

EMAG Data Processing Agreement pursuant to Article 28 GDPR for EMAG Software Products
(Version as of October 2026)

between

[the Customer as defined in the Main Agreement]

- hereinafter referred to as the “Controller” -

and

[EMAG company as specified in the Main Contract]

—hereinafter referred to as the “Processor”—

- collectively referred to as the “Parties”

-

Table of contents

Preamble.....	3
1 General Provisions	3
1.1 Validity	3
1.2 Exclusive Agreement and written Form.....	3
2 Data Processing pursuant to Art. 28 of the EU-GDPR	4
2.1 Principles of Data Processing.....	4
2.2 Rights and Obligations of the Controller.....	4
2.3 Rights and Obligations of the Processor	5
2.4 Data Protection Organization	7
2.5 Technical and Organizational Measures	8
2.6 Right of Inspection	8
2.7 Subprocessors.....	9
2.8 Liability	9
3 Final Provisions	10
Appendix 1: Purpose of Data Processing.....	12
Appendix 2: Subprocessors	15
Appendix 3: Technical and Organizational Measures	16
3.1 Confidentiality	16
3.2 Integrity	18
3.3 Availability	19
3.4 Confidentiality	20
3.5 Integrity	22
3.6 Availability	23

Preamble

The Controller hereby commissions the Processor to process data pursuant to the agreement ("Main Contract"). To ensure compliance with data protection laws in connection with the Main Contract, it is necessary to enter into a data processing agreement. In this context, the parties enter into the following agreement:

1 General Provisions

1.1 Validity

- This Data Protection Agreement (hereinafter: DPA) enters into force upon acceptance of the offer. It is a separate agreement between the parties and exists alongside the Main Contract concluded between the parties. If and to the extent that the Main Contract contains provisions that conflict with those of the DPA, the provisions of the DPA shall take precedence, unless otherwise provided in the DPA.

1.2 Exclusive Agreement and written Form

- a. This DPA supersedes all previous agreements regarding commissioned data processing between the parties. The provisions of the DPA are exhaustive.
- b. Any amendment must be in writing. The written form requirement does not apply to updates to the appendices; in such cases, text form (including via email) is sufficient. Any amendment to the appendices requires confirmation by the other party in text form (including via email) to be effective.

2 Data Processing pursuant to Art. 28 of the EU-GDPR

2.1 Principles of Data Processing

- a. The Processor processes personal data on behalf of the Controller. The Processor shall process personal data only to the extent described in the main contract and exclusively for the purpose specified therein. The scope, nature, and purpose of the intended collection, processing, or use of data must be set forth in Annex 1.
- b. Processing takes place exclusively within the territory of the Federal Republic of Germany, in a member state of the European Union, or in another state party to the Agreement on the European Economic Area. Any misalignments of data to countries outside the EU or the EEA—including by a Subprocessor of the Processor—require the prior consent of the Controller and may only take place if the specific requirements of Chapter 5 of the GDPR are met. The engagement of Subprocessors is governed by Section 2.7.
- c. The definitions of the GDPR apply.

2.2 Rights and Obligations of the Controller

- a. The Controller is responsible for protecting the rights and freedoms of data subjects. The Controller shall issue the Processor with the instructions necessary to protect those rights and freedoms. The Controller shall ensure that the instructions issued to the Processor contain all necessary information required by the Processor to carry out the processing in compliance with data protection regulations.
- b. The Controller is responsible for ensuring that the instructions it provides to the Processor comply with the legal requirements applicable to the processing in question. The Processor's obligations to independently design processing operations in accordance with Section 2.3.m. remain unaffected.
- c. The Controller hereby instructs the Processor not to independently change the purpose of data processing and not to use the personal data provided to it by the Controller for the purpose of data processing—or which becomes known to it during the performance of the contract, as a result of data processing, or in any other manner—for its own purposes. This also applies to the use of pseudonymized or anonymized data, unless the Controller has consented to the use of the data. In the event of consent, the Controller must ensure that the legal requirements for such use of the data are met.
- d. To the extent necessary for the use of data processing, the Controller shall obtain consent from the data subjects that meet the legal requirements. The Processor is entitled to independently obtain consent from data subjects and to make such consent a prerequisite for the use of its services by the data subjects.

