations submitted through the internal reporting channel referred to in Article 4 of Legislative Decree no. 24/2023; b) "external reporting" means the communication, written or oral, of information on violations, submitted through the external reporting channel referred to in Article 7 of Legislative Decree no. 24/2023;
Follow-up (follow up)	Action taken by the person entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the investigations and any measures taken
Violations	Conduct, acts or omissions that harm the public interest or the integrity of the public administration or private entity included in the types indicated in paragraph 2.1.

1 Purpose of this document

This whistleblowing policy [hereinafter, for the sake of brevity, also the "*WB Policy*"] is intended to govern the overall functioning of the whistleblowing management system.

In particular, the operation of this system implies the precise regulation of the following main aspects:

a) the definition and activation of the institutional channel identified by the Company to allow the secure transmission of reports;

b) the definition of the methods of safe transmission of reports;

c) the transparent organisational and procedural methods identified to follow up on the reports received and any interaction with the whistleblower;

d) the protection of whistleblowers and other parties involved.

The following paragraphs aim to provide more detailed operational indications about the methods of access to the institutional channel identified by Muviq Srl, the objective and subjective scope of application, the operational phases of examination and verification of the facts reported and the methods of conclusion of the same.

It is also the essential purpose of this policy to inform all recipients of this policy about the possible conclusions of the report management process, the related sanctioning profiles if illegal or irregular conduct is confirmed, as well as the forms of protection for the authors of the reports and for the other parties involved, provided for by the law and ensured by Muviq Srl.

2 The report

Persons who work in the work context of a public or private sector entity are entitled to formulate and transmit reports, as:

- civil servants (i.e. employees of public administrations referred to in Article 1, paragraph 2, of Legislative Decree No. 165/2001, including employees referred to in Article 3 of the same decree, as well as employees of independent administrative guarantee, supervision or regulatory authorities; employees of public economic entities, private law entities subject to public control, in-house companies, bodies governed by public law or public service concessionaires);
- employees of private sector entities;
- self-employed workers who carry out their work in public or private sector entities;
- collaborators, freelancers and consultants who work for public or private sector entities;
- volunteers and trainees, paid and unpaid;
- persons with administrative, managerial, control, supervisory or representative functions, even if these functions are exercised on a purely de facto basis, in public or private sector entities.

Persons with the above-mentioned characteristics can make reports:

a) when the legal relationship is ongoing;

b) when the legal relationship has not yet started, if information on violations has been acquired during the selection process or at other pre-contractual stages;

c) during the probationary period;

d) after the dissolution of the legal relationship if the information on the violations was acquired before the termination of the relationship itself (pensioners).

2.1 What can be reported

The activation and use of appropriate reporting channels is aimed at the emergence of behaviours, acts or omissions that harm the public interest or the integrity of the public administration or private entity.

The reference standard provides an initial list of the conducts subject to these regulations:

1) administrative, accounting, civil or criminal offences

2) significant unlawful conduct pursuant to Legislative Decree no. 231 of 8 June 2001 or violations of the Organisation, Management and Control Model adopted by the Company pursuant to art. 6 of Legislative Decree no. 231/2001;

3) offences falling within the scope of European Union or national acts relating – to the extent applicable to the Authority – to the following sectors: public procurement; financial services,

products and markets and the 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 European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union as specified in the relevant secondary legislation of the European Union;

5) acts or omissions concerning the internal market (e.g. competition and State aid infringements), and

6) acts or conduct which frustrate the object or purpose of the provisions referred to in Union acts in the areas referred to in points (3), (4) and (5);

In compliance with the principle of unitary nature of the internal reporting channel, conduct carried out in contrast with:

a) the provisions of the Code of Ethics adopted by the Entity, where not already included in the cases explained above;

b) the rules voluntarily adopted by the Body through management systems regulated by Certification Bodies.

The subject of the report may also concern – in addition to the aforementioned irregular conduct – the following:

i. information relating to conduct aimed at concealing the violations indicated above;

ii. illegal activities that have not yet been carried out but that the whistleblower reasonably believes may occur in the presence of precise and consistent concrete elements;

iii. the well-founded suspicions regarding the illegal conduct and activities referred to above.

2.1.1 The content of the report

In order for the report to be usefully taken into consideration, it must be made in sufficient detail to have a precise, detailed and verifiable content.

The absence of precise elements that do not allow an objective and concrete reconstruction of the facts, situations or conduct subject to the report may be an impediment to the carrying out of the investigation aimed at ascertaining the validity of the report.

The lack of validity of a report or the impossibility of verifying its validity due to the absence of the aforementioned requirements will result in the automatic filing of the report without any further follow-up.

2.1.2 The good faith of the whistleblower

The whistleblower must act in good faith.

At the time of reporting or reporting to the judicial or accounting authority or public disclosure, the reporting or complaining person must have reasonable grounds to believe that information about violations reported, publicly disclosed or reported is true and falls within the scope of the legislation or other circumstances permitted by this policy.

