

This policy is targeted at whistleblowers, individuals who assist whistleblowers in the reporting process (the so-called facilitators) and, finally, individuals to whom the informative content of the report may refer in their capacity as reported persons, who are somehow involved in the reported facts.

To this end **Società Agricola Giorgio Tesi Vivai S.S.**, in its capacity as *Data Controller*, informs, pursuant to articles 13-14 of the General Data Protection Regulation (UE) 2016/679 (hereinafter also referred to as "GDPR"), that the personal data acquired in the context of the reporting management process shall be processed with the following methods and for the following purposes.

	The Data Controller is Società Agricola Giorgio Tesi Vivai S.S., Via di Badia 14 51100 Pistoia
Data Controller	You can contact the Data Controller by e-mail at the following address: privacy@giorgiotesigroup.it
	The following types of personal data may be subject to processing:
Type of processed data	<ul style="list-style-type: none">– identification data and contact details of the whistleblower;– identification data of the persons involved in the reporting, information and data related to the reported breaches, including any personal data related to specific categories or criminal convictions and crimes;– any other information related to the whistleblower, or to the persons involved in the reporting to any other third party, which the whistleblower decides to share to better describe the alleged breach;– identification data, contact details and information related to the IT platform login account of the persons in charge of managing the reports.
Processing method	<p>The personal data shall be mainly processed through a specific IT platform, "Whistleblowing Software", which provides for the possibility of both a written and an oral reporting. In this latter case, the whistleblower's voice shall be distorted to ensure security and anonymity.</p> <p>Reports may also be managed by means of a direct meeting with the "Report Management Structure", which shall arrange for the meeting to be documented through the meeting minutes or, with the whistleblower's prior agreement, for it to be recorded on a suitable device for retention and listening purposes.</p>
Data source and nature of data provision	<p>The personal data subject to processing are those provided by the whistleblower and those that may be independently collected during the preliminary investigations, which are required to establish the circumstances of the report.</p> <p>Data provision is necessary and functional to the management of the reports received, according to the forms and methods outlined in the <i>Report management process (whistleblowing)</i>.</p>
Purpose of processing	Personal data shall be collected and processed for the purposes of breach reporting management, related to the national and European legislation on the relevant sectors and interests for the European Union, with the methods and instruments outlined in the <i>Report management process (whistleblowing)</i> .
Legal basis	Data processing comes from the need to apply the provisions of the Italian legislative decree 24/2023.

Data retention time

The reports and related documentation are retained for the time needed to process the report and, anyway, for no longer than five years from the date of notification of the final outcome of the reporting process, in full compliance with the whistleblower's confidentiality obligations. Any personal data that isn't demonstrably useful to the report assessment shall be promptly deleted.

Personal data shall be processed by the Report Management Structure, i.e., the company Siquam, located in Via Marco Polo 72, 56031 – Bientina (PI) – Italy, in its capacity of Data Processor. In full compliance with the provisions of the regulations in force and the report management process, the Data Processor shall ensure the confidentiality of the whistleblower's identity and the information coming to his/her knowledge.

Recipients of personal data

The whistleblower's identity, or any other information from which such identity may be directly or indirectly inferred, can be disclosed only with the whistleblower's explicit consent. When necessary for the purposes of the preliminary investigations, some information related to the report may be processed by other functions within the Company to which specific instructions were provided, such as the Company's internal area managers or CEO in case of conflict-of-interest events.

The IT platform for report management is managed by the company Ablex S.r.l., located in Via Giacosa 38 – 10122 Torino (TO), appointed as the Data Processor. The platform encryption system doesn't allow the above-mentioned Data Processor to access the whistleblower's identity or the content of the reports.

Finally, some data may be transmitted, in the cases provided for by the law, to the judicial authority and/or regulatory authorities.

As regards the data, in the cases provided for by the law, the interested parties may exercise the rights referred to in Chapter 3 of the GDPR.

In particular, the whistleblower may have the right to access his/her data, to amend or supplement such data, to delete or limit the processing of such data and to withdraw his/her consent, with the same methods used for reporting.

Rights of the interested parties

Furthermore, pursuant to article 77 of the GDPR, the whistleblower may raise a complaint to the Italian Data Protection Authority, if he/she considers that data processing breaches the above-mentioned Regulation.

Please be informed that the exercise of such rights by other interested parties, such as the reported persons or other persons involved, may be delayed, limited or excluded in case such exercise concretely and effectively affects the confidentiality of the whistleblower's identity, as provided for by article 2-undecies, f) of the Privacy Code (pursuant to article 23 of the GDPR). In such cases, the above-mentioned rights may be exercised through the Italian Data Protection Authority, with the methods referred to in article 160 of the Privacy Code.