Hausbrandt Trieste 1892 S.p.A.

Via Foscarini,

52 Nervesa della Battaglia

(TV) - Italy

Whistleblowing Policy

Index of changes

Rev.	Date	Summary of changes
0	17/12/2023	First Issue
1	14/06/2024	Correction of address for sending a report by ordinary mail
2	30/09/2024	Procedure update for introduction of reporting methods with computer system

INTRODUCTION

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

By adopting this Policy, the company Hausbrandt Trieste 1892 S.p.A. (hereinafter, the "Company") has intended to comply with the aforementioned regulatory requirements, as well as with the addresses provided in this regard by ANAC.

The aim of this procedure is to provide the whistleblowers, or those who report violations, with clear operational indications regarding the subject, content, recipients and methods of transmitting reports.

The reporting management procedure guarantees the confidentiality of the identity of the reporting party from the moment of receipt and in any subsequent contact. Pursuant to art. 5, para. 1, letter e) of the Decree, this policy therefore provides information on the channels, procedures and conditions for making internal and external reports.

1. REPORTING ENTITIES

Reports can be made by the following parties:

a) employees, including workers who perform:

   - part-time, intermittent, fixed-term, leasing, apprenticeship, ancillary work (whose employment relationship is governed by Legislative Decree no. 81/2015);

   - occasional services (pursuant to art. 54-bis of Legislative Decree no. 50/2017, conv. by the Law no. 96/2017);

b) self-employed persons:

   - with work contract (art. 2222 of the Italian Civil Code);
   - with a collaboration relationship (referred to in art. 409 of the Italian Code of Civil Procedure), such as agency, commercial representation and other collaboration relationships that take the form of a continuous and coordinated work, mainly personal, even if not of a subordinate nature;
   - with a collaboration relationship that materializes in exclusively personal, continuous work services and whose execution methods are organized by the client;

c) collaborators who carry out their work with persons who provide goods or services or who carry out works on behalf of the Company;

d) freelancers and consultants who work for the Company;

e) volunteers and trainees, paid and unpaid, who work for the Company;

f) the shareholder and persons with administrative, management, control, supervisory or representative functions, even if these functions are exercised on a purely factual basis at the Company (for example, members of the Board of Directors or the Supervisory Body).

The protection of whistleblowers (art. 7 of this Policy) also applies if the reporting, the complaint to the judicial or accounting authority or the public disclosure of information takes place in the following cases:

a) when the "professional" legal relationship has not yet begun, if the information on the violations was acquired during the selection process or at other pre-contractual stages;

b) during the trial period;

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

2. SUBJECT OF THE REPORT AND EXCLUDED REPORTS

The following reports can be made as indicated in the following table:

Number of employees	**With Organizational and Management Model as per Leg. Decree no. 231/'01**	**Subject of the report**
50 or more	Yes	- offences indicated in Leg. Decree no. 231/2001 (see point c below) - violations of the Model (see point c below) - European and national offences (see below points a and b) (Art. 3 para. 2, lett. b), second sentence, Leg. Decree no. 24/2023)

In more detail, the violations indicated in the table above may concern:

a) violations of national or European provisions consisting of offences 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; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy protection and protection of personal data and security of networks and information systems;

b) infringements of European provisions consisting of: i) acts or omissions affecting the financial interests of the Union; ii) acts and omissions concerning the internal market; iii) acts and conduct which undermine the object or purpose of the provisions of Union acts in the areas referred to above;

c) unlawful relevant conduct pursuant to Leg. Decree no. 231/2001 or violations of organizational models and management with the exception.

3. REPORTING CHANNELS: INTERNAL AND EXTERNAL REPORT, PUBLIC DISCLOSURE

The Company has established an internal reporting channel that guarantees the confidentiality of the identity of the whistleblower, 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.

We remind you that you must first proceed with the whistleblowing report using the internal channel.

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

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

[2] Whistleblowers may use the **external channel (ANAC)** when:
- within the work context, the mandatory activation of the internal reporting channel is not foreseen or this, even if mandatory, is not active or, even if activated, does not comply with what is required by law;
- the whistleblower has already made an internal report and it has not been followed up;
- the whistleblower has reasonable grounds to believe that, if he/she made an internal report, it would not be effectively followed up or that the same report could determine the risk of retaliation;
- the whistleblower has reasons for believing that the breach may constitute an imminent or clear threat to the public interest.

