Hausbrandt
Trieste 1892 S.p.a.

Via Foscarini, 52

Nervesa della Battaglia (TV)

Whistleblowing Policy

INTRODUCTION

The European Union, with Directive 2019/1937, has renewed the legislation regarding the protection of persons who report breaches of Union law, in order to create a minimum standard for the protection of whistleblowers' rights in all Member States. Italy has implemented the European Directive with the Legislative Decree 10 March 2023 no. 24 (hereinafter the "Decree").

By adopting this Policy, Hausbrandt Trieste 1892 S.p.A. (hereinafter, the "Company") intends to comply with the aforementioned regulatory requirements, as well as the guidelines provided in this regard by ANAC (the Italian National Anti-Corruption Authority).

The aim is to provide the whistleblower, i.e., the person who reports breaches, with clear operational indications regarding the subject, contents, recipients and methods of transmission of the reports.

The reporting management process ensures the confidentiality of the reporting person's identity from the time of receipt and in any subsequent contact. Pursuant to section 5, paragraph 1, letter e) of the Decree, this policy therefore provides information on the channels, procedures and conditions for internal and external reports.

1. REPORTING PERSONS

Reports may be made by the following parties:

a) employees, including workers who perform:

- part-time, intermittent, fixed-term, temporary agency, apprenticeship or ancillary work (whose employment relationship is regulated by Legislative Decree no. 81/2015);
- occasional work (pursuant to section 54-bis of Law Decree no. 50/2017, converted by Law no. 96/2017);

b) self-employed persons

- with a works contract (section 2222 of the Civil Code);
- with a collaboration relationship (as per section 409 of the Code of Civil Procedure), such as agency agreements, commercial representation and other collaborative relationships that result in the provision of predominantly personal, continuous and coordinated work, even if not of a subordinate nature;
- with a collaboration relationship that results in exclusively personal, continuous performance of work, the manner of performance of which is organized by the client;

c) collaborators who perform their work activities for entities that provide goods or services or perform works for the Company;

d) freelancers and consultants who perform their activities for the Company;

e) volunteers and interns, paid and unpaid, who perform their activities for the Company;

f) the shareholder and persons with administrative, management, control, supervisory or representation functions, even if these functions are exercised on a purely *de facto* basis within the Company (e.g., members of the BoD or SB).

The protection of reporting persons (section 7 of this Policy) also applies if the report, complaint to the judicial or accounting authorities, or public disclosure of information occurs in the following cases:

a) when the legal relationship described above has not yet begun, if the information about the breaches was acquired during the selection process or other pre-contractual stages;

b) during the probationary period;

c) after the dissolution of the legal relationship if the information on the breaches was acquired during the course of the relationship itself.

2. SUBJECT OF THE REPORT AND EXCLUDED REPORTS

The reports indicated in the following table may be made:

Number of employees	**With Organizational and Management Model Legislative Decree no. 231/'01**	**Subject of the report**
50 or more	Yes	- offenses specified in Legislative Decree no. 231/2001 (see point c below) - breaches of the Model (see point c below) - European and national offenses (see points a) and b) below) (section 3, paragraph 2, letter b), second sentence, Legislative Decree no. 24/2023)

More in detail, the breaches listed in the table above may concern:

(a) breaches of national or European provisions that consist of offenses concerning 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, and security of network and information systems;

(b) breaches of European provisions consisting of (i) acts or omissions that affect the financial interests of the Union; (ii) acts and omissions relating to the internal market; (iii) acts and conduct that defeat the object or purpose of the provisions of the Union acts in the areas mentioned above;

(c) unlawful conduct relevant under Legislative Decree 231/2001 or breaches of organizational and management models.

3. REPORTING CHANNELS: INTERNAL, EXTERNAL, PUBLIC DISCLOSURE

The Company has established an internal reporting channel that guarantees the confidentiality of the identity of the reporting person, the person concerned, and the person otherwise referred to in the report, as well as the content of the report and the related documentation.

