Robert Bosch Manufacturing Solutions GmbH
Bosch Connected Industry

Customer Leaflet for Data Protection and Data Security within the GDPR for **"Agentic AI Manufacturing Framework"**

System Version 1.1
Effective: November 2025

Table of contents

1. Introduction 3
2. General product description 3
3. General information about the processing of personal data 3
4. Affected data subjects 4
5. Support by the data processor in the context of fulfilling data subject requests 5
6. Deletion concept 5
7. Data transfers in third-party countries 6
8. Security 7
   8.1 Sensitization and Training of Employees 7
   8.2 Handling of Information and IT Systems 7
   8.3 Access to IT Systems 7
   8.4 Access to Information and Personal Data 8
   8.5 Encryption of Information and Personal Data 8
   8.6 Physical Protection of Information, Personal Data and IT Systems 8
   8.7 Secure Operation of IT Systems and Networks 9
   8.8 Acquisition and Development of IT Systems and Bosch Products 9
   8.9 Processing and Protection of Information and Personal Data by Third Parties 10
   8.10 Handling of Information Security and Data Protection Incidents 10
   8.11 Availability of Information, Personal Data and IT Systems 10
   8.12 Monitoring Compliance with Corporate Policies 10

1. INTRODUCTION

The following Customer Leaflet is intended solely as general information regarding data protection about the software "Agentic AI Manufacturing Framework" (hereafter referred to as "**AAMF**"), distributed by Robert Bosch Manufacturing Solutions GmbH ("**Bosch**").

This document is provided as an information source for your solution-specific data protection and data privacy topics and is not intended to provide and should not be relied on for legal advice.

2. GENERAL PRODUCT DESCRIPTION

AAMF, along with the software agents implemented and provided by it, forms an AI-driven information and assistance system for production and logistics. It is used to support typical workflows in industrial manufacturing plants. The provided agents utilize existing information sources and software tools of the plant, as well as generic sources and tools that are integrated via the framework.

For example, the Shopfloor AI Agent enables users to obtain decision-supporting metrics from a KPI reporting system (such as Nexeed IAS), record special occurrences like downtimes in the digital shift book, create handover protocols, and provide solution tips based on past occurrences.

The AAMF includes the integration of customer-specific information sources and systems as an integral component. The customer is responsible for approving this integration. The processed data are derived from these sources and systems and must be documented by the customer accordingly. This includes the legality of collecting and processing these data, including their identification and the specification of the respective processing purpose.

3. GENERAL INFORMATION ABOUT THE PROCESSING OF PERSONAL DATA

The term "personal data" encompasses both personally identifiable and personal data in the sense of the General Data Protection Regulation (GDPR). Many of the stated personal data mainly consist of purely technical data that could be associated with individuals under certain conditions, such as in conjunction with shift schedules, a small number of system users, or limited access permissions. In particular, references to individual users in the system are made using a so-called UUID (a 36-character random alphanumeric combination). In order to align with the principles of data protection regulations, such data is also treated as personally identifiable.

Customers and operators are obliged to review and adhere to national and industry-specific data protection laws, as applicable. AAMF can only be operated on a cloud instance as Software as a Service (SaaS). The following information is based on the standard version of AAMF within this cloud operation. The table below contains information about the personal data processed, and their processing purposes, for the framework and the available agents.

Component	Personal Data	Processing Purpose
AAMF	• Access permissions and roles within the application • Error logging and system monitoring • File uploads, file management (e.g., manuals) • Usage data from the chat interface • Interaction data with the agent	• Customization of Open WebUI functionality • Access to previous conversations, allowing the user to continue a dialogue with the AI beyond a single question • For the management of access rights to defined resources • Error and security analysis

	• Operations and support information (e.g., logs, timestamps, error messages) • Data to and from connected data sources via semantic search • Interaction data of agents with external systems • Conversation data of multiple agents • Voice recordings when using the speech-to-text functionality.	• For the operation and monitoring of the application's availability and performance • Facilitating the continuation of a conversation with an agent or a team of agents • For the analysis of latency and quality of the agent-gen-AI solutions • Code, files, text, or configurations uploaded by the user in their "workspace" in OpenWebUI • Speech-to-text functionality • User identification and authentication • User login and access permissions • User token update/session retention
Operations cloud	• Backups • All data within the application	• Setup, update, operation, and monitoring of the application on the cloud, including error handling • For monitoring the availability of product functionality and data • Detection of security-related incidents • To facilitate data recovery processes

4. AFFECTED DATA SUBJECTS

The following data subjects are affected by the aforementioned processing of personal data:

Data Subject	**Data Category**
System User/ Administrator	• Name, first name • Email address • IP address • User IDs • Access permissions and roles within the application • Display settings in user interfaces (e.g., language and country-specific configurations) • Error logging and system monitoring • Security logs including IP addresses • File uploads, file management (e.g., manuals) • Data analysis: configuration, results, and reports • Measurement data and error messages from machines and sensors • Master and transaction data related to deployment planning (only metadata without personal association)

	• Master and transaction data related to plant infrastructure, lines, and machines (including geolocation) • Technical configuration data from machines, devices, system components, and modules