[3] Whistleblowers may directly make a **public disclosure** when:
- the whistleblower has previously made an internal and external report or has made an external report directly and no response has been given within the established deadlines regarding the measures envisaged or adopted to follow up on the reports;
- the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or clear danger to the public interest;
- the whistleblower has reasonable grounds to believe that the external whistleblowing may involve a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case. For example, there may be circumstances where evidence may be concealed or destroyed, or where there is a well-founded fear that the recipient of the report may be colluding with or involved in the perpetrator of the violation.

4. CONTENT AND METHODS OF REPORTING

Whistleblowing report can be carried out if the following conditions are met:

- when there is information, including well-founded suspicions, concerning violations committed or which, on the basis of concrete elements, may be committed of national or European Union regulatory provisions that harm the public interest or the integrity of the Company, as well as concerning conduct aimed at concealing such violations

  and

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

Reports exclusively related to the following cannot be taken into consideration:

- to disputes, claims or requests related to a personal interest of the whistleblower;
- to individual employment relationships or collaboration of the whistleblower with the Company, or with hierarchically superior persons;
- to aspects of the private life of the whistleblower, without any direct or indirect connection with the company and/or professional business.

In addition, the following reports are not allowed:

- pretentious, defamatory, libellous reports or reports aimed exclusively at damaging the reported person;
- reports related to violations that the whistleblower knows are unfounded.

Whistleblowing contents

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

1. the **identification data** of the whistleblower (except for indications relating to anonymous reports) as well as an address to which subsequent updates can be communicated;
2. the **clear, complete and detailed description** of the facts subject to reporting;
3. **time and place** in which the fact being reported occurred and, therefore, a description of the facts being reported, specifying the details relating to the circumstantial news and where present also the methods by which the facts being reported were known;
4. the **general information** or other elements that allow the identification of the person(s) deemed responsible for the reported facts;
5. the indication of **any other parties** who could attest to the facts being reported;
6. the indication of **any documents** that can confirm the validity of these facts;

7. **any other information** that could provide useful confirmation on the veracity of the facts reported;
8. in the case of use of the analogue channel (see below), the e**xpress declaration of wanting to benefit from the whistleblowing protections**, e.g. by inserting the words "reserved to the whistleblower".

Signal mode

Whistleblowing reports can be made in the following ways:

> by calling the following number: **+39 0422.889101**;

> at the request of the whistleblower through a direct meeting with the manager of the internal reporting channel, Eng. Antonio Ereno, (Supervisory Body);

> through ordinary mail by inserting the report in two closed envelopes, including, in the first, the identification data of the whistleblower, together with an identity document; and in the second, the subject of the report; both envelopes must then be inserted in a third envelope showing, on the outside, the words "reserved for the manager of the report" and addressing it to: ODV (SB) – Eng. Antonio Ereno c/o Hausbrandt Trieste 1892 SpA, Via Foscarini, 52 31040 Nervesa della Battaglia (TV);

> through the **My Whistleblowing add-on** to the My Governance software, as an alternative reporting channel suitable to guarantee, with IT methods, the confidentiality of the identity of the whistleblower, in compliance with the regulations (hereinafter, the "Software"); in this regard, it is specified that registration to the Software does not affect confidentiality;

Through the IT channel and then through the Software, the whistleblower will be guided at each stage of the report and will be requested, for fuller clarity, to complete a series of mandatory fields to be filled in, in order to comply with the necessary requirements. It is essential that the elements indicated are known directly by the whistleblower and not reported or referred by other subjects.

Anonymous reports

The Company reserves the right to consider anonymous reports, in order to initiate inquiries/investigations for the assessment of what has been reported, only if they present precise, concordant and adequately detailed information. In any case, the protection measures to protect the whistleblower only apply if the whistleblower is subsequently identified and has suffered retaliation.

Transmission of reports

Whistleblowing reports must be sent to: Eng. Antonio Ereno, in accordance with the reporting channel adopted.

