

WHISTLEBLOWING - INFORMATION ON THE PROCESSING OF PERSONAL DATA

Pursuant to Articles 13 and 14 of the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”), TBS Crew S.r.l. (hereinafter also referred to as the “**Company**”), as the Data Controller, informs Whistleblowers (including any Facilitators), Reported Persons, and any individuals mentioned in a Report (“**Data Subjects**”) that the personal data provided in connection with the Reporting activities will be processed for the purposes of receiving, analyzing, investigating, and managing reports and any consequent actions, in compliance with the aforementioned regulation, Legislative Decree 196/2003 (as amended by Legislative Decree 101/2018), and Legislative Decree 24/2023.

A. Data Controller

The Data Controller is TBS Crew S.r.l., VAT No. 07310020966, with registered office in Piazza Cavour n. 3, 20121 - Milan, in the person of its *pro tempore* legal representative, and can be contacted by sending an e-mail to: privacy@tbscrew.com.

B. Categories of Personal Data Processed

The categories of personal data collected and processed include common type of data (personal data: name, surname, tax code, residential address, relationship with the company, and contact information: email address and/or phone number) necessary for the registration of a non-anonymous Report, common type data of individuals involved in the Report (e.g., name, surname, title), other data potentially contained in the Report and/or in the documentation provided by the Whistleblower for the purpose of the Report or otherwise necessary to verify the validity of the Report itself, as well as the voice of the person making the Report if he/she decides to use the voice messaging system available on the digital platform used.

In the case of anonymous reporting, the voice of the whistleblower, if captured through a voice message, will be appropriately masked and thus rendered unrecognizable.

In accordance with the principle of data minimization, only personal data necessary to satisfy the reporting request will be processed.

Special categories of personal data and judicial data should not be included in the Report by the user if not relevant to the subject of the Report. In any case, should such data be present, the Company will not use it, except where the processing is necessary for the ascertainment, exercise, or defense of legal claims and is authorized by law or by a decision of the Data Protection Authority or in any case by order of the Public Authority.

C. Purpose of Processing

The collection and subsequent processing of personal data are carried out to enable the Company to correctly and fully manage the investigation activities necessary to assess the validity of the Reports and take consequent actions regarding: (i) alleged violations of the Company's Code of Ethics and Organization, Management, and Control Model pursuant to Legislative Decree 231/2001 or of the procedural documentation adopted by the Company; (ii) unlawful conduct pursuant to Legislative Decree no. 231/2001.

The data may also be used to exercise or defend a right in judicial or extrajudicial proceedings, if this becomes necessary as a result of the Report, always in compliance with the confidentiality obligations under Article 12 of Legislative Decree 24/2023.

D. Legal Basis for Processing

The legal basis for the processing of the data related to the Report by the Data Controller can be found in the fulfillment of a legal obligation by the Data Controller (Art. 6, paragraph 1, letter c) of the GDPR).

The Whistleblower's consent is required by law to:

- record on a device suitable for storing and listening the voice of the Whistleblower who uses the voice message function to make the Report and/or to communicate with the Report Manager (i.e., the subject responsible for receiving and following up on the Report designated by the Data Controller) within the dedicated digital platform;
- reveal the identity of the Whistleblower and any other information from which such identity can be, directly or indirectly, inferred to persons other than the Report Manager.

The consent given can be revoked by the Whistleblower at any time, without affecting the lawfulness of the processing based on the consent given before the revocation.

Revocation of consent for voice messages must be communicated to the Report Manager via the platform's internal messaging system so that the procedure for inhibiting the listening of voice communications already transmitted can be activated.

E. Nature of Data Provision

The provision of data is mandatory for the registration of a non-anonymous Report and to verify the validity of the Report itself. In the absence of the provision of Whistleblower's identification data, the Report will be treated as an "anonymous" report and may be considered by the Report Manager only if adequately detailed and concerning potential serious illegalities or irregularities.

F. Methods of Personal Data Processing

The processing of data will be carried out exclusively for the aforementioned purposes with the support of paper and/or electronic tools, also automated with logic strictly related to the purposes and, in any case, in such a way as to guarantee the security and confidentiality of the data.

To ensure the confidentiality of the Whistleblower, of the persons involved or otherwise mentioned in the Report, of the content of the Report, and of the related documentation during all activities relating to the management of the Report, the identified process and communication channels established by the Company are implemented in such a way as not to make the aforementioned information and documentation accessible to persons other than those authorized (i.e., Report Manager and any other persons appointed for verification and investigation activities), also through the use of encryption tools.

It should be noted that the processing is not carried out through automated decision-making processes.