It is possible that – due to a specific condition, linked to the job position held by the whistleblower or to his or her incomplete availability of information – the report is unfounded. Valuing the good faith of the whistleblower at the time of reporting, it is provided that the reporting person will benefit from the protections only if, at the time of reporting, he or she had reasonable grounds to believe that the information on violations reported, publicly disclosed or reported was true.

In addition, the whistleblower is also protected if he reveals or disseminates information on violations:

- covered by the obligation of secrecy, other than that of the legal and medical profession, or
- relating to copyright protection or
- the protection of personal data, or

if, at the time of the report, complaint or disclosure, he had reasonable grounds to believe that the disclosure or dissemination of the information was necessary to make the report and the same was made in the manner required by law.

The reasons that led the whistleblower to make the report are to be considered irrelevant for the purpose of deciding on the recognition of the protections provided for by the decree.

2.2 What cannot be reported

Referring to the same definition of reporting, disputes, claims or requests related to a personal interest of the reporting person that relate exclusively to their individual employment or public employment relationships, or inherent to their employment or public employment relationships with hierarchically superior figures, are not allowed.

Any communications from the aforementioned content cannot, therefore, be taken into consideration and will be archived at the same time.

In order to facilitate the identification of the objective areas of possible application of this policy (and the related protections), a typed list of the cases considered admissible is set out in Annex 1. Failure to provide for these may result in extraneousness to the objective scope of application of this policy and consequent exclusion from the relevant forms of protection.

3 The reporting channels allowed by the law

The law provides for different channels to allow reports to be made. These channels are not discretionally alternative but scalability between them is allowed only when defined and precise conditions occur.

3.1 The internal channel

Legislative Decree no. 24/2023 provides, in art. 4, that public sector entities and private sector entities, after consulting the representatives or trade unions referred to in Article 51 of Legislative Decree no. 81 of 2015, shall activate their own reporting channels, which guarantee, including through the use of encryption tools, the confidentiality of the identity of the reporting person, of the person involved and of the person in any case mentioned in the report, as well as the content of the report and the related documentation.

The management of the reporting channel is entrusted to a dedicated autonomous internal person or office with staff specifically trained to manage the reporting channel, or it is entrusted to an external party, also autonomous and with specifically trained personnel.

Reports are made in written form, also by electronic means, or orally. Internal reports in oral form are made through telephone lines or voice messaging systems or, at the request of the reporting person, through a direct meeting set within a reasonable time.

For reports that refer to violations of the provisions contained in Legislative Decree no. 231/20001 or in the Organization, Management and Control Model, it is mandatory to use the internal channel, which is the only one that can be used for these types of reports. Therefore, communications of reports on administrative liability pursuant to the aforementioned decree are not allowed through the external channel or through public disclosure.

More details on how the internal channel can be accessed and operated can be found in paragraph 4.

3.2 The external channel

The competent authority for external reporting, including from the private sector, is the National Anti-Corruption Authority (ANAC).

It is possible to report to the Authority only if one of the following conditions is met:

a) there is no mandatory activation of the internal reporting channel in the context of the work context, or this, even if mandatory, is not active or, even if activated, does not comply with the provisions of Article 4 of Legislative Decree no. 24/2030;

b) the reporting person has already made an internal report and the same has not been followed up;

c) the reporting person has reasonable grounds to believe that, if he or she made an internal report, it would not be followed up effectively or that the same report could lead to the risk of retaliation;

d) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

For more information on how to access the external channel:

https://www.anticorruzione.it/-/whistleblowing

3.3 public disclosure

Public disclosure means making information about violations publicly available through the press or electronic means or in any case through means of dissemination capable of reaching a large number of people.

The reporting person who makes a public disclosure benefits from the protection provided for by Legislative Decree No. 24/2023 if, at the time of the public disclosure, one of the following conditions is met:

a) the reporting person has previously made an internal and external report or has made an external report directly and no feedback has been given within the established deadlines on the measures envisaged or adopted to follow up on the reports;

b) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;

c) the reporting person has reasonable grounds to believe that the external report may involve the risk of retaliation or may not be effectively followed up due to the specific circumstances of the specific case, such as those in which evidence may be concealed or destroyed or in which there is a well-founded fear that the person who received the report may be colluding with the offender or involved in the violation itself.

3.4 the complaint to the authorities

Unlawful conduct can always be reported to the accounting or ordinary judicial authority.

Persons who – due to the specific role held within the organisation – should find themselves in the capacity of [Società]public officials or persons in charge of public service have an obligation to report, by virtue of the provisions of the combined provisions of art. 331 of the Code of Criminal Procedure and Articles 361 and 362 of the Italian Criminal Code. In this case, reporting through the internal reporting channel does not replace, where the conditions are met, that to the judicial authority.

4 The internal signalling channel of Muviq Srl

Muviq Srl, after consulting the trade unions, has activated its reporting channel through the adoption of an electronic platform (hereinafter, the "*WB platform*") equipped with adequate security measures and designed to guarantee the confidentiality of the identity of the reporting person, the person involved and the person in any case mentioned in the report, as well as the content of the report and the related documentation.

The WB platform can be reached at the following web address:

HTTPS://MUVIQ.WHISTLELINK.COM/

The WB platform is resident on a domain external to the Entity, with an independent and qualified supplier to guarantee the security and confidentiality requirements.

