VERONALAMIERE
Technology Service Partner

Privacy Organisation Model
(Privacy Policy)

Summary version

Rev. 02 – November 2023

VERONA LAMIERE S.P.A.
Via G. Pascoli, 46 - S.S. 434 - Km 9
37059 Campagnola di Zevio, VR - IT
T +39 045 8738311
F +39 045 8739329
P. IVA 02079100232
www.veronalamiere.it

1. PURPOSES AND DEFINITIONS

Verona Lamiere S.p.A. has adopted guidelines to deal with legal obligations concerning the protection of personal data in a structured manner, to achieve the best results in protecting the information and data processed within the scope of its activities from all internal or external threats, whether intentional or accidental, in accordance with the provisions of European Union and national legislation

The purpose of this document and those related to it (stored at the company) is to define the Privacy Organisational Model (Privacy Policy), i.e. identify the strategies, general guidelines and internal regulations governing the processing of personal data by Verona Lamiere S.p.A., pursuant to the GDPR - General Data Protection Regulation.

The privacy policy (policy) resulting from this Organisational Privacy Model applies to the company as a whole, to all bodies and structures at any organisational or functional level.

Application is mandatory for all personnel and must be included as an integral part of the regulation of any agreement with all external parties involved in the processing of information falling within the scope of the Privacy Management System (PMS).

Verona Lamiere S.p.A. is committed to guaranteeing and demonstrating that personal data is processed in compliance with the provisions of the law and, according to the following legal principles, namely:

- processed in a lawful way that is fair and transparent for the data subject;
- collected for specified, explicit and legitimate purposes, and subsequently processed in a way that is not inconsistent with those purposes;
- adequate, relevant and limited to the extent required for the purposes for which the data is processed;
- accurate and, if necessary, up-to-date; in this regard, reasonable measures are taken to promptly delete or rectify data that is inaccurate for the purposes for which it is processed;
- kept in a way that makes it possible to identify the data subjects for a period of time not exceeding the purposes for which the data is processed;
- processed in a way that ensures adequate security of personal data, including protection, through appropriate technical and organisational measures, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

These indications apply not only to the processing of personal data for which the company Verona Lamiere S.p.A. is the Data Controller, but also to all processing operations for which the company is appointed as Data Processor by other Data Controllers, unless more restrictive measures on the protection of personal data are contained in the documents governing relations with the Data Controller.

Since similar guarantees of protection and the adoption of adequate security measures are required from third parties to which the company Verona Lamiere S.p.A. entrusts the task of Data Processor, this policy is made available to such Data Processors.

2. INFORMATION SECURITY

The information assets to be protected consist of all the information processed in the performance of company procedures, with respect to which the company ensures integrity and protection and allows access only to the necessary and previously authorised roles and functions. In order to always achieve

regulatory compliance and increase control capacity, the company has established and keeps an updated processing activity register.

When deemed necessary by the results of the personal data processing risk analysis, the company identifies additional security requirements through the data protection impact assessment, which provides an additional level on awareness of the degree to which the company's data management systems are exposed to threats.

The risk assessment, carried out on all existing or planned processing operations, makes it possible to assess the potential consequences and damage that may result from the non-application of security measures to the information system and to the entire organisation in general, as well as to indicate the likelihood that the identified threats will be actually implemented. The results of this assessment determine the actions necessary to identify the correct and adequate security measures and mechanisms to guarantee the protection of personal data. Information security management is based on a number of essential general principles, which are set out below:

- There is a regularly updated list of company information management assets, and a manager is identified for each of them;
- Information is classified according to its level of criticality, so that it is managed with consistent and appropriate levels of confidentiality, integrity and availability;
- Access to information systems is subject to an identification and authentication procedure. Furthermore, information access authorisations are differentiated according to the role and duties of individuals, so that each user can access only the information needed, and these authorisations are periodically reviewed;
- Procedures are defined for the safe use of assets (locations, means of transport, tools) and company information;
- Full staff awareness of information security issues is encouraged;
- To prevent or as a minimum promptly deal with incidents, everyone is required to be part of the company's security system and must therefore notify any security-related problems of which they are aware;
- Unauthorised access to the premises and equipment where the information is managed must be prevented;
- Compliance with legal requirements and information security principles in contracts with third parties is ensured;
- A continuity plan is provided to ensure that the company can effectively cope with an unforeseen event, guaranteeing the recovery of critical services in a timely way and in a way that limits negative consequences on the company's business mission. Security features are included in all design, development, operation, maintenance, support and decommissioning phases of IT systems and services;
- Compliance with the provisions of the law, statutes, regulations or contractual obligations and any information security requirements is ensured, minimising the risk of legal or administrative sanctions, significant losses or reputational damage.