- e. The Controller is entitled to leave the details of data processing for the fulfillment of the contract to the Processor, provided that the Processor complies with the requirements set forth in Section 2.3.m.
- f. The Controller shall immediately inform the Processor if it detects errors or irregularities in the processing results, particularly if it has reason to believe that the manner in which the Processor processes the data violates data protection requirements.
- g. The Controller shall fulfill all obligations to safeguard the rights of data subjects to information, access, and other rights arising from the legal bases applicable to the processing in each case.
- h. The Controller shall independently create and maintain documentation of the data processing in its procedural overview and, where necessary, conduct a data protection impact assessment for the processing.

2.3 Rights and Obligations of the Processor

- a. The Processor is obligated to process personal data provided to it by the Controller within the scope of the contract for the purpose of data processing, or data that becomes known to it during the performance of the contract, as a result of data processing, or in any other manner, only in accordance with the Controller's instructions. The Processor is obligated to notify the Controller immediately if it believes that an instruction issued by the Controller violates applicable data protection law. In this case, the Processor may refuse to process the data.
- b. The Processor declares that, even due to legal requirements of the European Union or a member state of the European Union, it is not obligated to process data without instructions from the Controller.
The Processor shall inform the Controller immediately if it nevertheless receives a corresponding request to process data. This does not apply if the Processor is bound by legal provisions regarding confidentiality.
- c. The Processor may not disclose data pursuant to Section 2.3.a to third parties based outside the EU or the European Economic Area, unless the Controller has explicitly consented to such disclosure in writing. This does not apply to the extent that the Controller is responsible for the disclosure and the Processor has no influence over it.
- d. The Processor warrants that it is familiar with all relevant data protection regulations necessary for the lawful performance of data processing and guarantees their implementation to the extent that it is obligated to do so under this Agreement or by law. It guarantees that all persons it has commissioned to perform the contract have been bound by a confidentiality obligation or are subject to an appropriate statutory duty of confidentiality prior to the commencement of processing.

- e. To the extent that the Processor is unable, for technical or practical reasons, to correct, block, or delete personal data affected by the processing, the Controller is obligated to assist the Processor in carrying out the respective measure. The Processor shall, in accordance with Section 2.3.a., generally correct, delete, or block data only upon instruction from the Controller. The termination of the contractual relationship pursuant to Section 2.3.f. remains unaffected.
- f. Upon termination of the contractual relationship, the Processor shall, in accordance with the Controller's instructions, either transfer to the Controller any personal data under Section 2.3.a. that has not yet been transferred or delete such data. No later than upon termination of the main contract and after the expiration of any retention periods agreed upon therein, all personal data arising from the contractual relationship must be deleted, unless the Processor can demonstrate that it is required by law to retain the personal data.
- g. Should the Controller's property held by the Processor be jeopardized by actions of third parties—such as attachments, insolvency proceedings, or other events—the Processor must notify the Controller immediately and before such actions take place, so that the Controller's data can be removed from the Processor's IT systems in a timely manner.
- h. If and to the extent that the Controller receives a request from a supervisory authority or other competent body in connection with the processing of data pursuant to Section 2.3.a., the Controller must immediately inform the Processor and forward the request without delay.
- i. For its part, the Processor guarantees that it will immediately inform the Controller of any inspections or measures taken by the supervisory authority, to the extent that they relate to this contract. The Controller shall reimburse the Processor for the expenses incurred in this regard, provided that this is permitted under applicable data protection law.
- j. Should data subjects or other third parties direct data protection-related inquiries to the Processor or assert data protection rights against the Processor regarding the data specified in Section 2.3.a., the Processor shall forward these inquiries to the Controller without delay. The Controller shall reimburse the Processor for the expenses incurred in this regard, provided this is permitted under applicable data protection law.
- k. The Processor shall immediately notify the Controller of any serious disruptions to operations, suspected violations of data protection laws or the provisions set forth in the contract, or other irregularities in the processing of the Controller's data.

