

1 Object and Purpose

This guideline addresses the access, use, processes, duties and responsibilities for digital data related to automated intralogistics systems for automated warehousing and distribution centres.

It addresses all the involved parties:

- Asset Owner or Operator
- Manufacturer and/or System Integrator
- Service Providers
- End Customers

The purpose of this guideline is to provide a framework for setting up of appropriate data sharing agreements between asset owners, operators, manufacturers, system integrators and service providers.

This guideline considers the following aspects of data sharing:

- The key aspects of digitalisation:
 - Data Responsibility and Rights
 - Communication and Remote Access
 - Cybersecurity
- The main layers of the material handling automation solution are addressed:
 - Physical equipment layer
 - Controls & Communication layer
 - Software & Application layer

This document provides details of the topics that should be considered, so that no important aspect is overlooked and helps to define of roles, rights and responsibilities of the parties, so that the interests of each stakeholder are respected. It aims to provide a tool-box for the definition and development of system and project specific data sharing agreements for automated warehousing and distribution solutions.

2 Contents

1 Object and Purpose.....	1
2 Contents.....	2
3 Introduction and General Remarks.....	3
3.1 How to read and use this document.....	3
3.2 Important notice for all stakeholders.....	4
4 Summary of Recommendations.....	5
5 Remote Access Connection.....	7
5.1 Advantages and purpose of remote access connections.....	7
5.2 Data Exchanged.....	8
5.3 Security of Remote Access Connections.....	11
5.3.1 Introduction.....	11
5.3.2 Cybersecurity Threads.....	11
5.3.3 Secure Remote Access.....	12
6 Data sharing agreement.....	14
6.1 Overview.....	14
6.2 Data Category and Reasoning.....	14
6.3 User Roles and Types including Access Types.....	15
6.3.1 Asset Owner.....	16
6.3.2 End Customer.....	17
6.3.3 Manufacturer.....	17
6.3.4 Regulatory Bodies.....	18
6.3.5 Service Provider.....	18
6.3.6 Software Provider.....	18
6.3.7 System Integrator.....	19
6.4 Ownership, Responsibility and Accountability.....	19
6.5 Data Privacy Regulations.....	20
6.6 Supplier Access to Data.....	21
6.7 Revision Clause.....	22
7 Glossary.....	23
8 References.....	24

3 Introduction and General Remarks

3.1 How to read and use this document

This document addresses all stakeholders for the use, the provision and the access of digital data related to automated intralogistics systems for warehousing and distribution centres. The following are recommendations for the respective stakeholders regarding the use of this guideline. The section 4 “Summary of Recommendations” provides an overview and summary relevant to all stakeholders. The section 6 “Data sharing agreement” presents the recommended content and structure for a data sharing agreement and is therefore relevant for all stakeholders. Please also read the Important notice for all stakeholders in section 3.2 .

Asset Owner or Operator

Asset Owners or Operators should acknowledge the need for a data sharing agreement, see sections 5.1 and 5.2. The section 5.3.2 provides an overview of the cybersecurity threads and derives from it the shared responsibility for cybersecurity. The section 5.3.3 provides an overview of cybersecurity recommendations for remote access and serves as both, a recommendation for your own measures as well as an overview of the measures to be expected from the respective interface partners.

In the following the term “Asset Owner” will be used for both, the asset owner and the operator(s).

Manufacturer and/or System Integrator as well as Service Providers

Manufacturers and/or System Integrators shall especially read

- Section 5.1 Advantages and purpose of remote access connections
- Section 5.2 Data Exchanged
- Section 5.3 Security of Remote Access Connections

In the following the term “Manufacturer” will be used for the manufacturer, the system integrator, and the service provider(s).

End customers are considered in this document, but are not the direct addressees of this guideline.

3.2 Important notice for all stakeholders

This document serves as a guideline for enhancing **shared digital data and access measures** in the context of warehouse and distribution automation.

Whilst reasonable efforts have been made to provide accurate and up-to-date information, it is essential to note that the shared digital data and access measures, including cybersecurity measures, are complex and evolving. The guidelines and the recommendations presented here should be used as a reference and starting point for shared digital data and access in warehouse and distribution automation.

This guideline does **not** aim to define the technical and implementation details for the secured sharing and accessing of digital data. (see also section 5.3.2)

Cyber security-related aspects are continuously changing, and attacks are adjusted to undermine the current state of security. New vulnerabilities and attack vectors are discovered regularly.

It is essential to recognise that the responsibility for cybersecurity ultimately lies with the Asset Owner and the Manufacturer of warehouse and distribution automation systems and therefore they must stay informed about emerging threats and adapt their security measures accordingly to avoid risks.

Depending on geographic location and industry segment, warehouse and distribution automation systems may be subjected to various cybersecurity and other regulations and standards.

In this context, particular attention should be drawn to the EU Cyber Resilience Act and the EU Data Act.

4 Summary of Recommendations

This section summarises the key recommendations. Further details on each of the recommendations is given in the individual section of this document.

1. A remote access connection should be enabled and established between the machine manufacturer and asset owner

Remote access is a key enabler for the maintenance and improvement of the system. Therefore, the requirements and functions of a remote access connection are a fundamental part of this guideline.

This includes the definition of data and communication categories as well as purpose and usage requirements.

This guideline recommends establishing a connection to exchange data between the asset owner and the machine manufacturer to exchange several data categories with a defined purpose and a clear definition of data usage requirements.

2. Remote access connections should be secured by state-of-the-art cybersecurity controls

To secure the assets, their operations and the exchanged data, implementation of state-of-the-art security controls is essential for the data exchange connection.

Because state-of-the-art will frequently change and there will also be company specific and regional regulations, this guideline defines key principles together with references to existing standards for further detailed work.

3. Agree on a formalized data sharing agreement following the key recommendations of this FEM guideline

The connection between asset owner and machine manufacturer needs to follow a formalized data sharing agreement. This will provide a contractual foundation to act as a solid basis for a trustworthy partnership and allow both parties to derive value from the exchanged data.

The structure of the data sharing agreement should as a minimum include the following content:

a) Data Categories and Reasoning ("Why and What")

A clear definition of the use-cases the data is used for and formulate a basic description of the data categories including details such as the sharing frequency.

This is needed to have a clear scope of the data exchange and a common understanding of the mutual expectations.