Through the WB platform, the person who intends to make a report is enabled to do so:

i. in written mode, through the guided compilation of a form containing the questions referred to in Annex 2;

ii. in oral mode, through a voice recording. The WB platform does not currently alter the voice tone, therefore, the author of the report could be identifiable.

4.1.1 Technical and organisational security measures

The WB platform – in accordance with the provisions of art. 32 GDPR (security of processing) – is equipped with adequate technical and organizational measures to ensure a level of security appropriate to the risk. These measures include, among other things, the encryption of data both in transit to/from the platform and within the database.

The WB platform is equipped with measures aimed at ensuring access only to authorized persons, the availability and integrity of data. The IP address of the whistleblower is not tracked, while the activities carried out within the platform by the persons authorized to access the platform are stored through a log file.

The service provider is ISO 27001:2017 certified for Information Security Management Systems. The databases reside within the European Economic Area (EEA).

Muviq Srl, in accordance with the provisions of the GDPR, has regularly carried out a data protection impact assessment.

5 The whistleblowing process

Before proceeding with the description of the organizational and procedural structure regarding the report management process, it is considered appropriate to specify a fundamental aspect for the

confidentiality and security of the entire life cycle of a report and of the people involved in any capacity (whistleblowers, reported, facilitators, verifiers, etc.).

The choice made by Muviq Srl. to equip itself with a WB platform dedicated to this management was made in order to be able to ensure and store within it every single activity, operation and assessment pertaining to the report, thus avoiding the leakage of potentially sensitive and sensitive information and replacing traditional communication tools between verifiers and whistleblowers and between verifiers themselves – such as ordinary e-mail – deemed inadequate to ensure the [Società]**security standards necessary** to carry out processing in compliance with regulatory provisions and respect for the fundamental rights and freedoms of the data subjects.

Therefore, this policy provides that all the activities carried out with reference to the specific report are carried out within the WB platform, taking advantage of the features made available by the same also in terms of involvement of third parties (where necessary) and communication to the various interested parties.

For the same reason, Muviq Srl urges the exclusive use of the WB Channel identified in paragraph 4, as it cannot guarantee the adequacy of the technical and organisational measures put in place to guarantee security and confidentiality in cases where reports should be received through other channels not expressly recognised by this policy.

5.1 Roles and responsibilities

The Company has defined a specific internal organisational structure for the management of reports.

In particular, the following internal structures are important:

i. **Supervisory Body of Muviq Srl** – a body composed of professionals with proven autonomy and independence, appointed pursuant to Article 6 of Legislative Decree no. 231/2001 (hereinafter, also, "**SB**").
   The SB is responsible for:
   a) the receipt of all reports received on the WB platform. In this context, it is responsible for carrying out a **preliminary admissibility check**, as well as for following up on the management of reports, as regulated below, also through the possible involvement of the subjects indicated below;
   b) the performance of the further management phases of the reports, in cases where they are of potential relevance for the purposes of the administrative liability of Muviq Srl pursuant to Legislative Decree no. 231/2001, the correct functioning of the organization, management and control model and compliance with the Code of Ethics. In this context, in fact, the SB is entrusted with precise tasks of analysis and investigation – which it can carry out directly or through professionals appointed for this purpose – aimed at documenting an investigation aimed at clarifying the "**validity**" of each report.

The SB, having assessed the absence of incompatibility and conflict, may share – for preliminary and in-depth purposes – the contents of the same with other subjects, identified below as persons authorised to process the reports.

As of the adoption of this WB Policy and at each renewal of the composition, the SB shall define and adopt its own internal operating regulations, in the name of transparency and fairness of treatment. The Internal Regulations are sent to the Chairman of the Company for information purposes.

ii. **Chairman of Muviq Srl** – in cases where the report relates to issues unrelated to the discipline of Legislative Decree no. 231/2001 and to the proper functioning of the organization, management and control model or compliance with the Code of Ethics, the Supervisory Body of Muviq Srl, having assessed the absence of incompatibility and conflicts, will entrust the Chairman of the company with the task of following up on the report. In this circumstance, the Chairman of the company – in compliance with the principles of confidentiality provided for in this WB Policy – may avail himself of the collaboration and support of Directors/Functional Area Managers – senior figures with management and/or management/coordination tasks in the various areas of company operations, who may be entrusted with the task of following up on the management of the report. These resources, if appointed, also assume the same commitments and obligations of confidentiality and data protection contained in the report already set out above.

The overall scope of the parties potentially involved in the whistleblowing process may also include – in the final phase of the management of reports – the members of the Board of Directors and the members of the Board of Statutory Auditors. These bodies are responsible for:

- become aware - on the initiative of the person who followed up on the report - of the existence of the report and the outcome of the analysis of its merits and
- **assess the admissibility of the report** and, therefore, the adoption of any disciplinary measures - in accordance with the disciplinary systems and regulations adopted by Muviq Srl - or, in the most serious cases, of reporting to the competent Judicial Authority.

