Whistleblowing procedure

TABLE OF CONTENTS

STATUS OF REVIEWS

Rev.	Date	Description of modifications	Drafted by	Verified and approved by
1.0	[to be completed]	First draft	[to be completed]	[to be completed]

1. LEGAL FRAMEWORK

This procedure (hereinafter "**Procedure**") covers the procedures for receiving and handling reports of wrongdoing in the corporate sphere regarding whistleblowing (that is the institution established to protect the individual who reports breaches of which it becomes aware in the work context).
Furthermore, Medical Microinstruments, Inc. (hereinafter "**Company**") undertakes to comply with the applicable legislation prescribed by the European Union and national legislators regarding (i) the protection of persons who report breaches of Union and national law and (ii) the protection of individuals with regard to the processing of personal data and the free movement of such data.
The Company also undertakes to comply with all other provisions adopted by the competent authorities aimed at providing guidance and principles for the proper performance of the established obligations (hereinafter collectively referred to as "**Applicable Legislation**").

2. THE WHISTLEBLOWER

The whistleblower (hereinafter referred to as "**Whistleblower**") is the person who makes a report (hereinafter referred to as "**Report**") on the breaches acquired in the work context, thereby exposing himself/herself to the risk of retaliation, understood as any act, measure, conduct or omission, even if only attempted or threatened, that causes or is likely to cause, directly or indirectly, unjustified harm to the person/entity.
These Reports represent an effective widespread control solution that provides an internal protection mechanism within the Company, indirectly creating a self-sustaining compliance system.
For such Reports to be encouraged, it is necessary for the Whistleblower to be "protected" from retaliation, for example, by being able to benefit from the protection of confidentiality about his or her identity.

3. PURPOSE

The Procedure sets the manner in which Reports are received and handled, with the overall objective of protecting the Whistleblower by limiting, as much as possible, the presence of factors that may discourage the use of the institution of whistleblowing.
Specifically, it is deemed proper to provide the Whistleblower with all operational indications about the subject, content, recipients, and mode of transmission of Reports, taking care to indicate the protections that the Applicable Legislation makes available to him/her.

Further objectives of the Procedure can be summarized as to define and formalize:

- The reporting procedure by establishing terms, roles and responsibilities;
- The rules that need to be observed in order to ensure the confidentiality of the identity of the Whistleblower, the person involved, and the person mentioned in the Report, as well as the content of the Report and related documentation;
- The duties of the managing party of the internal reporting channels (hereinafter "**Handler**").

4. INDIVIDUALS WHO CAN MAKE REPORTS

Reports may be made by:

- Employees, including trainees and those in part-time, intermittent, fixed-term, temporary, contract, casual or occasional employment relationships with the Company;
- Collaborators of the Company in various capacities, such as: independent contractors, partners (e.g., attorneys), freelancers and consultants who work for the Company;
- Volunteers and interns (paid and unpaid) who perform their activities for the Company;
- Shareholders (individuals) of the Company;
- Members of management and supervisory bodies.

If a Report is submitted, the protection of the confidentiality of the identity of the Whistleblower and of the person reported (hereafter "**Person Concerned**") or otherwise mentioned in the Report, as well as of the content of the Report and its documentation, is guaranteed to all the aforementioned persons from the moment of receipt and in any subsequent contact. However, the protection of the confidentiality of identity is not to be understood as anonymity: indeed, in order to benefit from the protection offered by the Applicable Legislation, the Whistleblower must identify itself.

5. SUBJECT OF THE REPORT

The Whistleblower may Report any unlawful conduct that has come to his/her attention as a result of his/her relationship with the Company, regardless of whether the reported breach occurred during, before or after the establishment of the legal relationship: in fact, the Report may be submitted during the selection process, during the probationary period or after the termination of the employment relationship. The Report must be based on factual information related to the Company.