- l. In the event that the Processor determines, or facts give reason to believe, that personal data processed by the Processor on behalf of the Controller has been unlawfully disclosed, the Processor shall immediately and fully inform the Controller in writing or in text form (fax/email) of the time, nature, and scope of the incident(s). The notification must include a description of the manner in which the data was unlawfully accessed. The notification shall also include a description of any potential adverse consequences of the unlawful access. The Processor is further obligated to immediately report what measures it has taken to prevent such unlawful disclosure in the future. The Processor shall cooperate fully in investigating the incident and implementing countermeasures.
- m. If and to the extent that the Processor plans to collect or otherwise process additional data for its own use within the scope of or in addition to the commissioned data processing (e.g., usage data from its services used by the Controller's employees), this requires the Controller's consent. If this data collection is based on a statutory authorization—such as the creation of pseudonymous usage profiles based on the data subject's right to object—the Processor must inform the Controller of these measures prior to the technical implementation of the processing. The Processor is obligated to comply with all legal requirements for such processing and, in particular, to observe and uphold the data subjects' statutory rights to object, to access, and to receive information. The Processor is obligated to provide the Controller, upon request, with evidence of compliance with the legal requirements for processing. The Controller is entitled to prohibit the performance of such processing if the Processor cannot provide this evidence. The Processor may make the use of its services by employees, business partners, customers, or other data subjects who are authorized under the main contract to use the Processor's services contingent upon consent to such data processing.
- n. If and to the extent that the Processor is responsible for determining the specific arrangements for data processing pursuant to Section 2.2.e., the Processor undertakes to carry out such processing in accordance with the provisions of the GDPR. In particular, the Processor must comply with the provisions of Article 25 of the GDPR and, upon request, provide the Controller with appropriate proof of compliance with these provisions. Such proof may be provided through an approved certification procedure pursuant to Article 42 of the GDPR.

2.4 Data Protection Organization

- a. The Processor shall appoint a data protection officer to the extent that it is required to do so. If the Processor is not required to appoint a data protection officer, it shall designate the person within its organization who is responsible for data protection.
- b. The Data Protection Officer or the person responsible for data protection is the Processor's primary point of contact for data protection matters and can be reached at privacy@emag.com.
- c. The Controller has the right to contact the Data Protection Officer or the person responsible for data protection at any time regarding data protection matters affecting the DPA.

2.5 Technical and Organizational Measures

- a. The Processor provides sufficient guarantees that appropriate technical and organizational measures will be implemented to ensure that processing is carried out in accordance with the GDPR and the rights of the data subject.
- b. The Processor shall independently ensure the implementation of the technical and organizational measures specified in Section 2.5.a. The status as of the date of execution of the Data Protection Agreement is documented in Appendix 3.
- c. The Processor may not make any changes that fall significantly short of the requirements documented in Annex 3. The Processor must inform the Controller of any significant changes to the technical and organizational measures.
- d. If a change request from the Controller is based on a directive or recommendation from a supervisory authority responsible for data processing, or if it is preceded by an incident as described in Section 2.3.I., the Processor must adjust the technical and organizational measures accordingly.

2.6 Right of Inspection

- a. The Processor grants the Controller the right to verify compliance with data protection regulations and the Processor's instructions during normal business hours. The Controller shall notify the Processor of the planned audit at least 4 weeks in advance.
- b. To this end, the Processor grants the Controller a comprehensive right to information and inspection, as well as—in consultation with the Processor—a right of access to the Processor's relevant business premises, including the data processing facilities; however, the Controller must take the Processor's operational interests into account when exercising these rights. The Processor shall cooperate with these audits to the extent necessary. This obligation exists even before the start of data processing and may be repeatedly requested by the Controller, but only if there is a justified reason for a repeat audit.
- c. At the Controller's discretion, the audit may be replaced by proof of compliance with approved codes of conduct pursuant to Article 40 of the GDPR or an approved certification procedure pursuant to Article 42 of the GDPR.
- d. The Controller is entitled to engage knowledgeable external third parties to conduct the audit, who are bound by professional confidentiality or by a contractual agreement to maintain confidentiality. The costs of such additional audits shall be borne by the Controller.
- e. The Controller shall reimburse the Processor for the expenses incurred as a result of the audits pursuant to Section 2.6, provided that this is permitted under applicable data protection law.