At the end of the assessment of admissibility, the subjects identified above may involve the competent company functions (e.g.: Human Resources, Legal Affairs, etc.) according to the criteria of necessity and reasonableness.

Finally, the subjects who – for specific purposes attributed to them – are involved in the process of managing reports, acting as data processors pursuant to art. 28 GDPR:

iii. the provider of the web platform for the management of reports, made usable in Software as a service (SaaS) mode configured and customized without any type of physical technological supply or license costs for Muviq Srl;

iv. (if any) **external professionals** appointed from time to time by the above-identified parties to carry out investigation, audit and investigation activities to ascertain the facts and conduct reported.

5.2 The transmission of the report

The person who intends to submit a report can freely connect to the web address **htts://muviq.whistlelink.com/** . The system is configured in such a way that it does not track – for the protection of the reporting person – the IP address from which the same makes the connection.

When the screen is opened, the whistleblower finds a brief description of the purposes of the platform. In particular, it is explained what can and cannot be reported and other information on how to manage reports.

On the opening screen, some options are also available, among which the main ones are:

- **SEND THE REPORT HERE:** opens the detail screen containing the guiding questions to issue a complete and detailed report [see form in attachment 2];
- **FOLLOW YOUR CASE:** allows the person who has already made a report to securely access their report to provide or receive updates to/from the person in charge of following up on the same;
- **INFORMATION ON THE PROCESSING OF PERSONAL DATA:** it is possible to read the Information on the processing of personal data pursuant to articles 13 and 14 GDPR.
- **OUR REPORTING CHANNELS:** indicates the contact and communication methods activated;
- **REPORT MANAGEMENT POLICY: at the** end of the opening screen, there is a link to the web page where you can find the updated version of this document.

The person who makes a report is also free to declare his or her identity – which will always be protected in every location – or to remain anonymous. To this end, it is of fundamental importance that the reporting person writes down – in a secure and confidential manner – the credentials for subsequent access to the WB platform. These credentials consist of:

- an **identification code** of the report entered, provided by the WB platform at the end of the procedure for entering the required information;
- a **password** defined independently by the reporting person.

The loss of the aforementioned credentials will not allow access to the same report. Neither the company nor the WB Platform provider is able to retrieve such information. In the event that the reporting person loses these credentials and has an interest in interacting with the persons in charge of following up on the reports, he or she may possibly re-enter the report which will be linked – by the person in charge – to the previous one.

5.2.1 The transmission of the report by direct interview

Article 4 of Legislative Decree no. 24/2023 provides, in paragraph 3, for the specific possibility for the reporting person to issue his or her report also "*through a direct meeting set within a reasonable time*".

In this case, the SB is available, within 10 working days of the request, to hold a meeting in a place suitable to guarantee the confidentiality of the reporting person.

The content of the report, thus taken over by the SB, is promptly transcribed by the same within the WB platform, in order to allow it to be managed in the secure and confidential manner ensured by the platform itself.

In order to ensure the correct interpretation and transcription of the content of the report transmitted orally by the reporting person, the same may receive – where available – the access credentials to the report entered in the WB platform to verify its content and possibly integrate or modify it as well as to allow any subsequent interaction with the person in charge to follow up.

5.3 Receipt of the report and analysis of admissibility

The WB platform is configured in such a way that, following the insertion of a report, the members of the SB automatically receive a notification, by e-mail, notifying them of the receipt of a report.

Without delay, the SB – in the manner that it will have had the opportunity to define within its Operating Regulations – takes steps to "take charge" of the report and carry out a preliminary verification of its admissibility.

The objective of the preliminary check is to:

- ascertain the relevance of the report, in terms of entities and subjects involved, scope and content, sufficient degree of concreteness of the information produced;
- verify and possibly rectify – where the conditions are met – the objective area of reference indicated by the whistleblower, in order to identify the person required to follow up on the report in the most appropriate way, once the preparatory checks aimed at ascertaining the absence of incompatibility and conflict of interest have been carried out.

The SB, as the person responsible for receiving reports, is responsible for notifying the whistleblower of receipt and taking charge of the report within 7 days of receipt of the same. This notification is carried out exclusively within the WB platform and the reporting person will be able to evidence of it within his or her case by accessing it with the credentials received at the time of sending the report.

In cases where the admissibility test does not give a satisfactory result because:

a) [*Notification not applicable*] - the content of the alert appears to be completely unrelated to the context of Muviq Srl
b) [*unsubstantiated or unverifiable report*] - the content of the report is rather generic and in any case lacks concrete and circumstantial elements on which to start an investigation;
c) [*report outside the scope of application*] - the content of the report relates to disputes of an individual personal nature; therefore, outside the scope of application of Legislative Decree no. 24/2023 as already specified above or the other areas allowed by this WB Policy;

The SB shall archive the same, drawing up an internal note justifying the decision and giving feedback to the reporting person.