Subject of the Report may be all behaviors, acts or omissions consisting of:

1. Breaches of European Union law using all available reporting channels (internal and external channels, public disclosure, reporting to judicial authorities):
    a. Offenses falling within the scope of EU acts related to the following areas: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; protection of the environment; radiation protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; protection of privacy and personal data; security of network and information systems;
    b. Acts or omissions that harm the financial interests of the EU, such as fraud, corruption, and any other illegal activities related to Union expenditures;
    c. Acts or omissions relating to the EU internal market, including any mechanism designed to obtain a tax advantage that nullifies the object or purpose of the applicable corporate tax law;
    d. Acts or conducts that frustrate the object or purpose of the EU provisions set forth above.
2. Breaches of national law, reportable through internal channels only:
    a. Prerequisite offenses for the application of national law (in Italy, Italian Legislative Decree No. 231 of June 8, 2001), included but not limited to: receiving undue disbursements, committing fraud against the State, a public entity, or the European Union, or obtaining public disbursements, computer fraud against the State or a public entity, and fraud in public procurement, embezzlement, extortion, undue inducement to give or promise benefits, bribery and abuse of office, etc.;
    b. Breach of internal regulations adopted by the Company (in Italy, the so-called *Modello di Organizzazione e Gestione* – Organization, Management and Control Model, hereinafter "**MOG**") – adopted in compliance with the Italian Legislative Decree No. 231 of June 8, 2001, as amended).

The Report may also contain information (including well-founded suspicions) about conducts aimed at concealing the above-mentioned breaches, information about illegal activities that have not yet been carried out, but which the Whistleblower reasonably believes may occur on the basis

of concrete elements (including irregularities and anomalies) or on the basis of the existence of concrete, precise and consistent elements. However, Reports based on mere suspicions or rumors are not worthy of protection.

In any case, the following may not be the subject of Reports:

- Facts related to a personal interest of the Whistleblower or pertaining exclusively to his or her individual employment relationships (including in relation to hierarchically superior figures);
- Facts related to breaches already compulsorily regulated in certain special sectors, to which a specific reporting discipline continues to apply (such as financial services, products and markets, prevention of money laundering, prevention of terrorism financing, transport safety, environmental protection, etc.);
- Facts concerning national security and defense.

6. CONTENT OF THE REPORT

The Whistleblower must provide all relevant elements so that the Handlers can proceed with the investigations aimed at verifying the validity of the facts brought to his attention.

To this end, the Report must contain the following elements:

a) Identity and contact details of the Whistleblower;
b) Clear and complete description of the facts that are the subject of the Report;
c) The circumstances of time and place in which the facts were committed;
d) The personal details or other elements that enable identification of the person(s) affected by the reported facts.

Additionally, if available, the following information may also be indicated:

- The particulars of other informed persons who can give details of the facts that are the subject of the Report;
- Documents that can confirm the substantiation of such facts;
- Any other data that may serve to provide useful feedback about the existence of the reported facts.

7. ANONYMOUS REPORTS

Anonymous reports are considered to be those that do not contain elements that allow their

author to be identified; by virtue of the Applicable Legislation, they do not fall within the scope of implementation of the Procedure and are therefore treated in the same way as ordinary reports.

The Handlers must also record anonymous reports, which are retained with all related documentation attached. The Handlers shall therefore ensure that:

- the Whistleblower who has identified himself/herself later, and
- who has notified the territorially competent anti-corruption authority (hereafter, "**Authority**") after having suffered retaliatory measures due to the Report,

has the protections offered by the Applicable Legislation.

Such Reports, which in principle are not allowed, may however be subject to subsequent verification only if they relate to facts of particular gravity and with a content that is adequately detailed and circumstantiated.

In such cases, the protection typical of the institution of whistleblowing will be guaranteed only in the case of Reports made by clearly identifiable and/or correctly identified individuals.