2.7 Subprocessors

- a. The engagement of Subprocessors is permitted only with the Controller's prior written consent. As of the date of execution of this Agreement, the Processor shall engage the Subprocessors listed in Annex 2.
- b. In the written agreement with the Subprocessor, the Processor shall ensure that the provisions agreed upon in this Data Processing Agreement also apply to the relationship between the Processor and the Subprocessor.

2.8 Liability

- a. The Controller and the Processor shall be liable to third parties, within the scope of their respective responsibilities and in accordance with the statutory provisions of Article 82 of the GDPR, for damages resulting from data processing that does not comply with the GDPR.

3 Final Provisions

If and to the extent that requirements of the supervisory authorities and/or additional statutory requirements necessitate amendments to the provisions of the DPA and/or the associated annexes, the parties are obligated to cooperate in implementing the requirements and incorporating them into the DPA. Requirements of the supervisory authority responsible for the data processing covered by this agreement or of any other competent official body shall be deemed binding in this regard.

Overview of Annexes

Appendix	Contents
Appendix 1	Subject Matter of Data Processing
Appendix 2	Subprocessors
Appendix 3	Technical and Organizational Measures

Appendix 1: Purpose of Data Processing

The purpose and duration of data processing are planned as follows:

FOR EDNA Health Inspect:

- Diagnosis, Monitoring, and Analysis
- Allocation, Planning, Predictive Maintenance
- Customer Support
- For additional details, please refer to the scope of services and duration as specified in the main contract

FOR EDNA User Management:

- User management
- Assignment, management, administration
- For further details, please refer to the scope of services and duration as specified in the main contract

FOR EDNA Platform:

- Software-as-a-Service hosting
- Administration
- Performance optimization
- For further details, please refer to the scope of services and duration as specified in the main contract

The nature and purpose of the data processing are planned as follows:

FOR EDNA Health Inspect:

- Diagnosis, monitoring, and analysis, as well as the provision of a system for predictive maintenance management
- Assignment of measurements, planning of service and maintenance calls – Predictive Maintenance
- Customer support, creation and coordination of service and support requests and cases
- Provision of the service
- For further details, please refer to the scope of services in the main contract

FOR EDNA User Management:

- User management, authentication, and traceability of user actions (e.g., in the event of malfunctions or anomalies)
 - Assignment of measurements, planning of service and maintenance tasks – Predictive Maintenance
 - Management of user logins to ensure system security, logging, system monitoring, and bug fixing, administration
 - Provision of the service
 - For further details, please refer to the scope of services in the main contract
-

FOR EDNA Platform:

- Provision of a user agent platform / hosting of the cloud application
- Management of user logins to ensure system security, logging, system monitoring, and bug fixing, administration
- Storage of user preferences to improve usability
- Performance optimization, reduction of load times, offline availability of application data
- Management of the maintenance software as a Software-as-a-Service product
- Provision of the service
- For further details, please refer to the scope of services in the main contract

Data processing involves the following types of personal data:

Depending on the settings (on the customer's side), the following data types are possible

FOR EDNA Health Inspect:

- EDNA user data: First name, last name, email address, user ID, user IP address, password hash, customer number, customer name
- EDNA authentication and security cookies (session cookie, security cookie, Keycloak cookie)
- EDNA preference cookies (language preference, theme/display settings)
- EDNA browser cache / offline cache (React Query)
- EDNA Health Inspect application data: First name, last name, customer number, customer name, machine location address, machine serial number, measurement comment, measurement result

FOR EDNA User Management:

- EDNA user data: First Name, Last Name, Email Address, User ID, User IP, Password Hash, Customer Number, Customer Name Association, Scheduling, Predictive Maintenance
- EDNA Authentication and Security Cookies (session cookie, security cookie, Keycloak cookie)
- EDNA preference cookies (language preference, theme/display settings)
- EDNA browser cache / offline cache (React Query)

FOR EDNA Platform:

- EDNA user data: First name, last name, email address, user ID, user IP, password hash, customer number, customer name
 - EDNA authentication and security cookies (session cookie, security cookie, Keycloak cookie)
 - EDNA preference cookies (language preference, theme/display settings)
 - EDNA browser cache / offline cache (React Query)
-

The processing covers the following categories of data subjects:

FOR EDNA Health Inspect:

- Employees of the controller

FOR EDNA Health Inspect:

- Employees of the controller

FOR EDNA Health Inspect:

- Employees of the controller
-

Appendix 2: Subprocessors

[illegible]

Appendix 3: Technical and Organizational Measures

3.1 Confidentiality

3.1.1 Access Control

- Visitor Policy
- Access Control to Buildings and Rooms
- Granting, Monitoring, and Revocation of Access Rights Based on the Need-to-Know Principle
- Physical security of buildings and rooms, e.g., fencing, doors
- Visitors may only enter and remain on the premises when accompanied
- Access policy for restricted areas such as server rooms
- Requirement that service providers with access comply with data protection regulations
- Access for cleaning and maintenance staff
- Access permissions defined and documented, e.g., logging
- Security services, video surveillance
- Documentation/logging of the locking system

3.1.2 Access control

- Process for assigning, modifying, and deactivating user accounts and permissions
- Login with a personal username and password
- Regular password changes
- Authorization policies for IT systems, applications, and data
- Firewall policy
- External access to the corporate network
- Malware protection, EDR
- Automatic screen lock
- Regular Review of User Accounts
- Awareness / training courses
- Password complexity and length
- IT System Servicing
- Patch management
- Deletion and Disposal of Data and IT Equipment
- System-level lockout for failed login attempts
- Role-Based Administration
- System Hardening
- Internal Audits
- Change management
- Monitoring and logging of permission changes
- Password security for system accounts

3.1.3 Access Control

- Process for Granting, Modifying, and Revoking Access Rights
- Access protection for data backups
- Access concepts for IT systems, applications, and data
- Permissions and role concepts
- Permissions concept for IT administrators
- Logging of access during administrative activities
- Process for granting, modifying, and revoking access rights based on the need-to-know principle
- Regular review of access permissions
- Encrypted Communication Channels
- Zone and tier concept, e.g., DMZ, reverse proxy
- Conducting security audits
- Network security features, e.g., port security
- Network segmentation
- Data deletion policy
- Encryption of IT systems, applications, databases, and transmission channels
- Multi-factor authentication for external access
- IDS / IPS
- Vulnerability management
- Monitoring of Privileged Access

3.1.4 Separation of duties

- Logical separation of data, e.g., multi-tenant capability in applications
- Separation of production and test systems
- Permissions for controlling access to data
- Database Segregation
- System Environment Separation

3.1.5 Pseudonymization

- Pseudonymization during data transfer
- Pseudonymization in Analyses

3.2 Integrity

3.2.1 Transfer Controls

- Organizational measures to prevent data transfer
- Training courses on Data Protection
- Secure physical transport
- Encrypted Communication Channels
- Logging of data disclosure
- Encryption of transmission channels
- Logging of remote access

3.2.2 Input control

- Logs of entries, changes, and deletions
- System-level restriction of write and delete permissions

3.2.3 Order control

- Obligations of subProcessors: confidentiality, data confidentiality, telecommunications confidentiality
- Training courses for the Processor's employees
- Data processing agreements with subProcessors
- Obligation of sub-Processors to comply with the data protection policy
- Processor's Duty to Audit SubProcessors
- Employees' Obligations: Data Confidentiality, Telecommunications Confidentiality
- Access rights, rights to information, and rights of inspection granted by the Processor to the Controller

3.3 Availability

3.3.1 Availability Monitoring

- Securing server rooms
- Patch management
- Fire safety measures
- Regular servicing
- Data backup strategy for IT systems and configuration data, including functional testing
- Outsourcing of data backup
- SLAs with service providers
- Monitoring of IT systems
- Network plan, IT asset management
- Uninterruptible Power Supply (UPS), lightning protection
- Monitoring of environmental parameters, e.g., temperature, humidity
- Uninterruptible power supply for controlled shutdown in an emergency
- Redundancy (IT systems, network, spare hardware), mirrored systems, virtualization, clusters
- Distribution of IT services across multiple systems
- Documented data backup strategy
- IT emergency management
- Redundant power and data connections
- Servicing of utility infrastructure
- Monitoring of the technical utility infrastructure (HVAC, UPS, emergency power supply)
- High-availability systems (Kubernetes, etc.)
- Geographic redundancy of IT systems
- Multi-tier system landscape, e.g., design and development, quality assurance, production
- Emergency power supply
- Redundant air conditioning
- Secure storage of data media and documents in a safe