In cases where the admissibility check highlights information worthy of verification, the SB:

i. having ascertained the absence of incompatibility and conflicts, informs the Chairman of the Company of the report received. This information must not infringe the principles of confidentiality or investigative competence, identified by this WB Policy;

ii. carries out directly, also with the support of third parties, the further activities of verification and in-depth analysis of the reports in order to ascertain their validity, through documented investigative activity conducted on a confidential basis, assuming in this sense the role of person in charge;

iii. forwards the report received, in cases where it does not relate to the matters within its competence (see paragraph 5.1 point i) to the Chairman of the Company, after having carried out the preparatory verification of the absence of incompatibility and conflict of interest.

The Chairman of the Company, having examined the nature of the report, assesses the assignment of the task of following up on the in-depth investigations aimed at ascertaining the validity of the report to a specific person, individual or collegial, within the organization or external to it (who becomes the person in charge).

The forwarding and assignment are carried out through the internal functions of the WB platform by granting access rights to the specific report.

5.4 The preliminary investigation and the verification of validity

The person in charge has the task of examining the information and any documentary evidence provided by the reporting person in order to ascertain the validity of the facts reported.

During this in-depth analysis, the person in charge may contact the reporting person – by means of special communications to be included in the communication exchange area – in order to obtain clarifications and clarifications as well as any further evidence where available.

In order to fully carry out the preliminary activity, the person in charge may:

- make use – where deemed appropriate – of other structures of the Companies in order to acquire information, data and evidence useful for verifying the validity of the report;
- make use of external professionals specialized in carrying out audit activities or forensic investigations.

In both cases just described, it is the responsibility of the person in charge to transfer the same confidentiality obligations on personal data and facts contained in the report and proceed – where necessary – to the appointment as Data Processor pursuant to art. 28 GDPR.

In the presence of several reports relating to the same facts, the SB and/or the Chairman of the Company shall link them in order to standardise the initiatives to be followed up and the consequent conclusions.

The internal meetings held during the investigation by the person in charge, any interactions with other authorised parties (SB, Company Chairman, Directors/Function Managers, external consultants, etc.),

any interviews or interactions with the whistleblower as well as the final conclusions are tracked and documented within the WB platform.

The preliminary investigation is normally completed within 3 months of receipt of the report. If, for reasons of particular complexity of the preliminary activity, it is necessary to extend the aforementioned deadline, the person in charge shall inform the reporting person of this need with the relevant reasons.

At the end of the preliminary investigation, the person in charge informs the SB and/or the Chairman of the Company and the reporting person of the conclusion.

The outcome of the preliminary investigation can be codified as follows:

- Unfounded reporting: in this case, the filing is carried out if the conditions of good faith on the part of the reporting person are met. In the presence of a report made with intent or gross negligence, the person in charge transmits the conclusions to the competent Human Resources Department – for information, informing the Supervisory Body and/or Chairman of the Company – for the analysis of the admissibility against him;

- reporting not founded with actions: this is the case in which the report, although not presenting any credible profiles, highlights areas for improvement in the internal control system of Muviq Srl . It is the task of the person in charge to formulate a summary of the critical issues encountered to be brought to the attention of the Head of the competent structure of Muviq Srl, at the same time providing information for the knowledge of the Supervisory Body. The report is, therefore, archived;

- well-founded report: the person in charge proceeds to prepare a final report to be submitted to the attention of the competent administrative body – for information, informing the Supervisory Body – for the conduct of the examination of the procedure. In the event that the preliminary investigation has highlighted areas for improvement of the internal control system of ,Muviq Srl these will be brought to the attention of the examination of admissibility for the adoption of the improvement actions deemed appropriate. The report is then archived.

5.4.1 Ongoing court proceedings

In cases where the report relates to facts and events subject to investigations by the Judicial Authority or the same are initiated after the investigation has begun, the latter is, as a rule, suspended until the conclusion of the investigations carried out by the competent bodies appointed by the Authority, without prejudice to any defensive needs of Muviq Srl, in which case the verification activities are absorbed within the scope of the assignment assigned to the lawyers identified by Muviq Srl.

5.5 The examination of admissibility and the closure of the report

The recipient of the results of the investigation is called upon to express himself on the basis of the results of the investigation on the admissibility in terms of sanctions for the conduct found.

In particular, the following cases can be highlighted:

a) admissibility against the subjects involved in the report for the application of sanctioning measures in accordance with the disciplinary system adopted by Muviq Srl– both against subjects belonging to the internal organization and to subjects external to it – consistently, to the extent applicable, with the CCNL and the Workers' Statute;

b) admissibility against the subjects involved in the report for the complaint to the Judicial Authority;

c) prosecution against the reporting person (in the presence of an unfounded report transmitted with intent or gross negligence) for the application of sanctioning measures in accordance with the disciplinary system adopted by the companies, in line with the related CCNL and the Workers' Statute where applicable.

The SB and/or the Chairman of the company shall be informed of the assessment and decision taken.

The SB monitors the closure of ongoing reports every six months.

5.6 The archiving of reports

The SB oversees that all reports that have come to an end are accurately documented within the WB platform with particular reference to the assessments of admissibility.

The person in charge shall proceed to close the report and file it.