As a reminder, a *whistleblowing* report must first be made using the internal channel.

Reporting through the external channel, established and managed by ANAC[1], may be done only under certain conditions[2], and public disclosure under even stricter conditions[3], without prejudice to the possibility of making complaints to the judicial authorities.

[1] https://www.anticorruzione.it/-/whistleblowing

[2] Reporting persons may use the **external channel (ANAC)** when:
- there is no provision within the work-related context for mandatory activation of the internal reporting channel or this channel, even if mandatory, is not active or, even if activated, does not comply with what is required by law;
- the reporting person has already made an internal report and it has not been followed up on;
- the reporting person has reasonable grounds to believe that, if they made an internal report, the report would not be effectively followed up on or that the same report could lead to a risk of retaliation;
- the reporting person has reasonable grounds to believe that the breach may pose an imminent or manifest danger to the public interest.

[3] Reporting persons may directly make a **public disclosure** when:
- the reporting person has previously made an internal and external report or has directly made an external report and no feedback has been given within the established timeframe regarding the action envisaged or taken as follow-up;
- the reporting person has reasonable grounds to believe that the breach may pose an imminent or manifest danger to the public interest;
- the reporting person has reasonable grounds to believe that the external report may carry the risk of retaliation or may not be effectively followed up on due to the specific circumstances of the particular case, such as those where evidence could be concealed or destroyed or where there is a well-founded fear that the person who received the report may be in collusion with the perpetrator of the breach or involved in the breach.

4. CONTENTS AND METHOD OF SUBMISSION OF THE REPORTS

A **whistleblowing report** may be made if the following conditions are met:

- when there is information, including reasonable suspicions, regarding breaches that have been committed or that, on the basis of concrete evidence, may be committed in relation to national or European Union regulatory provisions, harming the public interest or the integrity of the Company, as well as information regarding conduct aimed at concealing such breaches

  and

- such information is learned, or suspicions have arisen, within the work-related context.

Reports pertaining exclusively to the following cannot be addressed:

- disputes, claims or requests related to a personal interest of the reporting person;
- the reporting person's individual working relationship or collaboration with the Company, or with hierarchically superordinate figures;
- aspects of the reported person's private life, without any direct or indirect connection with the company's business and/or professional activities.

Furthermore, reports of the following nature are not allowed:

- specious, defamatory, slanderous or aimed solely at damaging the reported person;
- relating to breaches that the reporting person knows to be unfounded.

Contents of the report

The report, **under penalty of inadmissibility**, must contain:

1. the **identifying data** of the reporting person (except for the indications related to anonymous reports) as well as an address to which subsequent updates should be communicated;
2. a **clear, complete and detailed description of the facts** being reported;
3. the **circumstances of time and place** in which the fact that is the subject of the report occurred and, therefore, a description of the facts that are the subject of the report, specifying the details relating to the circumstantial information and, where present, also the manner in which the facts that are the subject of the report came to light;
4. the **particulars** or other elements that allow the identification of the person(s) held responsible for the reported facts;
5. the indication of **any other persons** who may report on the facts being reported;
6. the indication of **any documents** that may confirm the validity of such facts;
7. **any other information** that may provide useful feedback about the existence of the reported facts.

8. in case the analog channel is used (*see below*), the **express statement that the reporting person wants to benefit from whistleblowing protections**, e.g., by inserting the words "confidential to the reporting manager."

How to report

Whistleblowing reports may be made as follows:

> by calling the following number: **+39 0422 889101**;

> at the request of the reporting person through a direct meeting with the manager of the internal reporting channel, Mr. Antonio Ereno, (Supervisory Board) or his designated deputy, the Chairman of the Board of Statutory Auditors;

> by sending an email to **odv231@hausbrandt.it**.

through regular mail by placing the report in two sealed envelopes, including, in the first one, the identifying data of the reporting person, together with an identity document, in the second one, the subject of the report; both envelopes should then be placed in a third envelope bearing, on the outside, the words "confidential to the reporting manager" and addressed to: ODV – Hausbrandt Trieste 1892 S.p.A., Via Foscarini, 52 31040 Nervesa della Battaglia (TV).