Operator	• Backups
	• All data within the application, i.e.
	  ○ Chat history
	  ○ Workflow results

Support	• Master data of the contracting party • Name, first name • Email address • User IDs • Telephone number • Department • Location • Error logging and system monitoring • Security logs including IP addresses • Support messages including description of the issue and any key data related to the issue

5. SUPPORT BY THE DATA PROCESSOR IN THE CONTEXT OF FULFILLING DATA SUBJECT REQUESTS

The controller, as defined in Article 4 No. 7 GDPR, is responsible for fulfilling the rights of data subjects under Articles 12 ff. GDPR. Bosch in its role as processor, supports the controller in this regard (see clauses 3.4, 3.9, 3.10, 5 of the GDPR processing agreement). As contractually agreed, Bosch does not directly respond to information requests from data subjects.

To request support from the processor, a support inquiry must be sent to: aiincubator.bci@de.bosch.com.

If the support service requires the transfer of personal data to the controller, this will be done exclusively in encrypted form. This is intended to prevent unauthorized access by third parties.

6. DELETION CONCEPT

The chat frontend component represents the user management of the AAMF and is utilized by other components. For each user, an internal UUID is generated, establishing a link to the user's user ID. Within the components, only the UUID is used. Therefore, data in the framework and agents' chat histories are not directly personal, but they can be indirectly associated with personal data through the UUID.

If a user is deleted from the chat frontend, the link between the UUID and the user ID is lost. The data in the framework and chat histories are then no longer personally identifiable.

Despite the removal of the link, personal or personally identifiable data may remain in the system in the following areas:

- Personal information potentially entered in free-text fields (chat windows).
- Local browser data possibly stored on the user's computer.

- Data potentially downloaded from the framework and stored locally by the user (e.g., reports, chat histories).
- Membership of the user in identity providers or groups that are recorded in the framework but maintained outside the framework.
- Access, identification, and personal data created within independently connected tools, data sources, or workflows.

If present, these data must be manually deleted. Support can be obtained upon request at aiincubator.BCI@de.bosch.com.

Deletion requests for tenants, as well as customer-specific data sources and software tools, are always triggered manually and executed only after verification.

The following deletion periods are planned for data in the cloud application:

Data Category	**Retention Policy**
User data and permissions	Upon deletion of the user account
Master data and other technical data	Deletion functions available in the system
Log files	180 days
Backups	30 days
Support-Tickets	6 month

For the deletion of customer data after the end of the contract, please refer to clause 3.10 of the GDPR processing agreement.

If a customer connects custom data sources to the AAMF deletion of personal or personally identifiable data is in the responsibility of the customer.

7. SUBPROCESSORS

In the course of providing and using AAMF, service providers, referred to as "sub-processors", are contracted. These may include other companies within the Bosch Group. Bosch carefully selects appropriate sub-processors and may monitor them regularly, especially with regard to the careful handling of stored personal data. Furthermore, all sub-processors are obligated to maintain confidentiality and comply with legal requirements.

The individual sub-processors and the conditions for their appointment can be found in the GDPR processing agreement.

8. DATA TRANSFERS IN THIRD-PARTY COUNTRIES

The use of AAMF requires the transfer of personal data to recipients located outside the European Union (EU) or the European Economic Area (EEA), to so-called "third-party countries". Prior to the transfer of personal data, compliance with legal requirements is ensured.

Details regarding encryption methods and security measures are subject to technical changes.

9. SECURITY

Information security and data protection are integral parts of our corporate policy. To securely process information and personal data, appropriate technical and organizational measures are implemented in accordance with the current state of the art to achieve a protection level that is appropriate to the risk.

Security incidents and vulnerabilities in Bosch products can be reported to us at any time via https://psirt.bosch.com/.

9.1 Sensitization and Training of Employees

To reduce risks in handling information and personal data by employees, the following measures, among others, are implemented:

A process exists for new hires in sensitive areas to ensure that employees are suitable for the roles intended for them.
Employees are regularly instructed, trained, and made aware of the risks associated with handling information or product development.
Employees are obligated to comply with laws and internal rules regarding information security and data protection.

9.2 Handling of Information and IT Systems

To mitigate risks from insufficient protection of information, personal data, or IT systems, the following measures, among others, are implemented:

Information, personal data, and IT systems are identified, inventoried, assigned to responsible parties, and classified according to their protection needs.
The processing of information on privately acquired IT systems is prohibited.
Data carriers containing sensitive information and personal data are securely disposed of by deleting the data or destroying the data carriers.
Upon termination of employment, employees return any information or IT systems in their possession to the Bosch Group.

9.3 Access to IT Systems

The following Technical and Organizational Measures, among others, have been implemented to reduce risks arising from unauthorized access to IT systems:

Employee user accounts are centrally managed, regularly reviewed, and deleted when necessary.
Administrative accounts are granted restrictively, their necessity is regularly reviewed, and they are deleted when no longer needed.

Secret access information (e.g., passwords) follows a strict password management protocol and is securely managed, stored, and transmitted within IT systems.
Access to IT systems is conducted using secure authentication methods, depending on the type of access and the protection requirements of the information.