5.7 Reporting

The SB and the Chairman of the Company carry out half-yearly reporting, according to their respective competences, with statistical content and without identifying elements of the persons involved, to the Board of Directors and the Board of Statutory Auditors (the Chairman of the Company also to the Supervisory Body), regarding the reports received, the nature of the same and the conclusions reached.

6 The processing of personal data

The processing of personal data relating to the receipt and management of reports is carried out by the Companies, in their capacity as Data Controller, in compliance with European and national principles on the protection of personal data, providing appropriate information to the reporting persons and persons involved in the reports, as well as adopting appropriate measures to protect the rights and freedoms of the data subjects.

The rights referred to in art. 15 to 22 of Regulation (EU) 2016/679 may be exercised within the limits of the provisions of Article 2-undecies of Legislative Decree No. 196 of 30 June 2003.

The reports transmitted on the internal channel made available by the Companies and the related documentation are kept for the time necessary to process the report and in any case no longer than 5 years from the date of communication of the final outcome of the reporting procedure, in compliance

with the confidentiality obligations set out in European and national legislation on the protection of personal data.

More details on the methods of processing are available in the Information on the processing of personal data pursuant to art. 13 and 14 GDPR, made available – in an up-to-date version – directly within the WB platform.

7 Confidentiality in the whistleblowing process

The identity of the whistleblower may not be disclosed to persons other than those competent to receive or follow up on reports. The protection concerns not only the name of the whistleblower but also all the elements of the report from which the identification of the whistleblower can be derived, even indirectly.

The protection of confidentiality is extended to the identity of the persons involved and of the persons named in the report until the conclusion of the proceedings initiated on the basis of the report, in compliance with the same guarantees provided for the reporting person.

The report is exempt from access to administrative documents and the general right of civic access.

Furthermore, Legislative Decree no. 24/2023 expressly provides in art. 12 paragraphs 3 et seq.:

(3) In criminal proceedings, the identity of the reporting person is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure.

(4) In proceedings before the Court of Auditors, the identity of the reporting person may not be revealed until the conclusion of the investigation phase.

(5) In the context of disciplinary proceedings, the identity of the reporting person may not be revealed, where the challenge to the disciplinary charge is based on separate and additional findings with respect to the report, even if consequent to the same. If the complaint is based, in whole or in part, on the report and knowledge of the identity of the reporting person is essential for the defence of the accused, the report will be usable for the purposes of disciplinary proceedings only in the presence of the express consent of the reporting person to the disclosure of his or her identity.

The reporting person shall be notified, by written communication, of the reasons for the disclosure of confidential data, in the case referred to in paragraph 5, second sentence, as well as in internal and external reporting procedures when the disclosure of the identity of the reporting person and of the additional information, from which it is possible to deduce, directly or indirectly, such identity, is also essential for the purposes of defending the person involved.

Any act of management and communication of data and information relating to reports is carried out in strict compliance with the above.

8 The protections provided for by law

Chapter III of Legislative Decree No. 24/2023 regulates the protection measures provided for persons who make reports and for other persons directly or indirectly involved.

It should be noted that it is possible to benefit from the protections provided for by law only in cases where:

a) at the time of reporting or reporting to the judicial or accounting authority or public disclosure, the reporting or complaining person had reasonable grounds to believe that the information about the violations reported, publicly disclosed or reported was true and fell within the objective scope permitted by this Policy;

b) the report or public disclosure was carried out on the basis of the provisions of Chapter II of Legislative Decree no. 24/2023, referred to in paragraph 3.

8.1 Prohibition of retaliation

The entities or persons referred to in Article 3 of Legislative Decree No. 24/2023 may not suffer any retaliation. Specifically, the following subjects are protected from acts of retaliation, discriminatory or otherwise unfair conduct, implemented as a result of the report:

a) the reporting person;

b) "facilitators", i.e. those who assist the reporting person in the reporting process, operating within the same work context;

c) persons in the same working context as the reporting person, linked to the same by a stable emotional or kinship bond within the fourth degree;

d) the reporting person's work colleagues who work in the same work context and who have a habitual and current relationship with the latter;

e) entities owned by the reporting person or for which the same works or operate in the same working context as the reporting person.

The following constitute acts of retaliation, by way of example but not limited to:

- dismissal, suspension or equivalent measures;
- demotion in rank or non-promotion;
- the change of functions, the change of the place of work, the reduction of salary, the modification of working hours;
- suspension of training or any restriction of access to it;
- negative notes of merit or negative references;
- the adoption of disciplinary measures or other sanctions, including financial sanctions;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;

- the failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the worker had a legitimate expectation of such conversion;
- the non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunity and loss of income;
- improper listing on the basis of a formal or informal sectoral or industry agreement, which may result in the person not being able to find employment in the sector or industry in the future;
- the early conclusion or cancellation of the contract for the supply of goods or services;
- the cancellation of a license or permit;
- the request for psychiatric or medical examinations.