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

5. REPORT MANAGEMENT

This procedure regulates the process of receiving, analysing and processing reports of illegal conduct of which the reporting party has become aware within the work context.

As part of the management of the internal reporting channel, the reporting manager (hereinafter also the "manager" or "receiver") acts in the following ways:

Receipt of the report

In the event that the report has been erroneously transmitted/received to/from a person not in charge of receiving it, and it is evident that it is a whistleblowing report, it will be its obligation to promptly evidence its receipt to the manager of the report, in any case within 7 (seven) days of such receipt, giving simultaneous notice of such transmission to the whistleblower, without prejudice to all the confidentiality obligations provided for in this policy also in relation to the same (and consequent its responsibility in the event of violation of the same).

The receiver shall issue to the whistleblower notice of receipt of the report within **seven days** from the date of receipt. The notice will be sent to the address indicated by the whistleblower and, if not indicated, the report will be filed.

Anonymous reports are recorded and their documentation is kept.

The Company will archive reports received by ordinary mail through suitable tools that guarantee confidentiality (e.g. within archives protected by security measures).

The report made orally - in the forms indicated in this Policy - with the consent of the whistleblower, is documented by the manager of the report by recording on a device suitable for storage and listening or by minutes.

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

In the event of a direct meeting with the whistleblower, the same will be registered, or, if this does not happen or the whistleblower does not consent to the registration, the appropriate meeting report will be drawn up, which will be signed by both the manager and the whistleblower and of which a copy will be provided to the latter.

If the report is made through the Software, the Software itself will provide for a complete and confidential logging in accordance with the relevant legislation. The documents are stored and archived in digital format, through the Software, in order to guarantee the traceability, confidentiality, conservation and availability of the data throughout the process.

Relations with the whistleblower and additions to the report

The receiver maintains discussions with the whistleblower and may request, if necessary, additions.

In the event of a report drawn up following a meeting with the whistleblower, the latter may verify, rectify and confirm the report of the meeting by signing it.

Examination of the report

The recipient follows up on the reports received, assessing the existence of the legitimacy of the whistleblower and that the report falls within the scope of the rule; the assessment of the circumstances of time and place in which the event occurred follows.

At the end of the preliminary check:

- if the prerequisites are not met, the report will be **archived**, with an explanation of the reasons provided;
-
- if the conditions are met, the **investigation** is initiated.

Investigation

The recipient guarantees the correct conduct of the investigation through:

- the collection of documents and information;

- the involvement of external parties (in the event that it is necessary to make use of the technical assistance of third-party professionals) or other company functions, which have the obligation to collaborate with the reporting manager;

- the hearing of any other internal/external subjects, where necessary.

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

- the necessary measures are taken to prevent the identification of the whistleblower and the persons involved;

- the checks are carried out by people with the necessary preparation and the activities are tracked and archived correctly;

- all parties involved in the evaluation maintain the confidentiality of the information received, unless otherwise provided by law;

- the verifications are carried out ensuring the adoption of appropriate measures for the collection, use, disclosure and storage of personal information and ensuring that the needs of the investigation are balanced with those of the protection of privacy;

- the appropriate measures are guaranteed to manage any conflicts of interest if the report concerns the recipient.

Response to the whistleblower

Within three months from the date of the notice of receipt or, in the absence of such notice, within three months from the expiry of the seven-day period from the submission of the report, the recipient shall provide feedback on the report, communicating alternatively:

- the **archiving**, providing the reasons for the decision, or
- the **reasonableness** of the report and sending it to the competent internal bodies responsible for its follow-up, or
- the activity carried out and still to be carried out (in the case of reports that involve, for the purposes of checks, a longer assessment activity) and any measures adopted (measures adopted or referral to the competent Authority).

6. CONFLICT OF INTEREST

If the manager of the reports is in conflict of interest, for example as a reported or reporting party, the report may be transmitted to ANAC, as indicated in point 3 of this procedure.

7. WHISTLEBLOWER PROTECTION AND RESPONSIBILITY

Whistleblowers may not suffer any form of retaliation. In fact, the law provides that those who make the report cannot be sanctioned, demoted, dismissed, transferred or subjected to another organizational measure that ends up having, directly or indirectly, negative effects on working conditions, or effects of discrimination or retaliation against them.