Anonymous reporting

The Company reserves the right to consider anonymous reports, in order to initiate in-depth investigations to ascertain what has been reported, only where they include precise, consistent and adequately substantiated information. In any case, the measures to protect the reporting person apply only if such person is subsequently identified and retaliated against.

Transmission of reports

Whistleblowing reports should be sent to: Mr. Antonio Ereno, in accordance with the chosen reporting channel.

In the event of prolonged absence of the recipient/reporting manager, the Chairman of the Board of Statutory Auditors is indicated as his substitute. Furthermore, reports must be addressed to the latter also in cases where the reporting manager is in a state of conflict of interest pursuant to point 6 below of this policy.

Finally, it should be noted that the receipt of reports is suspended during the period when the Company is closed.

5. REPORT MANAGEMENT

This procedure regulates the process of receiving, analyzing and processing reports of unlawful conduct of which the reporting person has become aware within the work-related context.

As part of the management of the internal reporting channel, the reporting manager (hereinafter also referred to as the "manager" or "recipient") operates in the following ways:

Receipt of the report

In the event that the report is mistakenly transmitted to/received by a person not appointed to receive it, and it is clear that it is a whistleblowing report, it shall be the latter's obligation to promptly provide evidence of its receipt to the reporting manager, in any case within 7 (seven) days of such receipt, simultaneously giving notice of such transmission to the reporting person, without prejudice to all the confidentiality obligations provided for in this policy also on the part of the same (and consequent liability of the same in the event of violation of said policy).

The recipient shall issue the reporting person with an acknowledgment of receipt of the report within **seven days** from the date of receipt. The notice will be sent to the address indicated by the reporting person and, if not indicated, the report will be filed.

Anonymous reports will be recorded and their documentation will be kept.

The Company will file reports received by regular mail through appropriate means to ensure confidentiality (e.g., within archives protected by security measures).

Reports made orally - in the forms indicated in this Policy - subject to the consent of the reporting person, shall be documented by the reporting manager either by recording on a device suitable for storage and listening or through minutes.

In the latter case, the reports will be kept within devices suitable for storage and listening, or, alternatively, the report will be transcribed in full.

In the case of a direct meeting with the reporting person, a recording of the meeting will be made, or, if this does not occur or the reporting person does not consent to the recording, specific minutes of the meeting will be drawn up, which will be signed by both the manager and the reporting person and a copy of which will be provided to the latter.

Relationship with the reporting person and additions to the report

The recipient maintains discussions with the reporting person and may request additions, if necessary.

In the case of minutes drawn up following a meeting with the reporting person, the reporting person may check, rectify and confirm the minutes of the meeting by signing them.

Review of the report

The recipient follows up on the reports received, assessing the legitimacy of the reporting person and whether the report falls within the scope of the rule; this is followed by an assessment of the circumstances of time and place in which the event occurred.

At the outcome of the preliminary check:

- if the conditions do not exist, the report is **dismissed**, stating the reasons;
- if the conditions do exist, the **preliminary investigation** is started.

Preliminary investigation

The recipient ensures that the preliminary investigation is properly conducted by:

- collecting documents and information;
- involving external parties (in case it is necessary to use the technical assistance of third-party professionals) or other corporate functions, which have the obligation to cooperate with the reporting manager;
- hearing any other internal/external parties where necessary.

The preliminary investigation is carried out in accordance with the following principles:

- the necessary measures are taken to prevent the identification of the reporting person and the people concerned;
- checks are conducted by people with the necessary training, and the activities are properly tracked and filed;
- all parties involved in the assessment maintain the confidentiality of information received, unless otherwise required by law;
- checks are conducted by ensuring that appropriate measures are taken for the collection, use, disclosure, and storage of personal information and by ensuring that the needs of the investigation are balanced with that of privacy protection;
- appropriate measures are ensured to handle any conflicts of interest if the report concerns the recipient.