8. SAFEGUARDS PROVIDED

The Applicable Legislation provides the following protection measures:

1. **Protecting the confidentiality of the Whistleblower's identity**

   The identity of the Whistleblower, as well as any other information from which it may be inferred (directly or indirectly), may not be disclosed to persons other than the Handlers without the Whistleblower's express consent; this principle, in the context of any proceedings instituted as a consequence of the Report, is declined as follows:

   a. In criminal proceedings, the identity of the Whistleblower must be kept confidential until the accused is informed of it, and in any case, no later than the end of the preliminary investigation;

   b. Within the scope of disciplinary proceedings, the identity of the Whistleblower may not be disclosed, where the contestation of the relevant charge is based on separated investigations and additional to the Report (even if consequent to it). If the charge is based, in whole or in part, on the Report and knowledge of the identity of the Whistleblower is essential for the defense of the accused, the Whistleblower's Report will be usable for the purposes of disciplinary proceedings only if the Whistleblower expressly consents to the disclosure of his/her identity.

1.1. Protection of the confidentiality of the identity of other parties

It is also protected the confidentiality of the identity:

a. Of the Person Concerned;
b. Of the facilitator, i.e., the person who assists the Whistleblower in the reporting process and who operates within the same work context (confidentiality must be guaranteed both with regard to identity and with reference to the activity in which the assistance takes place);
c. Of persons different from the Person Concerned but mentioned in the Report (e.g., witnesses).

2. Protection from retaliation

Retaliation may consist of: suspension, lay-off, dismissal or equivalent measures; demotion or withholding of promotion; transfer of duties, change of location of place of work, reduction in wages, change in working hours; withholding of training; a negative performance assessment or employment reference; imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty; coercion, intimidation, harassment or ostracism; discrimination, disadvantageous or unfair treatment; failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment; failure to renew, or early termination of, a temporary employment contract; harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income; blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry; early termination or cancellation of a contract for goods or services; cancellation of a license or permit; request for submission to psychiatric or medical examinations.

The above list of retaliatory measures is not exhaustive: in fact, “retaliation” should be considered all those instances that directly or indirectly cause or are likely to cause unfair harm to the person.

Individuals who are protected from possible retaliation, even if only attempted or threatened, include:

a. Whistleblower;
b. Facilitators;
c. Persons in the same work environment with stable emotional or kinship ties within the

fourth degree with the Whistleblower;

d. Colleagues working in the same work context who have a regular and current relationship with the Whistleblower;
e. Entities owned or operating in the same work context as the Whistleblower or in which the latter works.

To be protected from retaliation, the following conditions must be met:

- The Whistleblower reported based on the reasonable belief that the information about the breaches was true and within the range of the reportable ones, as clarified in paragraph "**5. SUBJECT OF THE REPORT**"; and
- The Report was made in compliance with the discipline provided within the Procedure; and
- There is a cause-and-effect relationship between the Report made and the retaliation suffered; the burden of proof on the causal relationship shifts depending on the person who complains of retaliation and/or harm: if the Whistleblower proves that the Report was made and that retaliation was suffered as a result, the burden shifts to the person who perpetrated the alleged retaliation; conversely, the burden of proof shifts to all other persons, other than the Whistleblower, who enjoy the protections against retaliation listed above.

3. Limitations of liability with respect to disclosure and dissemination of some categories of information.

In addition to the protections listed, Whistleblowers are also safeguarded by limited liability for disclosing certain categories of information. These categories include information covered by official, professional, scientific, and industrial secrecy, as well as information that, if revealed, would violate copyright or personal data protection laws, or damage a person's reputation.

For this protection to operate, two conditions must be met:

- At the time of the disclosure or dissemination of the information, the Whistleblower has reasonable grounds to believe that it is necessary to disclose the breach; and
- The Report was made in compliance with the discipline set forth in the Procedure and Applicable Legislation.

9. INTERNAL REPORTING CHANNELS

The Company has implemented the internal channels listed below, from which the Whistleblower

is free to choose.

- Written communication: The Company has opted for the use of an IT platform to receive and manage Reports (hereinafter the "**Platform**"), which, by means of a questionnaire, guides the Whistleblower in the filling in of all the information that must be provided, with the possibility to attach any document and to remove metadata from them, in order to guarantee (through the use of encryption tools) the confidentiality of the identity of the Whistleblower, the Person Concerned and the persons in any case mentioned in the Report, as well as the content of the same and of the related documentation, thus resulting in compliance with the provisions of the Applicable Legislation;
- Oral communication: through the Platform it is also feasible to send an oral Report by recording a voice message, with the possibility of distorting the recorded voice and deleting the metadata of the record, in order to ensure the confidentiality of the identity of those involved in the Report, as explained in the previous point;
- Oral communication in person: by meeting directly with the Handlers (at the request of the Whistleblower), who ensures that the meeting can be held within a reasonable time.

