

COMPAGNUCCI HIGH TECH

WHISTLEBLOWING MANAGEMENT PROCEDURE

SUMMARY

Contents

Part I – GENERAL.....	
1. Nomative References	
2. Objective	
3. Scope of application	
4. Principles	
5. Definition	
Part II – WHISTLEBLOWING PROCESS.....	
6. Roles and responsibilities	
7. Reports	
8. Whistleblower	
9. Whistleblowing Channels	
10. Whistleblowing Management	
a. <i>Receipt of reports</i>	
b. <i>Evaluation of the Admissibility of the Report received</i>	
c. <i>Investigation</i>	
d. <i>Closure</i>	
11. Prohibition of Retaliation	
Part III - FINAL PROVISIONS	
12. The Protection of Confidentiality	
13. Continuous Improvement Process	
14. Archiving and Traceability of Documentation	
15. Information and Communication	
16. Disciplinary Measures	
17. Rules and Privacy	

Compagnucci High Tech Srl	
Whistleblowing Management Procedure	Date: 11.12.2023
Authorized by: CEO	Revision: v.01

Part I - GENERAL

1. Normative References

The main regulatory framework and other relevant references that form the basis of this procedure and related processes are listed below:

- EU Directive no. 1937/2019 on the protection of persons who report breaches of Union law and its local transpositions;
- Legislative Decree no. 24/2023 "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws."
- international ISO 37002 "Whistleblowing management systems;
- EU Regulation no. 679/2016 "General Data Protection Regulation - GDPR" and its local transpositions;
- The Company's Code of Ethics.

2. Objective

Compagnucci High Tech S.r.l (hereinafter also referred to as the "Compagnucci High Tech" or the "Company"), in adherence to its values, the behavioral principles defined in its Code of Ethics and its commitment to respect and comply with current regulations, adopts the following procedure for the management of whistleblowing and appropriate internal whistleblowing channels so that all persons acting on behalf of the Company may have an all-inclusive tool through which to convey reports of breaches of the Code of Ethics and Legislative Decree 24/2023.

The purpose of this document is to describe the stages of receiving, evaluating, analyzing, and managing reports by defining the roles and responsibilities in the process, the subject of reports, the individuals entitled to make reports, and the management process that the Whistleblower and the Company are required to follow and comply with.

3. Scope of application

This procedure applies to Compagnucci High Tech including all entities under Legislative Decree 24/2023, i.e. those who work in the name of and on behalf of the Company such as directors, executives, permanent and even temporary employees or those who perform occasional services, contracted workers, volunteers and interns, shareholders, as well as Third Parties (such as self-employed workers, freelancers and consultants).

Compagnucci High Tech is also committed to extending the scope of application to recipients of the Company's Code of Ethics, such as customers, suppliers and partners who collaborate with the Company and who may in turn make reports regarding possible breaches.

4. Principles

The parties involved in the activities governed by this procedure must operate in compliance with the regulatory, organizational and power system and the principles set forth below:

Confidentiality

Omissis

Transparency

Omissis

Autonomy, Impartiality, Independence and Professionalism

Omissis

Truthfulness and reasonableness

Omissis

Prohibition of retaliation to protect whistleblowers and other parties involved

Omissis

5. Definitions

<i>Compagnucci High Tech S.r.l.</i>	The Company subject to the procedure
<i>Breaches under Art. 2 Legislative Decree 24/2023</i>	<p>Harmful conduct, acts or omissions that harm the public interest or integrity of a public administration or private entity and that consist of:</p> <ul style="list-style-type: none"> - offenses that fall within the scope of the European Union acts listed in Annex 1 to the Decree and all national provisions implementing them, even if not listed in the Annex to the Decree; - acts or omissions detrimental to the financial interests of the Union referred to in Article 325 of the Treaty on the Functioning of the European Union ("fight against fraud and other activities detrimental to financial interests") specified in the relevant European Union secondary legislation; - acts or omissions concerning the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including breaches of EU competition and state aid rules, as well as breaches concerning the internal market related to acts that breach corporate tax rules or mechanisms whose purpose is to