3.4 Confidentiality

3.4.1 Access control

- Visitor Policy
- Access control to buildings and rooms
- Granting, monitoring, and revoking access rights according to the need-to-know principle
- Physical security of buildings and rooms, e.g., fencing, doors
- Visitors may only enter and remain on the premises when accompanied
- Access policy for restricted areas such as server rooms
- Requirement that service providers with access comply with data protection regulations
- Access for cleaning and maintenance staff
- Access permissions defined and documented, e.g., logging
- Security services, video surveillance
- Documentation/logging of the locking system

3.4.2 Access control

- Process for assigning, modifying, and deactivating user accounts and permissions
- Login with a personal username and password
- Regular password changes
- Authorization policies for IT systems, applications, and data
- Firewall policy
- External access to the corporate network
- Malware protection, EDR
- Automatic screen lock
- Regular Review of User Accounts
- Awareness / training courses
- Password complexity and length
- Servicing of IT systems
- Patch Management
- Deletion and Disposal of Data and IT Equipment
- System-level lockout in case of failed login attempts
- Role-Based Administration
- System Hardening
- Internal Audits
- Change management
- Monitoring and logging of authorization changes
- Password security for system accounts

3.4.3 Access Control

- Process for Granting, Modifying, and Revoking Access Rights
- Access protection for data backups
- Access policies for IT systems, applications, and data
- Permissions and role concepts
- Permissions concept for IT administrators
- Logging of access during administrative activities
- Process for granting, modifying, and revoking access rights based on the need-to-know principle
- Regular review of access permissions
- Encrypted Communication Channels
- Zone and tier concept, e.g., DMZ, reverse proxy
- Conducting security audits
- Network security features, e.g., port security
- Network segmentation
- Data deletion policy
- Encryption of IT systems, applications, databases, and transmission channels
- Multi-factor authentication for external access
- IDS / IPS
- Vulnerability management
- Monitoring of privileged access

3.4.4 Segmentation control

- Logical separation of data, e.g., multi-tenant capability in applications
- Separation of Production and Test Systems
- Permissions for Controlling Access to Data
- Database Segregation
- System Environment Separation

3.4.5 Pseudonymization

- Pseudonymization during data transfer
- Pseudonymization in Analyses

3.5 Integrity

3.5.1 Transfer Controls

- Organizational measures to prevent data transfer
- Training courses on Data Protection
- Secure physical transport
- Encrypted Communication Channels
- Logging of data disclosure
- Encryption of transmission channels
- Logging of remote access

3.5.2 Input control

- Logs of entries, changes, and deletions
- System-level restriction of write and delete permissions

3.5.3 Order control

- Obligations of subProcessors: confidentiality, data confidentiality, telecommunications confidentiality
- Training courses for the Processor's employees
- Data processing agreements with subProcessors
- Obligation of sub-Processors to comply with the data protection policy
- Processor's Duty to Audit SubProcessors
- Employees' Obligations: Data Confidentiality, Telecommunications Confidentiality
- Access rights, rights to information, and rights of inspection granted by the Processor to the Controller

3.6 Availability

3.6.1 Availability Monitoring

- Securing server rooms
- Patch management
- Fire safety measures
- Regular servicing
- Data backup strategy for IT systems and configuration data, including functional testing
- Outsourcing of data backup
- SLAs with service providers
- Monitoring of IT systems
- Network plan, IT asset management
- Uninterruptible Power Supply (UPS), lightning protection
- Monitoring of environmental parameters, e.g., temperature, humidity
- Uninterruptible power supply for controlled shutdown in an emergency
- Redundancy (IT systems, network, spare hardware), mirrored systems, virtualization, clusters
- Distribution of IT services across multiple systems
- Documented data backup strategy
- IT emergency management
- Redundant power and data connections
- Servicing of utility infrastructure
- Monitoring of technical support infrastructure (air conditioning, UPS, emergency power supply)
- High-availability systems (Kubernetes, etc.)
- Geographic redundancy of IT systems
- Multi-tier system landscape, e.g., design and development, quality assurance, production
- Emergency power supply
- Redundant air conditioning
- Secure storage of data media and documents in a safe