Personal data privacy policy.

1 Preamble

Marsilli acknowledges the importance of the right to data protection. In an increasingly interconnected world, with growing challenges related to information management, respect for privacy becomes crucial to establishing a relationship of trust with stakeholders. This Privacy Policy (hereinafter also the "Policy") is intended as a tangible commitment to ensure that personal information is protected in accordance with applicable laws and regulations. It defines the principles that guide the Group in collecting, recording, organizing, storing, modifying, extracting, consulting, using, communicating, disseminating, deleting or destroying personal data in accordance with the laws of the countries where Marsilli operates, establishing the minimum protection criteria for personal data protection.

2 Regulatory framework.

This Policy, in addition to the principles described in the Marsilli Code of Ethics and EU privacy legislation, is also inspired by those found in the international legislation indicated below:

- Universal Declaration of Human Rights (1948): In particular, article 12.
- The OECD Guidelines on the protection of privacy.

3 Recipients and field of application

This Policy is adopted by all the companies of the Marsilli Group. Recipients are company's highest administrative bodies and all the bodies and individual subjects who make up the hierarchical chains that govern the organizational structures. They are required, without any exception, to apply the principles set out below, due to the importance that each individual area assumes in the specific business activity, to the legislation in force and the operational limits in the countries in which the individual companies operate.

Given the specific nature of the subject matter of this Policy, it is vital to emphasise that each company of the Group is designated as the autonomous controller of the personal data collected. This is aimed at ensuring that data protection responsibilities are clearly defined and at fostering transparency in handling personal information. Each entity is therefore required to comply with the privacy laws and regulations applicable in the countries where it operates, and to implement appropriate data protection security measures in accordance with the most appropriate standards. That being said, this Policy is therefore to be understood as a set of principles of minimum protection, applicable by each company of the Group, regardless of the law in force in the country where it is based.

4 Adoption of Principles.

4.1 DEFINITIONS AND PRINCIPLES FOR THE MANAGEMENT OF PERSONAL DATA COLLECTED.

"**Personal Data**" is defined as information that directly or indirectly identifies or make a natural person identifiable and which may provide information on his or her characteristics, habits, lifestyle, personal relationships, health, economic situation, etc.

Examples of personal data are: first name, surname, home address, telephone number or vehicle registration number, fiscal code, e-mail address, as well as data contained in personal documents (e.g. medical certificate, first payslip, certificate of qualification, tax return, etc.) and any other information attributable to a natural person, whether identified or identifiable.

"Processing" of personal data refers to a process involving the collection, use, storage and deletion of information about a natural person.

"Controller" is defined as the natural or legal person who decides on the purposes and means of processing personal data.

A **"data subject"** is the natural person to whom the personal data refers.

The basic principles to be observed when processing data are:

- Legality and Transparency.
- Minimisation of the Data collected and retention periods.
- Integrity and Confidentiality.
- Protection of the Data Subject's Rights.

4.1.1 Legality and Transparency.

Personal data must be processed in accordance with the privacy laws applicable in the country where the data controller is based. However, personal data must only be collected for legitimate and explicit purposes, and processed consistently with those purposes. The purposes of data collection must be clearly communicated to data subjects and their consent must be obtained when required by applicable laws.

4.1.2 Minimisation of the Data collected and retention periods.

Personal data must be obtained avoiding excessive or unnecessary collection and must be retained only as long as necessary to fulfill the purposes for which it was collected. This in compliance with the data retention periods laid down by the applicable laws and ensuring its secure deletion at the end of the retention period.

4.1.3 Integrity and Confidentiality.

Sharing of personal data with third parties will be limited to the stated purposes of collection and in compliance with the applicable laws. When personal data is shared with third parties, appropriate security and confidentiality measure shall be implemented as far as possible and in accordance with applicable law. Technical, physical and organisational measures must therefore be taken to prevent unauthorised access, unlawful processing and loss, destruction or damage, resulting from intentional or accidental acts, of personal data.

4.1.4 Protection of the Data Subject's Rights.

The data subject's rights regarding personal data must be implemented and protected. These rights include the right to information, to access, to rectification and to deletion or oblivion in certain circumstances. In addition, the data subject shall have the right to object the processing of their personal data on legitimate grounds or to restrict its processing.

5 Implementation and supervision.

The implementation of the Policy is delegated to the Management of the individual companies that compose the group, in the people that work in them, at various levels. Supervision of compliance with the principles established by this Policy is entrusted, for Italian companies, to the Supervisory Bodies of the individual companies, where present; while for non-Italian ones, or those without a Supervisory Body, this function is carried out by their highest administrative body or by other specifically appointed control body. Anyone is authorized to report violations to this Policy of which they become aware. For Italian companies, the reports will be addressed to the Supervisory Bodies of the individual companies, where present, while for non-Italian ones, or those without a Supervisory Body, the reports will be sent to Supervisory Body of Marsilli S.p.A. The competent Supervisory Body is responsible for investigating the validity of the report listening, if necessary, to the reasons of the reporting person and the person responsible for the reported violation and to report on the matter according to what is defined in the operating regulations of the Supervisory Body itself. For non-Italian companies or for those without a Supervisory Body, this function is performed by the highest administrative body or by another control body specifically appointed, on impulse from the Supervisory Body of Marsilli S.p.A.

6 Policy revision and Performance indicators (KPI).

Marsilli integrates the principles of this Policy into its own management model and, aware that other issues may become relevant over time, undertakes to update it annually in view of its adequacy and effectiveness of implementation. In order to monitor the implementation of the Policy, Marsilli undertakes to identify a number of indicators (KPI) and to measure their progress on an annual basis.