VIDEO SURVEILLANCE POLICY

TÜV Rheinland Italia S.r.l. wishes to inform anyone accessing its premises about the processing of personal data carried out through the video surveillance system installed at its headquarters in Via Enrico Mattei 3, 20005 Pogliano Milanese (MI). The processing is carried out in compliance with Legislative Decree 196/2003 ("Privacy Code") and Regulation (EU) 2016/679 ("GDPR"), the Provision of the Italian Data Protection Authority of April 8, 2010 on video surveillance, and Article 4 of Law No. 300/1970.

1. Who is the Data Controller? How can they be contacted?

The Data Controller is **TÜV Rheinland Italia S.r.l. a sole shareholder company**, with registered office in Via Enrico Mattei 3, 20005 Pogliano Milanese (MI), Tax Code and VAT No. 12184570153, which can be contacted at the following e-mail address:**dpr@it.tuv.com** (hereinafter, the "Data Controller" or the "Company").

2. Who are the data subjects?

"**Data** subjects" are all natural persons who access the Company's premises where the video surveillance system is in operation, including, by way of example:

- employees;
- collaborators;
- suppliers;
- visitors;
- other individuals who access the company premises.

3. What personal data do we collect and process?

The Data Controller processes only visual personal data acquired through closed-circuit cameras installed on company premises, such as:

- images and video recordings of people passing through areas under video surveillance.

The video surveillance system does not use facial recognition technology or automated biometric identification systems. The cameras are directed exclusively towards access areas, transit areas, and common areas and are not installed or directed towards individual workstations.
The recording and storage systems are protected by appropriate technical and organizational security measures, including:

- multi-factor authentication systems for access to recordings;
- storage of archiving devices in physically protected locations;
- access control systems and intrusion alarms to protect the premises where the data is stored.

4. Where does the personal data come from?

Personal data is collected directly through the video surveillance system installed on company premises. The presence of cameras is clearly indicated by appropriate information signs located in the areas concerned.

5. For what purposes do we process the data? What is the legal basis? How long do we store it?

Purpose of processing	Legal basis	Retention period
Protection of the security of company premises, people, and company assets	Art. 6(1)(f) GDPR – legitimate interest of the Data Controller	Maximum 72 hours from recording. After this period, the images are automatically overwritten by the system, except in exceptional cases indicated below.
Prevention of unauthorized access, theft, vandalism, or other illegal events	Art. 6(1)(f) GDPR – legitimate interest of the Data Controller	As above
Establishment, exercise, or defense of the Controller's rights in court	Art. 6(1)(f) GDPR – legitimate interest of the Data Controller	For the time necessary to manage the event and any disputes
Compliance with legal obligations or requests from competent authorities	Art. 6(1)(c) GDPR – legal obligation	For the period provided for by applicable legislation

6. Is the provision of data mandatory or optional?

Data is provided automatically by accessing the areas under video surveillance. If the data subject does not wish to be filmed by the video surveillance system, they may not access the Company's premises subject to video surveillance.

7. To whom are personal data communicated?

Personal data may be processed or communicated to:

a) authorized personnel of the Data Controller who have been duly trained in data processing;
b) suppliers responsible for the maintenance of the video surveillance system or security and surveillance services, appointed for this purpose as Data Processors pursuant to Article 28 of the GDPR;
c) TÜV Rheinland Group companies that support the Data Controller in system management, audit, or compliance activities;

7. To whom are personal data communicated?

d) public authorities or entities to whom the communication of data is required in compliance with regulatory obligations (e.g., judicial authorities, police forces).

8. Are the data transferred outside the European Union?

Data collected through the video surveillance system is not transferred to countries outside the European Economic Area.

9. What are the rights of data subjects?

Data subjects may exercise the rights provided for in Articles 15–22 of the GDPR, including:

1. the right to access personal data;
2. the right to rectification;
3. the right to erasure;
4. the right to restriction of processing;
5. right to object to processing;
6. right to data portability (where applicable).

Data subjects also have the right to lodge a complaint with the Italian Data Protection Authority, located at Piazza Venezia 11, 00187 Romewww.garanteprivacy.it

10. How can rights be exercised?

Requests relating to the exercise of rights can be sent directly to the Data Controller by writing to:**dpr@it.tuv.com** The Data Controller will respond within 30 days, except for any extensions permitted by applicable law.

11. Can this policy be updated?

Yes. This policy may be updated or modified to comply with regulatory, organizational, or technological changes. Updated versions will be made available through the Company's institutional channels.