3. CONFIDENTIALITY OF INFORMATION

Verona Lamiere S.p.A. undertakes to guarantee the confidentiality and privacy of the information and data of data subjects obtained in the course of its activities in accordance with the internal procedures provided for, which are consistent with this Privacy Organisational Model.

Data may be processed using manual, computerised and electronic instruments suitable for storing, processing, managing and transmitting the data in compliance with the security measures provided for all persons in any way involved in the processing of personal data, irrespective of compliance with the obligations under the code of ethics concerning the profession that may be regulated in the execution of their duties, are bound to confidentiality as provided for in Article 2407 of the Italian Civil Code.

The company undertakes to guarantee adequate minimum security levels for information made available by third parties with the same diligence and level of protection used for the security and confidentiality of its own data.

4. POLICY IMPLEMENTATION

The following are required to comply with and implement the privacy policy (policy) stemming from this Organisational Privacy Model:

- all personnel who, for whatever reason, collaborate with the company and are in some way involved with the processing of data and information falling within their field of competence. In fact, the staff is liable, each to the extent of his or her competence, to report all anomalies and violations he or she may become aware of;
- all external parties who have relations and collaborate with the company and who must ensure compliance with the requirements contained in the privacy policy (policy);

Company personnel who intentionally or negligently disregard established security rules and thereby cause damage may be prosecuted in the appropriate courts, in full compliance with legal and contractual constraints.

5. MONITORING OF THE PRIVACY MANAGEMENT SYSTEM

Management reviews the effectiveness and efficiency of the Privacy Management System at least once a year, so that adequate support can be given for the introduction of all necessary improvements and to encourage the activation of a continuous updating process.

The Data Controller, as the person responsible for the Privacy Management System (PMS), is in charge of operationally reviewing this policy.

The result of the entire periodic review process includes all decisions made and actions taken regarding the improvement of the Privacy Management System (PMS).

6. INFORMATION AND TRAINING

The objective of guaranteeing correct data processing, in compliance with the requirements of the regulations, is also and above all achieved by the company through special attention to training and awareness of the management of privacy issues.

For this purpose, the Privacy Organisational Model is disseminated to the personnel already employed and, where new human resources are included into the workforce, as soon as they join the company. Any updates are disseminated for the purposes of gaining knowledge and using the tools deemed most effective each time.

Training is adapted to the personal data processing system and according to the criticality of processing performed by the human resource being trained.

The company recognises its liability under applicable law and is committed to protecting the personal data that users entrust to the company from loss, misuse or unauthorised access. To protect users' personal data, the company avails of protection technologies and procedures according to the best practices available from time to time.

7. ORGANISATIONAL CHART, APPOINTMENT SYSTEM AND RESPONSIBILITIES

To ensure the protection of the rights of natural persons with regard to the processing of personal data, the company always ensures the precise identification of persons who play active roles in the processing. This is achieved by setting up and efficiently maintaining a traceable system of appointments and related tasks.

In this way, it is easy to understand the consequent allocation of the responsibilities of each subject, which are proportionate to the nature, scope, context and purpose of the processing, as well as the risks to the rights and freedoms of natural persons analysed whenever deemed necessary.

All of the above is reflected in the privacy organisational chart, which is updated at the periodic intervals deemed most appropriate in relation to the sector of activity and the structure of the company's organisation, or when any changes are made.

According to the reference legislation and the policy deriving from this Organisational Privacy Model, the following figures are essential.

Verona Lamiere S.p.A. is committed to guaranteeing the exercise of the rights of data subjects and, for this purpose, identifies and implements appropriate procedures to inform data subjects and guarantee each of them of their:

- right of access, i.e. to obtain confirmation of the existence or otherwise of their personal data and to have access to it;
- right of rectification, i.e. to obtain the updating, correction or, whenever necessary, supplementation of the data;
- right of erasure, i.e. to obtain the deletion, transformation into anonymous form or blocking of data processed in breach of the law;
- right of opposition, i.e. to restrict or oppose, for legitimate reasons, the processing, following the procedures described in the applicable rules.

Verona Lamiere S.p.A. undertakes to respond without delay to requests made by the data subject either directly to the company, to the persons in charge or to specially appointed authorised persons, in the forms and manner and through the means considered most appropriate.

Data Controller's Contacts:

Verona Lamiere S.p.A. Via G. Pascoli 46 35179 Zevio (VR)
To the attention of the Data Controller of GDPR Office
dedicated e-mail: privacy@veronalamiere.it

This corporate GDPR policy is published on the website https://www.veronalamiere.it