Data Notice

Emergency Exit Control System – FT-XX Family

Statement on Compliance with the EU DATA ACT

(Regulation (EU) 2023/2854)

As of 12 September 2025, all connected products placed on the EU market that collect or generate data, as well as related applications or software services, are required to provide a data notice in accordance with the EU Data Act.

Manufacturer:

MANIAGO GmbH, Nikolaus-Otto-Straße 5, 55129 Mainz, Germany

Product Category:

Emergency Exit Control System – FT-XX Family

Product Typs:

FT-XX Emergency Exit Door Control Terminal, FT-I/O-Module, FT-I/O-Module Mini, FT-Bus Coupler, API for Building Managament System integration, FT-Show Management Software

1. Description of Generated Data

During normal operation, the emergency exit control system generates various types of operational and usage data, including in particular:

- Door status information (e.g., locked, unlocked)
- Alarm events (e.g., local emergency release, emergency unlocking, forced entry attempts)
- Tamper events (e.g., enclosure opened, I/O module tampering)
- Device and system status information (e.g., online/offline status, temporary release, remote release authorization, permanent release, interlock operation)
- Diagnostic data
- System logs and configuration data

2. Data Access and Ownership

Operational data is collected and stored in the locally installed management software database. The system operators have access to the data generated by the product. They are considered the data holders and are responsible for the management, storage, and use of such data.

3. Disclosure to Third Parties

Any decision to disclose the generated data to third parties rests solely with the system operators. System operators act under their own responsibility and must ensure compliance with all applicable legal and regulatory requirements.

4. Data Retention

The retention period for locally stored data is defined by the system operators. Data remains stored until it is deleted by users or system operators, or until the application is reinstalled or the system is reset.

5. Technical and Organisational Measures for Data Protection

The manufacturer implements appropriate technical and organisational measures to ensure the security and protection of the data generated by the product. These measures are intended in particular to prevent unauthorised access, loss, manipulation, or unauthorised disclosure of data.

6. Restrictions on Data Access

Access to certain data may be restricted where disclosure would:

- compromise trade secrets or intellectual property,
- adversely affect the security or integrity of the system, or
- violate applicable legal or regulatory requirements.

Analytical or derived data generated internally by the manufacturer may fall outside the scope of the system operators' access rights.