In any case, once the Report has been sent (in any mode), the Whistleblower will receive a password automatically generated by the Platform, which he/she will need to access later in order to follow the case, see any updates and, if necessary, communicate with the Handler.

When submitting the Report, the Whistleblower can choose which Handler will receive and manage it; this is a feature designed to avoid conflicts of interest: in fact, by being able to choose who to entrust the Report to, a different party can be chosen if a Handler is involved.

10. HANDLERS OF INTERNAL REPORTING CHANNELS

Management of internal reporting channels is entrusted to the Company's HR & Legal Office.

The Company ensures that its appointed Handlers meet all the requirements of the Applicable Legislation; in particular, the Company has:

- Assessed that these are profiles endowed with autonomy;
- Expressly appointed the relevant members of the HR & Legal Office as individuals authorized to process personal data, giving specific instructions regarding the processing that can be carried out;
- Delivered specific training on whistleblowing and personal data protection.

11. REPORT MANAGEMENT

Upon receipt of the Report through the relevant internal channels, the Handlers must:

1. **Release acknowledgement to the Whistleblower within seven (7) calendar days from the date of receipt of the Report**; acknowledgment of receipt does not imply evaluation of the contents submitted. It is solely to inform the Whistleblower that the submission has been received correctly. The notification shall be sent to the contact details provided by the Whistleblower at the time of submission of the Report.
2. **Maintain communication with the Whistleblower** to request any necessary additional information in order to properly handle the Report.
3. **Diligently follow up on the Report,** i.e., assess processability, admissibility and merits; specifically:
    a. In terms of processability, the Handlers verify the existence of the subjective and objective prerequisites provided for in the Applicable Legislation, in order to ascertain that the Whistleblower falls within the scope of the subjects entitled to make the Report (see paragraph "**4. INDIVIDUALS WHO CAN MAKE REPORTS**") and that the related subject falls within the scope of the Applicable Legislation (see paragraph "**5. SUBJECT OF THE REPORT**"). If the Report does not fall within the scope of application, it may be treated as ordinary.

    For the purpose of admissibility, however, it will be necessary for the Report to contain all the required elements, as outlined in paragraph "**6. CONTENT OF THE REPORT**".

    A Report is deemed inadmissible when:

    - Factual elements attributable to the reportable breaches are missing or manifestly unfounded;
    - The statement of facts is generic and does not allow understanding of what happened and/or identification of the person to whom the violation is attributed;
    - Only documentation is produced without an actual Report being made.

    If the Report is found to be improper or inadmissible, the Handlers proceed with the filing, recording the reasons supporting the choice made.

    b. After confirming the admissibility of the Report, the Handlers will proceed to verify its merits by carrying out all appropriate activities, including personal interviews

with the Whistleblower and any other persons who can provide information on the reported facts, in accordance with the principles of impartiality and confidentiality. The goal is to analyze and evaluate reported facts to determine whether corrective actions are necessary to improve the internal control system for the business areas and processes involved.

At this step, the Handlers may rely on the support and cooperation of the relevant Company's structures and, if necessary, external parties (e.g., experts, consultants, etc.), always protecting the confidentiality of the identity of the Whistleblower, the Person Concerned, as well as the content of the Report and related documentation.

4. **Provide acknowledgement to the Whistleblower within three (3) months from the date of the acknowledgement of receipt** or, if such an acknowledgement has not been issued due to lack of knowledge of the identity and/or contact details of the Whistleblower or if there are other obstructive causes, within three (3) months from the expiration of the 7-day period provided for issuing the acknowledgement of receipt of the Report. The assessment activity does not necessarily have to close within three (3) months: in fact, the completion of the checks may take longer; therefore, after this period has elapsed, the Handlers may notify the Whistleblower:
   - The dismissal;
   - The initiation of an internal investigation and its findings;
   - The steps taken to address the reported facts;
   - Information regarding the activities to be undertaken and the progress of the investigation (in the latter case, once the activity is completed, it must also communicate the results to the Whistleblower).