Feedback to the reporting person

Within three months from the date of the acknowledgment of receipt or, in the absence of such acknowledgment, within three months from the expiration of the seven-day period from the submission of the report, the recipient shall provide feedback regarding the report, communicating either:

- its **dismissal**, providing the reasons for the decision, or
- the **validity** of the report and its forwarding to the competent internal bodies for follow-up, or
- the activities carried out and yet to be carried out (in the case of reports that involve, for the purposes of checking, a longer investigation period) and any measures taken (provisions taken or referral to the competent authority).

6. CONFLICT OF INTEREST

If the reporting manager has a conflict of interest, such as being a reported or reporting person, the report will be handled by its deputy, the Chairman of the Board of Statutory Auditors.

7. PROTECTION OF THE REPORTING PERSON AND THEIR RESPONSIBILITY

Reporting persons shall not suffer any form of retaliation. As a matter of fact, the law provides that those who make the report cannot be sanctioned, demoted, fired, transferred, or subjected to other organizational measures that end up having, directly or indirectly, negative effects on the working conditions, or effects of discrimination or retaliation against them.

A person's motives for reporting or exposing or publicly disclosing are irrelevant for the purposes of their protection.

In the context of judicial or administrative proceedings, or even extrajudicial proceedings aimed at ascertaining prohibited conduct against reporting persons, it shall be presumed that such conduct occurred as a result of the reporting, public disclosure, or complaint to the judicial or accounting authority. The burden of proving that such conduct toward the reporting persons is motivated by reasons unrelated to the report, public disclosure or complaint remains on the person who carried it out.

Moreover, the alleged discriminatory or retaliatory measures suffered must be communicated to ANAC, which alone is entrusted with the task of ascertaining whether the retaliatory measure is consequent to the reporting of unlawful conduct and, in the absence of proof by the Company that the measure taken is unrelated to the reporting, applying an administrative fine.

Processing of personal data. Confidentiality

All processing of personal data will be carried out in accordance with Regulation (EU) 2016/679, Legislative Decree no. 196 dated 30 June 2003, and sections 13 and 14 of the Decree; furthermore, failure to comply with confidentiality obligations may result in disciplinary liability, without prejudice to any further liability provided for by law.

The information regarding the processing of personal data following a whistleblowing report is available as an annex to this Policy.

Internal and external reports and the related documentation shall be retained for as long as necessary for the processing of 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 confidentiality and personal data protection obligations.

Responsibilities of the reporting person

The Company guarantees the reported person the right to be informed (within a reasonable timeframe) about any reports involving them, guaranteeing the right to defense where disciplinary measures are initiated against them.

This procedure is also without prejudice to the reporting person's criminal and disciplinary liability in the event of slanderous or defamatory reporting under the Criminal Code and section 2043 of the Civil Code.

Any forms of abuse of the whistleblowing reporting procedure, such as reports that are manifestly unfounded and/or made for the sole purpose of harming the reported person or other entities, and any other hypothesis of improper use or intentional exploitation of the procedure itself, are also a source of disciplinary liability and other types of liability.

8. ENTRY INTO FORCE AND AMENDMENTS

This policy will entry into force on December 17, 2023. Upon its entry into force, all provisions previously adopted on the subject, in whatever form communicated, shall be considered repealed, if incompatible or different, as they are replaced by the present ones.

The Company will provide the necessary publicity and deliver a copy of the policy to each employee.

All employees may propose motivated additions to this policy when deemed necessary; proposals will be considered by the Company's Board of Directors.

This policy shall nevertheless remain subject to periodic review.

Hausbrandt Trieste 1892 S.p.A.