The reasons leading the person to report or denounce or publicly disclose are irrelevant for the purposes of their protection.

In the context of judicial or administrative proceedings, or even extrajudicial proceedings concerning the ascertainment of prohibited conduct against reporting persons, it is presumed that such conduct was put in place due to the reporting, public disclosure or complaint to the judicial or accounting authority. The burden of proving that such conduct towards whistleblowers is motivated by reasons unrelated to the reporting, public disclosure or complaint remains with the whistleblower.

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 offences and applying, in the absence of proof from the Company that the measure taken is unrelated to the reporting, an administrative pecuniary sanction.

Personal data processing - Confidentiality

Any processing of personal data will be carried out in accordance with Regulation (EU) 2016/679, Legislative Decree no. 196 of 30 June 2003 and Articles 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 use of the Software guarantees the complete confidentiality of the reporting party, as only the SB will be able to access the report.

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

The internal and external reports and the related documentation are kept for the time necessary for the processing of the report and, in any case, no later 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.

Responsibility of the whistleblower

The Company guarantees the reported party the right to be informed (within a reasonable period of time) about any reports involving him, guaranteeing the right to defence where disciplinary measures are initiated against him.

This procedure is without prejudice to the criminal and disciplinary liability of the whistleblower in the event of slanderous or defamatory reporting pursuant to the Criminal Code and art. 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 damaging the reported person or other subjects, and any other hypothesis of improper use or intentional exploitation of the procedure itself, are also a source of responsibility in the disciplinary and other competent bodies.

8. ENTRY INTO FORCE AND AMENDMENTS

The policy came into force on 17 December 2023. At the meeting of the Board of Directors on 30/09/2024, the update of the same was acknowledged for the implementation of the electronic reporting channel (Rev.2). With its entry into force, all the related provisions previously adopted on the subject, in any form communicated, must be considered repealed, if incompatible or non-conforming, as they are replaced by these.

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

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

However, this policy remains subject to periodic review.

Hausbrandt Trieste 1892 S.p.A.

INFORMATION ON THE PROCESSING OF PERSONAL DATA PURSUANT TO ARTICLES 13-14 OF REGULATION (EU) 2016/679 AS PART OF THE WHISTLEBLOWING POLICY

By means of this information notice, Hausbrandt Trieste 1892 S.p.A. (hereinafter the "Company") intends to provide the indications 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 framework of its "Whistleblowing Policy", adopted in accordance with Legislative Decree dated 10 March 2023 no. 24[4] and, in particular, of all the activities and obligations related to the operation of the company system for the management of *whistleblowing reports*.

The following information is provided to "whistleblowers" and all other potentially "interested parties", such as, for example, the persons indicated as possible responsible for illegal conduct, any "facilitators" (as defined by the relevant legislation), as well as any other person in a different capacity involved in the "Whistleblowing Policy".

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

The Data Controller is Hausbrandt Trieste 1892 S.p.A. - Via Foscarini, 52 31040 Nervesa della Battaglia (TV). Italy. The Data Controller has named a Data Protection Officer ("DPO"), which the interested party may contact by writing to the following address: dpo@hausbrandt.it

2. Personal data processed and purpose of process

According to the setting of the regulations in question, personal data may be acquired by the Company as they are contained in whistleblowing reports, or in the deeds and documents attached thereto, received by the Company through the channels provided for in the aforementioned Policy.

The reception and management of such reports may result, depending on their content, in the processing of the following categories of personal data:

a) common personal data referred to in art. 4, point 1, of the GDPR, including, for example, personal details (name, surname, date and place of birth), contact data (landline and/or mobile telephone number, postal/email address), job role/task;
b) "special" personal data referred to in art. 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 pursuant to art. 10 of the GDPR, relating to criminal convictions and crimes, or related security measures.

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

With regard to the aforementioned categories of personal data, **it is important that the reports forwarded are devoid of information that is manifestly irrelevant for the purposes of the reference regulation**, inviting in particular the reporting subjects to refrain from using personal data of a "particular" and "judicial" nature if not deemed **necessary and essential** for the purposes of the same, in compliance with art. 5 of the GDPR.