   If at the outcome of the verification the Report proves to be well-founded, the Handlers will forward it to those responsible for assessing any responsibility profiles, pursuant to the disciplinary system adopted by the Company.

12. REPORT SENT TO PARTY OTHER THAN THE HANDLERS

If the Report is submitted to an entity other than the Handlers and the Whistleblower explicitly states that it wishes to benefit from the protection offered by the Applicable Legislation (or this intention can be inferred from the Report), the non-competent entity receiving the Report must forward it to the Handlers within seven (7) days of its receipt, without sending copies to any other

entity, and at the same time inform the Whistleblower. The operation must be carried out while maintaining the confidentiality of the identities of the Person Concerned and of any other person mentioned in the Report, as well as of the contents of the latter and its supporting documents.

13. EXTERNAL REPORTING CHANNELS

Provision is made for the possibility of submitting a Report through external channels, limited to breaches of the provisions of the law of the EU, as set out in paragraph "**5. SUBJECT OF THE REPORT**"; the Authority (which is in charge of the management of these channels) guarantees the confidentiality of the identity of the Whistleblower, of the Person Concerned and of the person mentioned in the Report, as well as of the content of the latter and of the related documentation, including through the use of encryption tools.

Access to external channels is only allowed when one of the following conditions is met:

1. Internal channels are not active or do not comply with the Applicable Legislation;
2. The internal Report produced has not been followed up;
3. The Whistleblower believes that an internal Report will not be effectively followed up or may result in a risk of retaliation;
4. The Whistleblower has reasonable grounds to believe that the breach may pose an imminent or obvious danger to the public interest.

The Authority acquires external Report through the channels specifically set up[1]:

- IT platform;
- Oral telephone communications;
- Oral communications in person (face-to-face meetings set within a reasonable time).

The Authority's platform enables the compilation, sending, and receiving of the Report form, the management of the investigation, and the possible forwarding to other competent authorities; this tool uses encryption mechanisms that guarantee the technological security of the Report process, while at the same time maintaining the confidentiality of all the data contained therein. The Whistleblower's data is obscured and segregated in a special section of the platform, making it inaccessible even to the Authority's investigating office. The platform assigns a unique progressive code to each received Report. The Whistleblower can freely access the relevant section of the platform (via the Authority's website) without prior authentication; in this section, the Report form

[1] The channels described below are those adopted by the Italian Authority, exemplifying for the purposes of this Procedure the external channels; different channels may be provided in other nations. In case of doubts, it is recommended to contact the Handlers.

to be filled in and submitted is displayed. The Report form includes a section titled “Identity” (or a similar title) that must be completed in order to sign it. As anticipated, the data entered in this section is encrypted and therefore not accessible to those who will carry out the investigation.
The Authority has established a telephone service with an operator to facilitate the acquisition of oral communication. The operator receives the Report by phone and enters it on the platform along with the corresponding audio file of the call recording. At the end of entering the Report, the user should receive a unique alphanumeric identification code (key code) from the platform, which it should communicate orally to the Whistleblower during the telephone call.
The Authority's latest tool allows for direct acquisition of the Report through an operator who enters the data into the IT platform, similar to the process for oral communication.

14. PUBLIC DISCLOSURE

Another way to Report breaches of EU law, as outlined in paragraph “**5. SUBJECT OF THE REPORT**”, is through public disclosure. This involves making public information about the breaches through press, electronic media, or other means capable of reaching a large audience.
The conditions for making a public disclosure are as follows:

- The Whistleblower previously submitted an internal Report to the Company but did not receive a response within the required timeframe. As a result, the Whistleblower submitted an external Report to the Authority (or directly to the Authority) but has not received a response within a reasonable timeframe;
- The Whistleblower believes that the breach poses an imminent or obvious danger to the public interest;
- The Whistleblower believes that the external Report may involve a risk of retaliation or may not be effectively followed up due to the specific circumstances of the particular case (e.g., evidence may be concealed or destroyed, or there is a well-founded fear that the Handler may plot with the reported person or be involved in the breach).

