

Video Surveillance Notice

Art. 13 EU Reg. 2016/679 "GDPR"

WHO IS THE DATA CONTROLLER?

The data controller is **TASTITALIA SRL**, Via Jesina 27/P – 60022 Castelfidardo (AN), whose contact details are: Tel. 071.7825276, E-mail: info@tastitalia.com

More information on the website: www.tastitalia.com

WHAT IS THE PURPOSE OF PROCESSING?

In compliance with the regulatory provisions regarding the processing of personal data, we inform you, as the "Data Subject," of the methods used for processing your personal data, which may be acquired through the video surveillance system active at our company. This ensures proper, lawful, and transparent processing of your data, in compliance with the principles of application established to protect your personal rights and freedoms.

WHAT IS OUR LEGAL BASIS FOR PROCESSING THE DATA?

We process your data to protect the safety of individuals who, for any reason, are present in the company premises and to prevent vandalism, damage, or theft of movable or immovable property located in company premises. Processing is carried out in accordance with the provisions of the GDPR, the Provision of April 8, 2010, issued by the Italian Data Protection Authority, and Guidelines 3/2019 on the processing of personal data through video devices, in particular pursuant to Article 6, paragraph 1, letter f), of the GDPR, for the legitimate interests of the Data Controller and users, such as the protection of assets and personal safety.

WHAT DATA CAN WE PROCESS?

We primarily request and process only personal data classified as "common," such as your images/videos when you transit through video-monitored areas. Only in certain cases may images/videos reveal "sensitive" data, but these are compatible with the purposes and the indicated legal bases. Video-monitored areas will be identified by signs indicating the "minimum" information in a clearly visible format and positioned within the cameras' range.

The acquisition of your data is necessary for the pursuit of the purposes of the processing.

TO WHOM DO WE DISCLOSE PERSONAL DATA?

Your personal data will not be shared with other parties and will never be disseminated.

If necessary, they may be entrusted to companies that carry out activities on behalf of the Data Controller, appointed as External Processors and trained to process the data in accordance with current legislation, or transmitted, upon express request, to the Authorities.

HOW DO WE PROCESS DATA?

We process your personal data at the Tastitalia SRL headquarters, in digital format. We take all necessary technical and organizational measures to prevent unauthorized access, disclosure, modification, or destruction.

Only personnel expressly authorized by the Data Controller may access the site to view the footage. Access to recorded images may only be granted if any unlawful conduct and/or significant events are detected or reported, or upon request of the judicial authorities.

The Data Controller will ensure that processing is carried out without unjustified interference with the fundamental rights and freedoms of the data subjects with respect to the purposes of the processing; in particular, it will comply with the prohibition set forth in Article 4 of Law 300/1970 regarding remote monitoring of employees' work activities. Recording, except for specific cases, is set to 24/7. No automated decision-making systems, including profiling, are used.

IS THE DATA TRANSFERRED TO COUNTRIES OUTSIDE THE EU?

Your data will not be transferred to third-party countries outside the European Union or whose data protection laws are non-aligned with EU Regulation 2016/679. Furthermore, we will not disclose your data to unauthorized third parties for purposes other than those described in this policy.

HOW LONG DO WE KEEP THE DATA?

Your personal data will be stored for a period not exceeding 3 days from the collection, unless specific retention requirements due to holidays or office closures. This will consider the specific security requirements pursued, related to the purposes of safeguarding the company's assets as well as protecting the safety of the people, and enabling the monitoring and reconstruction of all events, in the event of a request by law enforcement. The system is programmed to automatically delete all information upon expiration of this period, thus rendering the deleted data unrecoverable.

WHAT ARE YOUR RIGHTS?

You can directly request from the Data Controller to view, correct, delete, or limit the data we process about you. You also have the right to data portability and therefore, in certain situations, you can request a digital copy of your data or automatic transfer between public authorities.

You have the right to be informed about the identification details of the Data Controller and the Data Processor, as well as the purposes, legal basis, and other information required pursuant to Articles 13-14 of the GDPR.

You have the right to obtain, by the Data Controller, without delay and in any case no later than 30 days from the date of receipt of the request, or 45 days, prior notification to the data subject in the case of a valid reason, access to your data, with the necessary clarifications:

- I. The practical application of Article 15, paragraph 4, of the GDPR may have a negative impact on the rights of other data subjects. Actually, a video recording may contain the personal data of other data subjects. A data subject's request to receive a copy of a recording, pursuant to Article 15, may adversely impact their rights and freedoms. To avoid this side effect, the Data Controller may do not disclose the video to prevent other data subjects from being identified.
- II. The access request may not be granted if, pursuant to Art. 11, paragraph 2, GDPR, the Data Controller is unable to identify the data subject. For this purpose, the data subject must specify the relevant time period in his or her request (e.g., a time limit or location). If the Data Controller is unable to fulfil the request or it is not possible to comply with it, the Data Controller must notify the data subject.
- III. Pursuant to Article 12 of the GDPR, in the event of excessive or manifestly unfounded requests from the data subject, the Data Controller may alternatively charge a reasonable fee pursuant to Article 12, paragraph 5, letter a), not exceeding the costs actually incurred and including personnel costs, or refuse to process the request (Article 12, paragraph 5, letter b). The excessive nature of the request must be justified and demonstrated.

Any requests will be evaluated and, if necessary, granted within the legal timeframe, considering the limitations set forth in Articles 2 undecies and 2 duodecies of the Privacy Code, as amended following the entry into force of Legislative Decree 101/2018, and Article 23 of the GDPR.