9.4 Access to Information and Personal Data

The following Technical and Organizational Measures, among others, have been implemented to reduce risks from unauthorized access to information and personal data:

Access authorizations are limited to the necessary extent, are regularly checked, adjusted if necessary or withdrawn (need-to-know, need-to-use).
Administrative authorizations are assigned restrictively, their necessity is checked regularly and withdrawn if necessary.

9.5 Encryption of Information and Personal Data

The following Technical and Organizational Measures, among others, have been implemented to reduce risks from unauthorized reading, copying or modification of information and personal data:

Information is encrypted during storage and transport depending on its security classification.
Keys are issued and managed by an own Bosch Trustcenter to reduce the risk of theft or loss of the keys.
Encryption methods are state of the art.

9.6 Physical Protection of Information, Personal Data and IT Systems

The following Technical and Organizational Measures, among others, have been implemented to reduce risks arising from unauthorized access, damage or theft of information, personal data and IT systems:

Access to the Bosch Group properties (e.g. plants, buildings, offices) is based on identification and authorization of persons (e.g. via employee ID cards, visitor controls).
Dividing properties into security zones with appropriate security requirements.
Sensitive IT systems (e.g. servers) are placed in access protected IT data centers or IT rooms.
Employees are regularly advised to maintain a tidy work environment (clean desk) to reduce risks from the theft of documents, IT devices, or removable storage media.
A regulated process with documentation requirements has been implemented for transporting equipment, removable storage media and documents.

9.7 Secure Operation of IT Systems and Networks

The following Technical and Organizational Measures, among others, have been implemented to reduce risks arising from the improper operation of IT systems:

Operating procedures are implemented for the operation of IT systems, which describe the security-relevant operating processes (e.g. change and patch management, backup and recovery procedures).
Changes to IT systems are planned, approved and executed as part of change management processes.
Test and production systems are separated from each other.
IT systems are protected by a multi-level malware concept.
Software installation by users is restricted.
On IT systems, security-relevant events are logged under consideration of data protection in order to identify security and data protection incidents.
Vulnerability management: Technical vulnerabilities in IT systems are evaluated by the Bosch CERT (Computer Emergency Response Team) within the framework of regulated patch and change management processes, bindingly instructed and eliminated by the responsible parties.
Network segmentation and secure network interfaces are provided where technically necessary. IT systems requiring special protection or those with high risks are operated in separate network segments.

9.8 Acquisition and Development of IT Systems and Bosch Products

The following Technical and Organizational Measures, among others, have been implemented to reduce risks during the acquisition and development of IT systems and Bosch products:

When purchasing and developing IT systems, security requirements are derived from the protection requirements of the information and personal data.
Vulnerabilities are identified and eliminated during the development and before the implementation of IT applications.
Test data is protected according to its security classification.
A particular process exists for the development of Bosch products, which takes special account of the requirements for the protection of information and personal data ("Security by Design", "Data Protection by Design", "Data Protection by Default").

9.9 Processing and Protection of Information and Personal Data by Third Parties

The following Technical and Organizational Measures, among others, have been implemented to reduce risks in the processing of information and personal data by third parties:

Security requirements are established in supplier contracts to ensure that the information and personal data are protected to the same extent as when processed by the Bosch Group.
In the case of especially high-risk applications (e.g. external clouds), a preliminary check of the supplier's security concepts and processes is carried out to identify vulnerabilities and to reduce risks.
The implementation of the measures at the supplier is randomly checked.
If necessary, nondisclosure agreements (NDA) are signed when exchanging information with third parties.

9.10 Handling of Information Security and Data Protection Incidents

The following Technical and Organizational Measures, among others, have been implemented to reduce risks resulting from undetected or inadequately handled security incidents:

The Bosch Group has a computer emergency response team (Bosch CERT), which coordinates the handling of Enterprise IT security incidents and vulnerabilities.
The Bosch Group has a Product Security Incident Response Team (Bosch PSIRT), which coordinates the handling of security incidents and vulnerabilities in Bosch products.
Every employee is obliged to report security incidents or weaknesses to the Bosch CERT.
Data protection incidents can be reported to the Bosch Group’s Data Protection Officer via defined reporting channels, who coordinates further treatment.

9.11 Availability of Information, Personal Data and IT Systems

The following Technical and Organizational Measures, among others, have been implemented to reduce risks arising from unavailable information, personal data and IT systems:

To ensure availability of information and personal data, redundancy, emergency and re-start concepts for IT systems are available and implemented. An appropriate incident management is in place.
The information on IT systems is regularly backed up using tested procedures and, if necessary, archived to reduce the risks of information destruction or loss.

9.12 Monitoring Compliance with Corporate Policies

The following Technical and Organizational Measures, among others, have been implemented in order to reduce risks arising from specifications that have not been implemented:

The information and data protection organization conducts regular information security and data protection audits to reduce risks from missing or ineffective security measures.
Operators of IT systems conduct regular self-checks to reduce risks due to missing or ineffective security measures.