PERSONAL DATA PRIVACY NOTICE PURSUANT TO ARTICLES 13-14 OF REGULATION (EU) 2016/679 WITHIN THE SCOPE OF THE WHISTLEBLOWING POLICY

With this notice Hausbrandt Trieste 1892 S.p.A. (hereinafter the "Company") intends to provide the information provided for in Articles 13 and 14 of Regulation (EU) 2016/679 (or "*General Data Protection Regulation*" - "*GDPR*"), regarding the processing of personal data carried out by the Company within the scope of its "Whistleblowing Policy", adopted in accordance with Legislative Decree 10 March 2023 no. 24[4] and, specifically, of all activities and obligations related to the functioning of the Company's system for the management of *whistleblowing* reports.

The following information is provided to the "reporting" persons and all other potential data subjects, such as, for example, the persons indicated as possible perpetrators of the unlawful conduct, any "facilitators" (as defined by the reference legislation), as well as any other person involved in the "Whistleblowing Policy" in different capacities.

1. Data Controller and DPO – "Data Protection Officer"

The Personal Data Controller is Hausbrandt Trieste 1892 S.p.A. Via Foscarini, 52 31040 Nervesa della Battaglia (TV), Italy. The Data Controller has appointed a Data Protection Officer ("DPO"), who can be contacted by the Data Subject by writing to the following address: dpo@hausbrandt.it

2. Categories of personal data processed and purposes of processing

According to the approach of the regulations in question, personal data may be acquired by the Company as they are contained in the *whistleblowing* reports, or in the acts and documents attached to them, received by the Company through the channels established by the aforementioned Policy.

The receipt and management of such reports may give rise, depending on their content, to the processing of the following categories of personal data:

a) common personal data referred to in Article 4, point 1 of the GDPR, including, for example, personal details (first name, last name, date and place of birth), contact data (landline and/or mobile phone number, postal/e-mail address), job role/occupation;
b) "special" personal data referred to in Article 9 of the GDPR, including, for example, information relating to health conditions, political opinions, religious or philosophical beliefs, sexual orientation or trade union membership;
c) "judicial" personal data referred to in Article 10 of the GDPR, relating to criminal convictions and offenses, or related security measures.

[4] Legislative Decree implementing Directive (EU) 2019/1937 of the European Parliament and Council of 23 October 2019.

With regard to the aforementioned categories of personal data, **we underline the importance that the reports forwarded be free of information that is manifestly irrelevant for the purposes of the reference discipline**, inviting in particular the reporting persons to refrain from using personal data of a "special" and "judicial" nature unless deemed **necessary and unavoidable** for the purposes of the same, in compliance with Article 5 of the GDPR.

The aforementioned information will be processed by the Company – Data Controller – in accordance with the provisions of Legislative Decree no. 24/2023 and, therefore, in general, **in order to carry out the necessary preliminary investigation activities aimed at verifying the validity of the facts being reported and the adoption of the consequent measures**.

Furthermore, the data may be used by the Data Controller for **purposes related to the need to defend or establish one's rights** in the context of judicial, administrative or extrajudicial proceedings and in the context of civil, administrative or criminal disputes arising in relation to the report made.

3. Legal basis for the processing of personal data

The legal basis for the processing of personal data is mainly the **compliance with a legal obligation** to which the Data Controller is subject – Article 6, paragraph 1, letter c) of the GDPR – that, in particular, by virtue of the aforementioned legislation, is required to implement and manage information channels dedicated to receiving reports of unlawful conduct detrimental to the integrity of the Company and/or the public interest.

In the cases covered by the same regulations, **specific and free consent may be requested from the reporting person** – pursuant to Article 6, paragraph 1, letter a) of the GDPR – and, specifically, where there is a **need to disclose their identity**, or where the **recording of reports collected orally**, by telephone or via voice messaging systems, or through direct meetings with the person in charge of managing the reports is envisaged.