G. Extra-EU Transfer

The personal data processed are not transferred to countries outside the European Union.

H. Categories of Recipients of Personal Data

The personal data contained in the Reports are communicated and processed by the Report Manager designated by the Company and possibly by personnel belonging to certain company departments (e.g., Legal, Administration & Finance, etc.). Personal data may also be communicated to and processed for the above-mentioned purposes by external third parties appointed for verification and investigation activities (e.g., consultants, law firms, IT, investigative agencies, etc.) as well as by any competent Public Authorities, Judicial Authorities, Police Forces.

The aforementioned subjects processing personal data in the management of the Report:

- if internal to the Data Controller's organization, act as Authorized Processors, specifically instructed by the Data Controller to ensure the maximum confidentiality and protection of the data processed;

- if external to the Data Controller's organization, act as Data Processors pursuant to Article 28 of the GDPR, or as autonomous Data Controllers in the case of competent Public/Judicial Authorities or free professionals.

Moti-f s.r.l., the owner of the Secure Blowing IT platform for the management of Reports, as Data Processor acting on behalf of the Company, has implemented security measures to ensure the maximum confidentiality, integrity, and confidentiality of the personal data contained therein.

The Company makes available to the interested parties the list of the Data Processors, upon request via email to tbscrew@privacy.it.

Personal data identifying or making the Whistleblower identifiable are communicated to persons other than the Report Manager only with the Whistleblower's consent.

I. Data Retention Period

The personal data processed within a Reporting procedure are retained for the time necessary to process the Report and in any case for no more than five years from the date of the communication of the final outcome of the Reporting procedure, in compliance with confidentiality obligations, unless retention of personal data for a longer period is required for claim or litigation purposes, as a consequence of requests by competent authorities, or under applicable laws. Personal data not evidently useful for the processing of a specific Report should not be collected or, if accidentally collected, will be promptly deleted.

Personal data processed within a clearly unfounded or out-of-scope Reporting procedure will be deleted one (1) year after the Report's filing.

J. Data Subject Rights

Pursuant to Articles 15-21 of the GDPR, Data Subjects - where applicable and within the limits specified below - have the following rights with respect to the Company:

- the right to obtain access, updating, correction, or integration of their personal data;
- the right to limit the processing in the cases indicated in Article 18 of the GDPR;
- the right to obtain the deletion of data, where the latter are no longer necessary for the purposes for which they were collected. Deletion cannot be carried out if processing is necessary for compliance with a legal obligation, the performance of a task carried out in the public interest, or the establishment, exercise, or defense of legal claims;
- the right to data portability, i.e., the right to receive all personal data concerning them in a structured, commonly used, and machine-readable format;
- the right to withdraw consent at any time, provided that the processing is based on consent, without affecting the lawfulness of the processing based on the consent given before the withdrawal;
- the right to object to the processing of personal data concerning them, specifying the reasons justifying the objection to processing under Article 21 of the GDPR.

Such requests can be addressed to the Company by sending a registered letter with return receipt to Piazza Cavour, 3 - 20121 Milan or by sending an email to: privacy@tbscrew.com.

It is understood that, if the Data Subject believes that the processing concerning them violates the GDPR, they have the right to lodge a complaint with a supervisory Authority (in the Member State where they usually reside, in the one where they work, or in the one where the alleged violation occurred). The Italian Supervisory Authority is the Data Protection Authority, located at Piazza Venezia n. 11 - 00187 - Rome (<http://www.garanteprivacy.it/>).

Pursuant to and for the effects of Article 2-undecies, first paragraph, letter f) of Legislative Decree 196/2003 as amended, and Article 23 of the GDPR, the rights mentioned above (Articles 15-22 GDPR) cannot be exercised by the Reported Persons, or their exercise may be delayed or limited, if the exercise of such rights could result in actual and substantial prejudice to the confidentiality of the identity of the Whistleblower.

The Reported Person will receive a reasoned and timely communication from the Data Controller regarding the limitation, delay, or exclusion of the exercise of their right, unless the communication may compromise the very purpose of the limitation. The Reported Person can exercise their rights also through the Data Protection Authority according to the methods described in Article 160 of the Legislative Decree 196/2003. In such a case, the Authority informs the Data Subject of having performed all necessary checks or conducted a review, as well as of the right of the Data Subject to bring a judicial appeal.

This Whistleblowing Privacy Policy may be subject to changes. Therefore, it is advisable to regularly check the policy available on the 'Secure Blowing' platform accessible from the 'Whistleblowing' section on the website www.theblondesalad.com.