	<p>obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;</p> <ul style="list-style-type: none"> - Acts or conduct that frustrate the object or purpose of the provisions set forth in Union Acts in the areas indicated in the preceding paragraphs.
<i>Other breaches</i>	Conduct, deeds or omissions detrimental to the Company that, by way of example but not limited to, consist of breaches, or inducement to breach laws and/or regulations, the behavioral principles enshrined in the Code of Ethics, as well as in company policies and/or rules (e.g., procedures, internal circulars, service orders).
<i>Reporting Party/Whistleblower</i>	The person who reports breaches occurring within his or her work context.
<i>Third parties</i>	<ul style="list-style-type: none"> - Self-employed and contracted workers, contractors, freelancers, consultants; - Persons not yet hired who became aware of breaches during the selection process; - Former employees or partners of the Company who became aware of breaches while still holding relations with the Company.
<i>Report</i>	Communication, made in written or oral form or by meeting, regarding the breach.
<i>Person of interest</i>	The natural or legal person named in the Report as the person to whom the breach is attributable or as a person otherwise involved.
<i>Facilitator</i>	The natural person who assists the Whistleblower, if any, in the Reporting process and who may operate either inside or outside the work environment and whose assistance must be kept confidential. By way of example only, this could be the channel manager, line manager, a colleague or third party, or any other figure inside or outside the organization. In fact, the Facilitator enjoys the same protections as the Whistleblower governed in paragraph "11. Protection of confidentiality."
<i>Retaliation</i>	Any conduct, act or omission, even if only attempted or threatened, committed as a result of the Whistleblowing that causes, or may cause, the Reporting Party, directly or indirectly, unfair harm.
<i>Whistleblowing Channel Manager</i>	Figure that assumes the role of Channel Manager ex art. 4 par. 2 Legislative Decree 24/2023, identified as a person from outside the Company who meets the requirements of the regulations.

<i>Digital Platform</i>	IT tool to support the process that enables secure and anonymous communication between the Whistleblower and the Whistleblowing Channel Manager
<i>External Consultant</i>	Specialized professional offering advice and support to the Company in preparatory activities for the management of whistleblowing reports.
<i>Time Terms</i>	Where time terms are expressed in numbers of days, they are understood to mean calendar days.

Part II - WHISTLEBLOWING PROCESS

6. Roles and Responsibilities

Omissis

7. Whistleblowing Reports

Breaches under Art. 2 of Legislative Decree 24/2023:

- 1) Offenses that fall within the scope of the European Union or national acts specified in the Annex to Legislative Decree 24/2023, or national acts that constitute implementation of the acts of the European Union specified in the Annex to Directive (EU) 2019/1937, even if not specified in the Annex to Legislative Decree 24/2023, relating to the following areas: public procurement; financial services, products, and markets and prevention of money laundering and terrorist financing; product safety and compliance; transportation safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and data protection; and network and information systems security;
- 2) acts or omissions affecting the financial interests of the Union referred to in Article 325 of the Treaty on the Functioning of the European Union specified in the relevant European Union secondary legislation;
- 3) acts or omissions concerning the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including breaches of EU competition and state aid rules, as well as breaches concerning the internal market related to acts that breach corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;
- 4) acts or conduct that frustrate the object or purpose of the provisions set forth in Union Acts in the areas indicated in (1), (2) and (3).

Information about breaches must relate to conduct, acts or omissions of which the Whistleblower has become aware in the work context.

They do not, however, constitute the subject of the Report:

- disputes, claims or demands related to personal interest of the Whistleblower, or inherent exclusively to his or her individual working relationships with hierarchically subordinate figures;
- Blatantly unsubstantiated news;
- information already in the public domain;
- information acquired on the basis of indiscretion or poorly reliable rumors (e.g., "office rumors");
- breaches already regulated by other European Union or national acts (as indicated in "Part II of the Annex to Legislative Decree 24/2023");
- breaches in national security and defense or national security procurement unless such matters are covered by the relevant European Union secondary law.

In order for the Report to be admissible, it must not only meet the above objective requirements but also be as circumstantial as possible.

In particular, it is necessary for the following to be clear:

- The circumstances of time and place in which the event that is the subject of the Report occurred;
- description of the facts;
- the generalities or other elements that would make it possible to identify the person to whom the reported fact can be attributed.

It is also useful to enclose any documentation that may provide evidence of the facts that are the subject of the Report.

Finally, in order to increasingly foster a culture of transparency and facilitate the continuous improvement path initiated by the Company, the Whistleblowing channels can also be used to report behavior that is misaligned with the behavioral principles contained in the Code of Ethics.

8. Reporting Party/Whistleblower

Reporting Breaches under Art. 2 Legislative Decree. 24/2023 can be made by:

- all employees of Compagnucci High Tech, including those on temporary contracts or performing occasional services, volunteers and trainees;
- personnel with representative, administrative or managerial functions, or who exercise management and control over the company's activities;
- employed workers, self-employed workers, contractors, freelancers, consultants;
- persons not yet hired who have become aware of breaches during the selection process;
- former workers or partners (such as customers and suppliers) of Compagnucci High Tech who have become aware of breaches in the course of their relations with it.

Reports of other breaches attributable to the Code of Ethics can also be made by the recipients of the Code of Ethics such as, for example, customers, suppliers and other stakeholders in general.

To individuals who make a Report under Legislative Decree 24/2023, in line with this document, the rights of protection provided by the legislation itself and indicated in Part III of the same Decree are recognized.