The processing of "**special**" personal data which may be included in the reports is based on the **fulfillment of obligations and the exercise of specific rights of the Data Controller and the data subject in the field of employment law**, pursuant to Article 9, paragraph 2, letter b) of the GDPR.

As for the purpose of establishing, exercising or defending legal claims, the relevant legal basis for the processing of personal data is the **legitimate interest of the Data Controller** in this regard, as referred to in Article 6, paragraph 1, letter f), of the GDPR; for the same purpose, the processing of personal data of a "**special**" nature, if present, is based on Article 9, paragraph 2, letter f) of the GDPR.

4. Nature of the provision of personal data

The provision of personal data is optional, given the possibility of forwarding anonymous reports to the Company, where they include precise, consistent and adequately substantiated information, without prejudice to the provisions of the law, with regard to this case, on the subject of measures to protect the reporting person. If provided, the personal data will be processed to manage the report according to the limits and with the guarantees of confidentiality imposed by the relevant legislation.

5. Method of processing and storage period of personal data

The processing of personal data included in the reports forwarded in accordance with the "Whistleblowing Policy" will be carried out by the parties "in charge-authorized" by the Company and will be based on the principles of fairness, lawfulness and transparency, as per Article 5 of the GDPR.

The processing of personal data may be carried out in analogical and/or computer/telematic modes that are functional to storing, managing and transmitting them, in any case in application of appropriate physical, technical and organizational measures designed to ensure their **security and confidentiality at every stage of the procedure, including the filing of the report and related documents** - subject to the provisions of section 12 of the Legislative Decree no. 24/2023 - with particular reference to the identity of the reporting person, the persons concerned and/or otherwise referred to in the reports, the content of the same and the related documentation.

The reports received by the Company, together with the enclosed acts and documents, will be kept for the time necessary for their management and, in any case, as provided for by the regulations, **for a period not exceeding five years from the date of communication of their final outcome**. After this deadline, the reports will be deleted from the system

Consistent with the indications provided in paragraph 1, personal data included in reports that are manifestly irrelevant to the purposes of the same will be deleted immediately.

6. Scope of communication and transfer of personal data

In addition to the aforementioned internal figures specifically authorized by the Data Controller, the personal data collected may also be processed, within the scope of the "Whistleblowing Policy" and in pursuit of the indicated purposes, by the following third parties, formally designated as Data Processors if there are the conditions provided for in Article 28 of the GDPR:

- providers of consulting and assistance services in the implementation of the "Whistleblowing Policy";
- IT companies and professionals with respect to the application of appropriate technical, IT and/or organizational security measures on the information processed by the company system;

If necessary, personal data may be transmitted to the Judicial Authorities and/or Law Enforcement Agencies who request it in the context of judicial investigations.

Personal data will be processed within the European Economic Area (EEA) and stored on servers that are located there.

Under no circumstances will personal data be disseminated.

7. Rights of the data subject

Each data subject has the right to exercise the rights set forth in Articles 15 et seq. of the GDPR, in order to obtain from the Data Controller, for example, access to their personal data, their rectification

or erasure or the restriction of their processing, without prejudice to the possibility, in the absence of satisfactory response, to lodge a complaint with the Personal Data Protection Authority.

To exercise these rights, it is necessary to forward a specific request in free form to the following address of the Data Controller: **info@hausbrandt.it** or submit to the same address the form available on the website of the Personal Data Protection Authority.

In this regard, we inform you that the aforementioned rights of the data subjects may be limited pursuant to section 2-undecies of Legislative Decree 30 June 2003, no. 196 ("Privacy Code," as amended by Legislative Decree no. 101/2018), for the time and to the extent that this constitutes a necessary and proportionate measure, if their exercise could result in a concrete and effective prejudice to the confidentiality of the identity of the reporting persons.

In such cases, the data subjects will still have the right to contact the Data Protection Authority so that the latter can assess whether there are the conditions for acting in the manner provided for in section 160 of Legislative Decree no. 196/2003.