15. COMPLAINT TO THE JUDICIAL AUTHORITY

Individuals protected by the Applicable Legislation, as defined in paragraph “**8. SAFEGUARDS PROVIDED**”, section “**Protection from retaliation**”, may file a complaint with the competent judicial authorities, regarding a breach of EU law (as defined in paragraph “**5. SUBJECT OF THE REPORT**”) of which they have become aware in the course of their work. The offices of the judicial

authorities, to which the complaint is made, must also adhere to the aforementioned rules on confidentiality protection.

16. DATA PROTECTION COMPLIANCE

The Company is committed to complying with and implementing the obligations set forth in the applicable data protection regulations: therefore, it has taken steps to supplement its privacy documentation system as follows (with respect to the processing carried out in the context of the management of Reports):

- A specific privacy notice has been prepared for all data subjects so that they are aware of the purposes and means of processing their personal data; this notice is published on the Platform implemented for the management of Reports.
- The Company has updated the record of processing activities;
- The Handlers have been expressly appointed as the persons authorized to process personal data.

If the Handlers need the assistance of other parties, whether internal or external, to manage the Reports and are unable to keep the information confidential, the Company must designate those parties as persons authorized to process personal data (in internal parties) or data processor (if external parties), in compliance with applicable data protection regulation. To ensure proper performance of their assigned roles, all individuals mentioned have received adequate training on data protection regulations and obligations related to whistleblowing. They are also required to sign a confidentiality agreement to safeguard any information they may come across while performing their duties.

17. PENALTIES

Non-compliance with the Procedure may result in disciplinary sanctions, as outlined in the MOG. Pursuant to Applicable Legislation, the Authority may impose an administrative fine of 10,000 to 50,000 euros on:

- The natural person who: (i) has committed retaliation, (ii) obstructs, or attempts to obstruct, the Report, or (iii) has violated the obligation of confidentiality of the identity of the Whistleblower; on this subject it should be noted that the penalties applicable by the territorially competent data protection supervisory authority for the profiles of competence remain unaffected;

- The Handlers, in case of failure to carry out the verification and analysis activities of the Reports received;
- The Company's governing body, if (i) internal reporting channels are not established, (ii) a procedure for making and handling Reports has not been adopted, or has been adopted but does not comply with the provisions of the Applicable Legislation;
- The person who, as a result of the inspections, is found to be guilty of the facts that are the subject of the Report or otherwise of established breaches.

The Authority may impose an administrative fine of 500 to 2,500 euros on the Whistleblower who makes with willful misconduct or gross negligence Reports that turn out to be unfounded. On the subject, it is noted that the criminal and disciplinary liability of the same is left unaffected in the event of slanderous or defamatory Report under current civil and criminal law.

Lastly, if at the outcome of the verifications carried out as a result of the Report, substantiating elements have been found regarding the commission of an illegal act by an employee, the Company may file a complaint with the territorially competent judicial authorities. Similarly, if the findings of the verifications carried out have revealed unlawful behavior by a third party (e.g., a supplier), the Company may proceed with suspension/deletion from the Company registers, without prejudice to any further powers provided for by law and by contract.

18. COMPANY'S ACTIVITIES

The Company shall provide all internal personnel with specific communications and information regarding the institution of whistleblowing, the Procedure and any other relevant information deemed useful to inform and raise awareness of the purposes of this institution, the protections offered and the procedures for submitting and handling Reports.

19. UPDATES OF THIS PROCEDURE

The HR & Legal Office is responsible for updating the Procedure and reviews it on a periodic basis, at least annually. In any case, the HR & Legal Office is available for clarification.

In the event of modifications to the Procedure, the Company will make the new version available again in a manner that reaches the people involved in the most effective and efficient manner.