The aforementioned information will be processed by the Company – Data Controller – according to the provisions prescribed by Legislative Decree no. 24/2023 and, therefore, in general, **in order to carry out the necessary investigative activities aimed at verifying the substantiation of the facts subject to reporting and the adoption of the consequent measures**.

In addition, the data may be used by the Data Controller for purposes related to **defence needs or ascertainment of their 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 grounds for data processing

The legal basis for the processing of personal data is mainly constituted by the **fulfilment of a legal obligation** to which the Data Controller is subject - art. 6, par. 1, letter c) of the GDPR - which, in particular, by virtue of the aforementioned legislation, is required to implement and manage information channels dedicated to receiving reports of illegal conduct detrimental to the integrity of the Company and/or the public interest.

In the cases contemplated by the same regulation, a **specific and free consent** may be required **from the whistleblower** - pursuant to art. 6, para. 1, letter a) of the GDPR – and, in particular, where there is a **need to disclose their identity**, or where the **recording of reports collected orally**, by telephone or through voice messaging systems, or through direct meetings with the Reporting Manager, is envisaged.

The processing of **"particular"** personal data, possibly included in the reports, is based on the **fulfilment of obligations and the exercise of specific rights of the Data Controller and the data subject in the field of labour law**, pursuant to art. 9, par. 2), letter b) of the GDPR.

As for the purpose of ascertaining, exercising or defending a right in court, the relative legal basis for the processing of personal data is constituted by the **legitimate interest of the Data Controller** in this regard, referred to in art. 6, par. 1, letter f) of the GDPR; for the same purpose, the processing of personal data of a **"particular"** nature, if any, is based on art. 9, par. 2, letter f) of the GDPR.

4. The nature of the provision of your personal data

The provision of personal data is optional, pending the possibility of forwarding anonymous reports to the Company, where they present precise, concordant and adequately detailed information, without prejudice to the provisions of the legislation, in this case, regarding protection measures to protect the reporting party. If provided, 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. Methods of Processing and Period of Retention of Personal Data

The processing of personal data included in the reports submitted in accordance with the "Whistleblowing Policy" will be carried out by the subjects "appointed-authorized" by the Company and will be based on the principles of correctness, lawfulness and transparency, referred to in art. 5 of the GDPR.

The processing of personal data may be carried out in analogue and/or computer/ telematic ways, functional to store, manage and transmit them, in any case in application of appropriate measures, of a physical, technical and organisational nature, aimed at guaranteeing their **security and confidentiality at every stage of the procedure, including the filing of the report and the related documents** - without prejudice to the provisions of art. 12 of Legislative Decree no. 24/2023 - with particular reference to the identity of the whistleblower, the persons involved and/or in any case mentioned in the reports, their content and related documentation.

The reports received by the Company, together with the attached deeds and documents, will be kept for the time necessary to manage them and, in any case, as required by law, **for a period not exceeding five years from the date of communication of the related final results**. After this period, the reports will be deleted from the system

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

6. Areas of communication and data transfer

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

- suppliers of consultancy and assistance services in the implementation of the "Whistleblowing Policy";
- companies and IT professionals regarding the application of appropriate technical security measures and/or organisational information on the information processed by the company system.

If the details exist, personal data may be transmitted to the Judicial Authority and/or Police Bodies that request it in the context of judicial investigations.

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

Under no circumstance will the processed data be circulated.

7. Rights of the interested party

Each data subject has the right to exercise the rights referred to in articles 15 and following of the GDPR, in order to obtain from the Data Controller, for example, access to their personal data, the rectification or cancellation of the same or the limitation of the processing that concerns them, without prejudice the possibility, in the absence of satisfactory feedback, to lodge a complaint with the Guarantor Authority for the protection of personal data.

For the exercise of these rights, it is necessary to send a specific request in free form to the following address of the Data Controller: **info@hausbrandt.it** or transmit to the same address the form available on the website of the Guarantor Authority for the protection of personal data.

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

In these cases, the interested parties will in any case have the right to contact the Guarantor Authority so that the latter can assess whether the conditions for acting in the manner provided for in Article 160 of Legislative Decree no. 196/2003 are met.