Protection against retaliatory acts provides for:

i. ensure that the Whistleblower, even in the event that the report is unfounded, is not subject to any disciplinary action, except in cases of wilful misconduct and/or gross negligence attributable to him or in the other cases provided for by the applicable reference legislation;

ii. take the necessary measures to protect the physical integrity and moral personality of the whistleblower, so that he or she is adequately protected from any form of retaliation, penalization, discrimination or threat;

iii. adopt the necessary measures to ensure the confidentiality of the whistleblower's identity towards third parties (parties not involved in the report management process) (if this is not possible for reasons inherent to the verification activity following the report, the Company will ask the whistleblower for authorization to disclose his/her identity to third parties, except in cases where there is a cause for exclusion of consent).

The protection provided for the whistleblower who reveals his or her identity is also granted to the person who makes an anonymous report or anonymous disclosure in the event that the subject has subsequently been identified and has suffered retaliation as a result of his or her report.

8.2 The protection of the subjects involved in the report

Alleged violators enjoy the same protection of confidentiality as reports until the full reporting management cycle is completed.

They are also protected from negative repercussions deriving from the report in the event that the reporting procedure does not reveal elements that justify the adoption of measures against them.

In the event of measures being taken against the person responsible for the violation, he must be protected from any negative effects other than those envisaged by the measures adopted.

8.2.1 What to do in the presence of retaliatory acts deemed attributable to a report

The management of retaliatory communications in the public and private sectors is the responsibility of ANAC (https://www.anticorruzione.it) which may avail itself, as far as its respective competences are concerned, of the collaboration of the National Labour Inspectorate.

8.2.2 The declaration of nullity of retaliatory acts is the responsibility of the judicial authority.

ANAC must ascertain that the conduct (act or omission) deemed retaliatory is consequent to the report, complaint or disclosure. Once the whistleblower proves that he or she has made a report in accordance with the law and that he or she has been the victim of retaliatory behaviour, the burden of proof is on the employer to prove that such behaviour is in no way related to the report [reversal of the burden of proof].

Since it is a presumption of liability, it is necessary that evidence to the contrary emerges in the cross-examination before ANAC. To this end, it is essential that the alleged perpetrator provides all the elements from which to infer the absence of the retaliatory nature of the measure adopted against the whistleblower.

8.2.3 Loss of protection

Protections are not guaranteed when the criminal liability of the reporting person for the crimes of defamation or slander or in any case for the same crimes committed with the report to the judicial or accounting authority or his civil liability, for the same reason, in cases of intent or gross negligence is ascertained, even with a first instance judgment; In such cases, a disciplinary sanction may be imposed on the reporting or reporting person.

8.3 Support measures

Legislative Decree no. 24/2023 provides for support measures consisting of information, assistance and advice free of charge on the methods of reporting and the protection from retaliation offered by national and European Union regulatory provisions, on the rights of the person concerned, as well as on the methods and conditions of access to legal aid.

The list of Third Sector entities that provide reporting persons with support measures is established at ANAC. The list, published by ANAC on its website, contains the Third Sector entities that exercise, according to the provisions of their respective statutes, the activities referred to in Legislative Decree no. 117 of 3 July 2017, and that have entered into agreements with ANAC.

9 The sanctioning system

Violation of the provisions of this policy regarding confidentiality and protection of the whistleblower and the other subjects identified above will result in a disciplinary or contractual offence.

The disciplinary systems, provided for by Muviq Srl, set forth specific procedures for the imposition of sanctions against those who violate the protection measures of the whistleblower and other protected subjects, separately in the following cases:

a) of a person belonging to the organization of Muviq Srl, due to the related Disciplinary Regulations defined in accordance with the applicable CCNL and the Workers' Statute;

b) of subjects external to the organization of Muviq Srl, due to the contractual collaboration/supply agreements signed for various reasons.

The aforementioned disciplinary/contractual sanctions are cumulative with the administrative fines set out below applied directly by ANAC, against those who are ascertained to be responsible for the violations indicated by the legislation:

a) from 10,000 to 50,000 euros when it ascertains that retaliation has been committed or when it ascertains that the report has been obstructed (even if only attempted to obstruct it) or that the obligation of confidentiality has been violated;
b) from 10,000 to 50,000 euros when it ascertains that no reporting channels have been established or are not compliant;
c) from 500 to 2,500 euros for false reports if the responsibility of the whistleblower is ascertained in cases of intent or gross negligence.

This is without prejudice to any other liability profiles.

10 Formation

Muviq Srl ensures that appropriate information and training is carried out on its internal reporting channel.

The information and training activity falls within the scope of compulsory training that must be provided at least at any change in external legislation, this policy as well as the WB platform adopted by Muviq Srl.

Muviq Srl also ensures specific training for the SB and the Chairman of the Company as well as for all those called upon to carry out the role of person in charge pursuant to what is defined in this policy.