In line with the principles of the latter document, the Company undertakes to guarantee protection for individuals who report a breach of the Code of Ethics from any form of retaliation, discrimination or penalization. The possibility for the Company to make use of the Whistleblower's testimony, possibly even together with other testimonies remains without prejudice, where it is necessary to protect the Company itself in the appropriate seats, including judicial ones.

9. Whistleblowing Channels

Compagnucci High Tech has established an internal channel for sending reports of breaches ex art. 2 Legislative Decree 24/2023, including those relating to breaches of the Code of Ethics, which may be submitted in the following manner:

- **in written form** through the dedicated My Whistleblowing Digital Platform, accessible via the Company's website.
- **verbally**, through appropriate audio recording that can be activated through the My Whistleblowing Digital Platform mentioned above, accessible via the Company's website.

Under certain conditions, the Whistleblower also has the option¹ to use an external channel open at the National Anticorruption Authority (ANAC) or to use public disclosure.

In using the Reporting channels described above, the Whistleblower may enlist the support of an individual who can support him or her in the process and who assumes the role of Facilitator.

In particular, the Whistleblower is autonomous in his or her choice of Facilitator and can identify him or her as the person inside and/or outside the organization identified as most helpful. By way of example but not limited thereto,

¹ The external channel at ANAC can be activated under the following conditions:

- the internal channel is not active or is not suitable to guarantee confidentiality of the Whistleblower;
- the internal channel was used but the Report was not followed up by the Whistleblowing Channel Manager within the designated timeframe or no action was taken to manage it;
- the Whistleblower has reasonable grounds to believe that the use of the internal channel would not be effective or could result in a risk of Retaliation;
- the Whistleblower has probable cause to believe that the breach may pose an imminent or obvious danger to the public interest (e.g., health and safety or environmental damage).

Public disclosure ((through print or electronic media or otherwise through means of dissemination capable of reaching a large number of people) may be used in the following cases:

- the Whistleblower has previously made an Internal and External Report or has directly made an External Report and no response has been given within the prescribed time;
- the Whistleblower has reasonable grounds to believe that the breach may pose an imminent or obvious danger to the public interest;
- the Whistleblower has well-founded reason 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 particular case, such as those where evidence may be concealed or destroyed or where there is well-founded fear that the Whistleblower Person may be colluding with person committing the breach or involved in the breach itself.

the Facilitator can be identified as the Manager of the Whistleblowing Channel, the direct manager, a colleague, or another third party inside or outside the organization.

10. Whistleblowing Management

Reports received through the internal channels described in the previous paragraph will be handled as described below.

a. Receipt of reports

Reports can be received, in the manner described in Section 9 of this document.

The Channel Manager takes charge of the Report received and, where necessary, arranges for the entry of information about the Report on the dedicated Digital Platform.

Following the entry of the Report information, the Channel Manager will provide the Whistleblower with access references to the dedicated Platform (if the Whistleblower has indicated the minimum information necessary to be able to follow up on this contact), for subsequent management and monitoring purposes.

The Channel Manager shall inform the Whistleblower that the Report has been acknowledged, within 7 days of its receipt. Notification about the receipt of the Report and any subsequent changes referring to its status are notified to the Whistleblower through an automatic e-mail sent from the Dedicated Platform. The Whistleblower can check the progress of the Reporting process by accessing the dedicated Platform.

If the Report is sent to a party other than the competent party, the Report must be forwarded by the latter, within 7 days of its receipt, to the competent party, giving simultaneous notification to the Whistleblower.

b. Evaluation of the admissibility of the Report received

Omissis

This phase is aimed at:

1. verifying that the Report was made in accordance with the provisions of this procedure;
2. verifying that the subject of the Report falls within the cases covered by this procedure (breach ex Legislative Decree 24/2023 and/or the Code of Ethics);
3. initiating interlocutions with the Whistleblower by requesting, if necessary, appropriate additions.

The Channel Manager, having assessed the admissibility of the Report, notifies the Whistleblower. Notification about the admissibility of the Report and any subsequent changes referring to its status are notified to the Whistleblower via an automatic notification e-mail sent from the Dedicated Platform. The Whistleblower can check the progress of the Reporting process by accessing the dedicated Platform.

After ascertaining admissibility of the Report, the Channel Manager identifies the responsible parties to be involved in the next inquiry phase and sends the necessary information to them in order to initiate this phase.

c. *Instruction*

The Channel Manager initiates the investigation, ensuring that it is carried out according to the established terms and procedures, and arranging, if necessary, inclusion on the dedicated Platform of the data relating to the Report, for archiving and tracking purposes.

The activities regarding the preliminary phase and document archiving inherent to the Report must be carried out exclusively with the support of the dedicated Platform, suitable for ensuring traceability of the flow in compliance with the provisions of the regulations in force.

