

WHISTLEBLOWING PRIVACY POLICY

Information on the processing of personal data performed in the context of the management of whistleblowing reports.

ZEPHYR GROUP SRL provides, below, information on the processing of personal data of whistleblowers (where identified or identifiable), of those reported and of any other third parties involved ("Data Subjects"), performed in relation to the management of Whistleblowing reports pursuant to Italian Legislative Decree 24/2023, in the manner provided for by the Whistleblowing Policy of ZEPHYR GROUP SRL .

For anything not indicated here, for ZEPHYR GROUP SRL employees, reference is also made to the information provided to them in relation to the employment relationship.

ZEPHYR GROUP SRL invites careful reading of the information at the points indicated below and of the document called "Whistleblowing Policy", made available on the website <https://www.zephyr-group.eu/>

1) What data is processed?

The personal data being processed are those provided by the "whistleblower" through the internal reporting channel defined as the WB platform accessible at the following link: <https://whistleblowing.varhub.it/Whistleblowing?code=ZEPHYRGROUPSRL>

which offers two possible ways of submitting a report :

Anonymous Mode : Anonymous Reporting

Signed Mode : Signed Reporting

In anonymous mode, there is no provision for the collection of any personal data of the whistleblower. We therefore invite the whistleblower to take the utmost care to avoid

entering, in the fields of collection of information relating to the report, personal data that could in any way refer to their identity and, consequently, to their identification.

In all cases ZEPHYR GROUP SRL guarantees the confidentiality of the identity of the whistleblower from the receipt of the report in compliance with the applicable legislation on the subject.

ZEPHYR GROUP SRL encourages the whistleblower to only provide information based on facts strictly related to the subject of the report. Please avoid the disclosure of particular personal data, known as "sensitive" data (such as race, ethnic origin, political opinions, religious beliefs, trade union membership, health or sex life data). In the event that the report contains such "sensitive" data, they will be promptly deleted by the contact person if deemed irrelevant or not necessary for the verification and assessment phases, in order to prevent further processing.

The personal data being processed fall into the following categories:

Personal data of the reporting person in the event of reports made in the signed, non-anonymous manner, through the dedicated platform:

Common Data:

Mandatory: First Name, Surname, e-mail address

Optional: telephone, date of birth, place of birth, address, details of an identification document and other personal data processed because it is voluntarily communicated by the reporting person by filling in the forms provided in the reporting form.

Personal data relating to the person(s) involved in the report:

The data that the reporting person intended to provide to represent the facts described in the report.

It should be noted that, in this circumstance, ZEPHYR GROUP SRL is not able to predefine in advance the data included in the report. This implies the possibility that the report may contain information falling into specific categories within the meaning of article 9 of the GDPR, such as criminal convictions, offences, health conditions, political opinions, etc.

It is also stated that the data included in the report must not be subject to national defence secrecy, medical secrecy, secrecy of judicial deliberations, judicial investigations or secrecy of investigations or professional secrecy.

Theafore-mentioned data will be processed with computer and paper-based media that guarantee their security and confidentiality. Documentation in paper-based format will be limited to the minimum necessary, and where necessary archived and stored in cabinets and rooms fitted with security locks.

Transmission of the data provided by the reporting person through access to the platform is managed with HTTPS protocol.

Encryption techniques based on the AES Algorithm are also applied and all data is fully encrypted, thus guaranteeing the confidentiality of the information transmitted.

Cookies are not used to transmit personal information, nor are persistent cookies used to track users. Only technical cookies are used to the extent strictly necessary for the correct and efficient use of the platform. Use of session cookies (which are not stored persistently on the user's computer and disappear when the browser is closed) is strictly limited to the transmission of session identifiers (consisting of random numbers generated by the server) necessary to allow safe and efficient browsing of the reporting platform. (e.g. in the case of presentation according to the web model of personal data, e-mail or telephone number, division and those that may already be available to the Data Controllers referred to in point 3 below) or that they collect as part of the verification of the validity of the reports and in any related investigation, always in compliance with the relevant regulatory provisions.

All data not necessary for the management of the report is deleted.

Special categories of data may also be processed (among other information that may reveal religious beliefs, political opinions, membership of parties, trade unions, etc.) or judicial data or personal data relating to criminal convictions and offences. These data will only be used if strictly necessary for management of the Whistleblowing report, in full compliance with the principles of proportionality and necessity and, if deemed irrelevant for the purposes of the report, will no longer be subject to further processing.

2) For what purposes?

The purposes of the processing and the legal basis underlying it.

The processing is aimed at receiving, analysing, investigating and managing reports and any consequent actions, and in particular at ascertaining the reported facts and at adopting any measures. Pursuant to art. 6, paragraph 1 letter f) of European Regulation no. 679/2016 GDPR, all personal data collected in the context of this processing are strictly functional and necessary for the pursuit of the provisions of Italian Legislative Decree no. 24/2023, as well as for any needs of internal control, monitoring of corporate risks, defence of a right in court or for further legitimate interests of the Data Controller.

In addition, the personal data collected may be processed to comply with requests received from the competent administrative or judicial authority and, more generally, from public entities in compliance with the legal formalities.

In addition, your personal data will be processed whenever necessary to ascertain, exercise or defend a right in court or a legitimate interest of the Data Controller in any competent Court.