ANNEX 1

Non-regular State aid	Management of loans, subsidies and contributions from the public in a manner that does not comply with the regulations in force on the so-called "Loans and Contributions". "State aid"
Environment and public health	Irregularities in the management of environmental protection and danger to hygiene and public health
Procurement, Procurement, Irregular Work	Irregularities found in the procurement process of goods and services and in the awarding and conduct of contracts. Irregular work management
Unfair competition and disruption of the commercial activity of others	Actions aimed at altering fair competitiveness on the markets and obtaining a competitive advantage to the detriment of third parties, achieved or attempted through irregular or unlawful methods
Conflict of interest	Situations of incompatibility or conflict due to the presence of a potential conflict between the individual interest and the interest of the Entity
Corruption, subornation, bribery	Acts of corruption against public or private entities aimed at obtaining benefits for the Entity or individuals to the detriment of third parties, carried out or attempted through irregular or illicit methods
Crime, Illicit trafficking (including international trafficking), Terrorist financing	Any conduct not listed separately in this table, which is contrary to the national and EU regulations in force, carried out individually or in groups
Copyright, Intellectual or Industrial Property, Patents	Irregular or unlawful use of goods, works and information subject to copyright and/or intellectual/industrial property, to the detriment of legitimate owners and right holders
Diversity, Equity, Inclusion	Any conduct carried out in violation of the rights of the person, such as - by way of example - the rights to equality, dignity, fair pay and equal treatment free of any form of discrimination related to gender, colour, race, language or religion, freedom of opinion and the full development of the human personality.
Work-life balance, Welfare	Labour exploitation, non-compliance with workers' rights and incorrect practices in the management of corporate welfare
Theft or Fraud to the detriment of the Company or Third Parties	Any action aimed at achieving the interests or advantages of the Entity or individuals through unlawful conduct
Personnel Administration, Salary Compensation	Systematic irregularities in the administrative management of personnel and non-compliance with the provisions of the CCNL and/or the Workers' Statute
Privacy and Protection of Personal Data	Critical issues related to the protection of personal data and privacy or violations found in this area
Public Administration or Judicial Authority	Conduct aimed at providing the Public Administration or the Judicial Authority with an untrue, altered or falsified representation of what is required or due for compliance
Tax crimes, Receiving stolen goods, Money laundering, Financial crimes, Corporate crimes, Financial statements	Irregular conduct aimed at altering the fiscal, financial, administrative position and the correct preparation of the financial statements.

Health and safety in the workplace	Irregularities in the management of the protection and prevention of health and safety in the workplace or situations of danger to the safety of people
Cybersecurity and business continuity	Critical issues related to the use of information systems with the danger of potential breaches for the security and continuity of systems, applications and data
Violence, harassment, mobbing or other abuse in the workplace	Any practice of vexatious, aggressive, persecutory or discriminatory practices carried out by anyone in the workplace against a worker Any conduct (physical, verbal or even merely allusive) that harms the dignity of the person in the workplace, even in cases where it is carried out without apparent blackmail purposes related to the work environment. Such conduct includes - but not necessarily - pushed advances, humiliating phrases, sexual jokes, groping, physical and verbal aggression.
Conduct that does not comply with company rules that does not constitute a crime	Failure to comply with the rules defined internally by the Authority for the regular and integral functioning of its administration. These include the certified management policies and systems activated by the Authority, governed by procedures, service provisions, circulars and internal operating instructions.
Other	Failure to comply with the principles of conduct provided for by the Code of Ethics adopted by the Entity, where not already included in the cases analytically described in the table.

MUVIQ Srl
Stradale Torino 603 – Frazione San Bernardo d'Ivrea
10015 Ivrea (TO)
Cf: 12849500017 REA TO-1320586

ANNEX 2

1 Choose the reporting mode

In this section, the Whistleblower can decide whether to opt for anonymity or for the willingness to qualify by communicating some personal data. In any case, the Whistleblower is guaranteed confidentiality and the related protections. Any indication of the identification details will allow better interaction and will – in any case – be ensured the utmost confidentiality and protection to the whistleblower.

2. Your relationship with society*

Indicate what your current relationship with the Company is

3. What is the nature of your concern*

Select the most appropriate reference area for your report. [In this regard, cf. **Annex 1**]

4. Who is your report about

Indicate the persons involved in the offence Add all relevant information: a) persons involved who may have committed the act [in case you wish to provide the name of the natural person who committed the act or conduct, please be informed that this person will not be contacted until it is reasonably certain that what you have reported has actually happened and that it has been committed by the person reported] b) persons involved who may be damaged by the fact [if it is a natural person, do you think - in your opinion - that we can contact them to request further information, without affecting the confidentiality of the verification of the report? If you think it is possible, please indicate their contact number] c) persons who may benefit from the fact d) any other parties involved (explaining the reasons).

5. What happened?

Provide a description that is as concrete, detailed and accurate as possible (generic reports without elements on which to activate concrete investigations cannot be investigated in depth and will be archived)

6. Where did the irregularity or offence occur?

Enter as detailed a location as possible, e.g. place of work, room, department

7. When did the offence occur?

Indicate when the fact you are reporting happened: past, present, future, in progress, or a specific day and time.

8. Economic dimension

If your report also concerns economic aspects, are you able to give a dimension of the value expressed in the currency of your country?

9. Upload file

Attach supporting documentation where available and supporting the report. WARNING: Make sure that attachments do not contain any user data that could reveal your identity

10. Have you taken any other actions in relation to this case?

For example, have you talked about it with someone else or reported it elsewhere? If yes, describe the action here

11. Information on the processing of personal data and consent*