

Privacy policy for video surveillance



Controller:

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Germany

Phone: +49 5246 963-0

info@beckhoff.com

Data Protection Officer:

Phone: +49 5246 963-0

E-mail: dataprotection@beckhoff.com

Purposes and legal bases of processing:

Video surveillance is performed to enforce property rights. Video surveillance is also used to prevent crimes and facilitate the prosecution of crimes, as well as to assert, exercise, or defend legal claims.

The legal basis for video surveillance is Article 6(1)(f) of the GDPR, with our legitimate interests arising from the purposes mentioned above. To the extent that special categories of personal data are processed, this is done on the basis of Article 9(2)(f) of the GDPR.

Retention period:

Data obtained from video surveillance is generally deleted after 72 hours.

Data may be retained for a longer period in specific cases if facts justify the assumption that recordings from a specific time period will show acts that are intended to be prosecuted as a criminal offense or be used to assert claims under civil law.

Categories of recipients:

Internal recipients: If any criminal acts are suspected within our company, the Legal department, the internal data protection officer, and the IT department are authorized to access the video recordings. In addition, the "Real Estate" department may be granted access for the purpose of conducting maintenance.

External recipients: The service provider that has been commissioned by us and is responsible for maintaining and implementing the video surveillance cameras may also have access to the video recordings. If any criminal acts are suspected, the data may also be disclosed to external attorneys, insurance companies, and law enforcement agencies.

Otherwise, data will only be disclosed if there is a legal basis for doing so. In particular, this may be the case when the police or other law enforcement agencies request access to the video surveillance data for the purpose of preventing a threat.

Privacy policy for video surveillance



Data transfer to a third country

Data transfer to a third country (a country outside the European Economic Area) does not take place.

Rights of data subjects:

You have the right to:

- access information (Art. 15 of the GDPR)
- rectification (Art. 16 of the GDPR)
- erasure (Art. 17 of the GDPR)
- restriction of processing (Art. 18 of the GDPR)
- data portability (Art. 20 of the GDPR)
- lodge a complaint with a supervisory authority (Art. 77 of the GDPR)

In addition to the rights listed above, you also have the right to object in accordance with Art. 21 of the GDPR. Separate information about this right is provided below:

Right to object pursuant to Art. 21 of the GDPR

You have the right to object, on grounds relating to your particular situation, at any time to processing of your personal data which is based on Art. 6(1)(e) or (f) of the GDPR. This also applies to profiling in accordance with Article 4(4) of the GDPR, if applicable. In the event of an objection, we will no longer process your personal data further unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights, and freedoms, or for the establishment, exercise, or defense of legal claims. If you object to the processing of your personal data for marketing purposes, we will no longer process this data for such purposes, including any associated profiling in the context of direct marketing.

To exercise your rights, please contact the data protection officer.

Obligation to provide personal data / consequences if data is not provided:

Data is provided voluntarily. If the data is not provided, access to our company premises cannot be granted.

Profiling / Automated decision-making:

Profiling or automated decision-making does not take place.