

Information on the processing of personal data pursuant to Articles 13 and 14 of the Regulation (EU) 679/2016 ("GDPR")

This information on the processing of personal data is provided, pursuant to and for the purposes of Articles 13 and 14 of the GDPR, to all persons who report unlawful conduct of which they have become aware or witnessed, as part of their relationship with Savio Macchine Tessili S.p.A. The notice, therefore, applies whenever a report is made through one of the methods indicated in the Whistleblowing Regulations.

Data Controller

The Data Controller is Savio Macchine Tessili S.p.A. with registered office at 33170 Pordenone, via Udine 105 ("**Data Controller**"), who can be contacted at odv.saviospa@legalmail.it.

Personal data

The following data may be subject to processing: (i) common personal data of whistleblowers and any facilitators (e.g., first name, last name, contact information); (ii) personal data contained in reports (including, where applicable, data belonging to special categories under Art. 9 GDPR and personal data relating to criminal convictions and offenses under Art. 10 GDPR).

Sources of personal data

The data subject to processing may be communicated directly by the whistleblower with his or her report and through any subsequent contact with the Data Controller in the person of the Whistleblowing Manager (authorized for processing), or may be collected by the latter from third parties - internal or external - from public databases, other freely accessible sources, online and offline, and in general from any other source suitable to allow the necessary verifications to be carried out for the management of the report, in accordance with the provisions of the Whistleblowing Regulations.

Purpose and legal basis of processing - data retention period:

Purpose 1: To execute the reporting procedure adopted pursuant to Law No. 179 of November 30, 2017 (setting forth "Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship") and, therefore, with the purpose of carrying out the necessary investigative activities aimed at verifying the merits of the fact being reported and the adoption of the consequent measures. Moreover, the adoption of an internal reporting channel constitutes an obligation for the Data Controller under Legislative Decree No. 24 of March 10, 2023, which transposes and implements in Italy Directive (EU) 2019/1937.

Legal basis for processing: processing is necessary for the fulfillment of legal obligations.

Period of data retention: for the time necessary to process the report. In any case, the data are kept for the period of time necessary for the processing of the reports and in any case not more than 5 years from the communication of the final outcome of the reporting procedure in compliance with the confidentiality obligations under Article 12 of Legislative Decree No. 24/23. Data collected, if manifestly unnecessary or excessive for the processing of the report, will be immediately deleted by the Data Controller.

Purpose 2: Judicial protection purposes, to prevent or prosecute wrongdoing.

Legal basis for processing: the legitimate interest of the Data Controller to protect its rights and prevent

wrongdoing.

Period of data retention: without prejudice to the above, in the event of a judgment, data may be processed for defensive purposes until the judgment/judgment becomes final. Data collected, if manifestly unnecessary or excessive for the processing of the report, will be immediately deleted by the Data Controller.

Nature of data disclosure and consequence of non-disclosure

Anonymous reports that are not sufficiently substantiated will not be taken into consideration by the Whistleblowing Manager and, in any case, will be treated as ordinary reports with the consequent application of the relevant regulations, it being understood that the anonymous reporter, subsequently identified, will be able to benefit from whistleblowing protection following the communication to ANAC of any retaliatory measures suffered. Therefore, in order to enjoy Whistleblowing protection immediately, the provision of the whistleblower's data is mandatory.

The provision of the data contained in the report is necessary so that the report can be received, verified and processed.

Method of processing

Data are processed using computer and paper media that guarantee their security and confidentiality. Documentation in paper format is limited to the minimum necessary and stored and kept in cabinets and rooms equipped with security locks. Transmission of data provided by the reporting person through access to the platform is handled with HTTPS protocol. End-to-end communications between whistleblower and Whistleblowing Manager are further all protected using RSA-2048 asymmetric encryption.

No cookies are used to transmit personally identifiable 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. The use of session cookies (which are not stored persistently on the user's computer and vanish when the browser is closed) is strictly limited to the transmission of session identifiers (consisting of random numbers generated by the server) necessary to enable the safe and efficient exploration of the platform.

Personal data will be processed by individuals identified and specifically authorized and instructed in accordance with Art. 29 GDPR, 32 para. 4 GDPR and Art. 2 quaterdecies of the Privacy Code (Legislative Decree No. 196/2003).

Recipients or possible categories of recipients of personal data

For one or more of the above purposes, data may be shared with the following parties:

- service providers
- Judicial Authority

With the exception of the Judicial Authority, the aforementioned entities process data under a specific agreement on the processing of personal data pursuant to Article 28 GDPR, as data processors. You can receive the updated list of data processors at any time by contacting the Data Controller at the above addresses.

Transfer of personal data to a third country

Data will be processed and stored at the Data Controller's offices or at the systems of the Data Controller's

suppliers, who act as data controllers processors to agreements in accordance with Art. 28 GDPR, in Italy and within the European Union.

Rights of the person to whom the data refer

We inform you that, as a Data Subject, pursuant to Articles 15 to 22 of the GDPR, you have the right to:

- (a) request access, rectification, deletion, and restriction of the data concerning you;
- (b) object to the processing of his/her data;
- c) obtain data portability, i.e., receive data from the Data Controller in a structured, commonly used, machine-readable format and transmit it without hindrance to another data controller, including by direct transmission of the data, if technically feasible;
- (d) revoke consent to the processing of data, if it constitutes the legal basis for the processing. In this case, the data processing carried out before revocation remains lawful;
- (e) to lodge a complaint with the competent supervisory authority;
- (f) to request information regarding: the purposes of the processing; the categories of data; the recipients or categories of recipients to whom the data have been or will be disclosed, in particular if the data are transmitted to recipients in third countries or international organizations; the data retention period; if the data are not collected from the data subject, all available information on their origin.

You may exercise the aforementioned rights by writing to the Data Controller's address indicated above.

The exercise of these rights may be subject to limitations in the cases provided for in Article 2-undecies of Legislative Decree 196/2003, as amended - most recently - by Legislative Decree 24/2023.

We also inform you that, as a data subject, you have the right to lodge a complaint pursuant to Article 77 GDPR to the Guarantor Authority for the Protection of Personal Data, as the supervisory authority.

Pordenone, 18/12/2023

Signature of the Data Controller

A handwritten signature in black ink, appearing to read 'Daniel Ranta', written in a cursive style.