Legitimate interests of the Data Controller

The Data Controller may process your personal data without your consent in the following cases: in order to perform internal checks to ascertain the possible committing of illegal acts of which the Company should become aware, also through reports, in compliance with the regulations and internal policies of the Company and according to the principles established by the legislation on the protection of personal data and labour regulations, as well as the related internal reporting. For fraud prevention in order to increase the protection of personal data, through the optimisation and efficiency of internal processes.

It is understood that only the data collected for the purposes indicated above, where appropriate with respect to these purposes,

will be processed in the most aggregated/anonymous form.

The Data Controller ensures that the processing of your Personal Data will take place in compliance with the Relevant Principles in terms of Privacy and Data Protection and, in particular, the principles of necessity,

proportionality, relevance and non-excess, as governed by the data protection law.

In application of the afore-mentioned principles, ZEPHYR GROUP SRL, in order to manage Whistleblowing Reports, will generally choose the methods least detrimental to the rights of the data subject, preferring the omission of any personal data in the documents, where the need for investigation can be achieved without

involving the processing of personal data.

3) Data Controllers

The data controllers of personal data is ZEPHYR GROUP SRL, with registered office in LA SPEZIA

Within ZEPHYR GROUP SRL, personal data or those from which identity is detected may be known and processed by the "Internal Control Officer", a person appointed by ZEPHYR GROUP SRL and subject to its authority, and, only in the cases expressly provided for by Italian Legislative Decree 24/2023, by the competent authorities, by the Supervisory Body 231 and by the Board of Statutory Auditors. In any case, the personnel appointed to perform the processing operate under the authority of ZEPHYR GROUP SRL and receive from it appropriate written instructions to ensure the correctness of the processing.

4) To whom can we communicate the data?

For the pursuit of the afore-mentioned purposes, the personal data provided are made accessible only to those who, within the Company, are competent to receive or follow up on the analysis, investigation and management of reports and any consequent actions. These subjects are properly instructed in order to avoid loss, access to data by unauthorised subjects or unauthorised processing of the data and, more generally, in relation to personal data protection obligations. The data may also be processed by

external Consultants and Third Parties with technical functions (for example, the provider of the IT platform), who act as Data Processors/Sub-Processors and have signed a specific contract that duly regulates the processing entrusted to them and the obligations regarding data protection and security of processing pursuant to art. 28, paragraph 3 of the Regulation.

As an indication, the subjects indicated above can be included in the following categories:

a) Consultants and other external service providers strictly related to the purposes of the processing

(Exercise of information systems dedicated to this, Organisation, Litigation, Legal Studies, etc.),

b) Companies in charge of personnel administration and management,

c) Institutions and/or Public Authorities, Judicial Authorities, Police Bodies, Investigative Agencies.

d) Other companies of the group to which ZEPHYR GROUP SRL BELONGS

The identity of the reporting person and any other information from which such identity may be derived, directly or indirectly, may be disclosed to persons other than those competent to receive or follow up on reports only with the express consent of the reporting person in accordance with the provisions of Italian Legislative Decree no. 24/2023.

In the event that reports relating to another ZEPHYR GROUP SRL GROUP Company are received by ZEPHYR GROUP SRL, they will be addressed to the relevant Company, which will operate as an independent Controller.

Any contact details provided by the reporting person will be used in the event that direct contact with them is necessary and for updates regarding the status of the report.

5) How and for how long do we process the data?

The reports and the related documentation are kept for the time necessary to process the report for the duration of the verification procedures and for any subsequent events, also for litigation purposes and in any case no later than five years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations. If out-of-scope reports/complaints are received (for example disputes, claims or requests linked to a personal interest of the reporting person, communications or complaints relating to commercial activities or services to the public), they are retained for a period not exceeding 8 months from their archiving.

The data will not be transferred to parties with offices in third countries outside the EU

The acquired data will be processed and stored for a period of time not exceeding that necessary

for the purposes for which the data were collected or subsequently processed, for the duration of the verification procedures and for any subsequent events, including litigation, and subsequently stored within the limitation period and in compliance with the legal obligations and privacy procedures in force in the Company. In the event that the report is filed, the data are deleted within the period indicated by the "Whistleblowing Policy" (point 5) unless further processing is necessary in the event of unfounded reports submitted with intent or gross negligence, for the performance of activities, including disciplinary activities, indicated by the Policy.

6) What are the rights of the data subjects?

Data subjects have the right to request access to their personal data, the correction and deletion thereof, limitation of the processing that concerns them as well as to object to the same processing, on the basis and within the limits of the provisions of arts. 15-22 of EU Regulation no. 679/2016. With respect to any processing based on consent, the latter may always be revoked, without prejudice to the lawfulness of processing based on consent given before revocation.



ZEPHYR

A ZEPHYR GROUP COMPANY

Data subjects also have the right to lodge a complaint with the Guarantor for the protection of personal data, in the forms provided for by Italian Legislative Decree no. 196/2003.

Pursuant to the provisions of art. 2-undecies of Italian Legislative Decree no. 196/2003, the afore-mentioned rights cannot be exercised with a request to the data controller, or with a complaint pursuant to art. 77 of the Regulation, when the exercise of these rights may result in an effective and concrete prejudice to the confidentiality of the identity of the employee who has made the report, pursuant to Law of 30 November 2017 no. 179, of an offence of which they have become aware by reason of their office.

7) Who can be contacted?

For the purposes of exercising the rights referred to in paragraph 6 above, as well as for any clarifications, you can contact the privacy holder directly by sending an e-mail to the following address: **privacy@zephyr-group.eu**