Omissis

This phase must be conducted in accordance with the following principles, which are set forth below by way of example but not limited thereto:

- the purpose and scope of application must be clearly defined and documented;
- the investigation must ensure the safety and confidentiality of those involved, the content and documentation;
- Personal data must be managed in line with data protection;
- communication must be clear and unambiguous;
- the Whistleblower should be periodically informed of progress.

d. *Closure*

Omissis

The closure stage indicates the end of the process, as no further action or further investigation is deemed necessary

During this stage, the following steps should be considered:

- conclusion of the Report and communication of the result;
- action in response to any directions (e.g., disciplinary action);
- identification of any ongoing protective measures;
- collection of suggestions from the reporter and other interested parties;
- archiving of documents processed during the previous stages.

Omissis

In addition, with the possible support of the functions and/or consultants involved in the investigation, the Whistleblowing Channel Manager will proceed to:

- formalize measures to resolve the breach;
- identify the person responsible for verifying the proper implementation of the measures and subsequent monitoring;
- receive constant updates on the effectiveness of monitoring principals;
- define disciplinary measures, if applicable;
- involve the relevant authorities, if necessary.

At the end of the closure phase, with the support of the functions and/or consultants involved, the Whistleblowing Channel Manager provides feedback to the Whistleblower.

The feedback provided in such a communication must give an account of the outcome of the Report and, in particular, by way of example, this type of communication may be:

- dismissed for lack of grounds, lack of sufficient evidence or other reasons;
- concluded with measures taken to resolve the issue raised;
- referred to an appropriate authority for further investigation.

The Manager of the Whistleblowing channel shall acknowledge the Whistleblower within three months of the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within three months of the expiration of the period of 7 (seven) days from the submission of the Report.

11. Prohibition of Retaliation

No **form of retaliation** or **discriminatory measure** related, directly or indirectly, to the Report is permitted or tolerated against the Whistleblower.

Omissis

Part III - FINAL PROVISIONS

12. The protection of confidentiality

The identity of the Whistleblower and any other information from which their identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of said Whistleblower, to persons other than those authorized to receive or follow up the reports and expressly authorized to process such data.

In particular, with regard to the disclosure of the identity of the Whistleblower, Legislative Decree 24/2023 (Art. 16) provides the following protections:

- within the framework of criminal proceedings, the identity of the Whistleblower is covered by secrecy in the manner and to the extent provided for in Article 329 of the Code of Criminal Procedure;
- within the framework of the proceedings before the Court of Accounts, the identity of the Whistleblower may not be disclosed until the investigation stage is closed;
- within the scope of disciplinary proceedings, the identity of the Whistleblower may not be disclosed, where the allegation of the disciplinary charge is based on investigations that are separate and additional to the Report, even if consequent to the Report. 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 alleged perpetrator, the Report will be usable for the purposes of disciplinary proceedings only if the Whistleblower expressly consents to the disclosure of his or her identity. In such cases, notice shall be given to the Whistleblower by written communication of the reasons for the disclosure of confidential data, as well as in the Internal and External Reporting procedures referred to in this Chapter when the disclosure of the Whistleblower's identity and any other information from which it may be directly or indirectly inferred is also indispensable for the defense of the Person of interest (.

Confidentiality is also guaranteed:

- in the case of reports, internal or external, or at the request of the Whistleblower, through a direct meeting with the person handling the Report;
- When the Reporting is done through modes other than the ones established in accordance with Legislative Decree 24/2023 or reaches personnel other than those authorized to handle reports;
- to the reported person and persons other than the reported person, but mentioned in the Report or involved in the Reporting process.

Confidentiality is also respected by the adoption of a dedicated reporting tool through the dedicated My Whistleblowing Platform that ensures adequate encryption systems.

13. Continuous improvement process

Omissis

14. Archiving and traceability of documentation

Omissis

15. Information and communication

Omissis

16. Disciplinary measures

Omissis

17. Rules and Privacy

The main regulatory framework and other relevant references that form the basis of this procedure and related processes are listed below:

- EU Directive no. 1937/2019 on the protection of persons who report breaches of Union law and its local transpositions;
- Legislative Decree no. 24/2023 "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws."
- international ISO 37002 "Whistleblowing management systems";
- EU Regulation no. 679/2016 "General Data Protection Regulation - GDPR" and its local transpositions.

Personal data must be handled in compliance with the GDPR and its local transpositions.

All personal data not useful for management of the Report should not be collected. In addition, in the event of accidental collection, such data must be promptly deleted.

The processing of personal data is handled in accordance with the GDPR Regulation, as well as any other applicable laws and/or regulations.

Both the personal data of the Whistleblower - if the Report is not anonymous - and the personal data of the person involved and/or any third parties, as well as any additional information collected as part of the investigation necessary and appropriate to ascertain and verify whether or not the Report is well-founded, will be processed.

The Data Controller is Compagnucci High tech Srl.