DATA PROTECTION

Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR

This Data Processing Agreement (DPA) is the standard data processing agreement of EVOMECS GmbH, Kanalstraße 6, 80538 Munich, Germany (hereinafter "EVOMECS") within the meaning of Art. 28 GDPR. It applies to all customers (hereinafter "Controller") for whom EVOMECS processes personal data within the scope of cloud services or support, maintenance, servicing or consulting services, and becomes part of the respective contractual relationship by reference.

This English version is a convenience translation. In the event of any discrepancy, the German version shall prevail.

1. Relationship to the Main Contract and Order of Precedence

(1) This DPA supplements the contracts concluded between the parties, in particular the EVOMECS Cloud Terms, Software License Terms, Maintenance Terms and IT Services Terms (hereinafter collectively the "Main Contract").

(2) It becomes part of the contractual agreement by reference in the offer, in the order confirmation or in the ordering process of the EVOMECS online store, in the version valid at the time of conclusion of the contract.

(3) The term of this DPA follows the term of the Main Contract. It does not end as long as EVOMECS still processes personal data of the Controller.

(4) In the event of contradictions between this DPA and the Main Contract, this DPA takes precedence in all matters of data protection. In all other matters, in particular regarding the scope of services and remuneration, the Main Contract applies.

2. Roles of the Parties

(1) The Customer is the controller within the meaning of Art. 4 no. 7 GDPR. It is responsible for the lawfulness of the processing, including the admissibility of processing employee data and any co-determination rights of a works council.

(2) EVOMECS is the processor within the meaning of Art. 4 no. 8 GDPR and processes personal data exclusively on behalf of and on the instructions of the Controller.

(3) Insofar as EVOMECS processes data for its own purposes, such as anonymised and aggregated data under the Main Contract or the Customer's contract and billing data, EVOMECS does not act as a processor in this respect. Anonymised data is not personal data.

3. Subject Matter, Purpose and Duration of Processing

3.1 Cloud operation

(1) In the case of cloud services, EVOMECS operates the EVOMECS software on a cloud infrastructure and processes the Controller's personal data on an ongoing basis for the term of the Main Contract.

(2) The purpose of processing is the provision of the EVOMECS software for the digital control and documentation of the Controller's manufacturing, including storage, data backup, operation, maintenance, support and data export.

(3) Processing takes place exclusively within the European Union or the European Economic Area, unless Clause 9 permits otherwise. The sub-processors used are listed in Annex 2.

3.2 On-premise operation

(1) In on-premise operation, the EVOMECS software runs on systems within the Controller's area of responsibility. EVOMECS has no permanent access to productive data and no control over these systems.

(2) EVOMECS processes personal data in this case only on an ad hoc basis, for a limited time and on instruction, in particular during remote maintenance, support, maintenance or consulting.

3.3 Hybrid scenarios

Combined operating models are permitted. The provisions of Clause 3.1 or 3.2 apply to each part according to the agreed operating model.

4. Types of Data and Data Subjects

(1) Depending on use and configuration, the following types of personal data are processed:

- user and contact data (name, user ID, e-mail address, role, department);
- activity and feedback data (activities booked at workstations and orders, time stamps, quantities, quality characteristics, comments);
- machine and process data, insofar as they can be attributed to a person (e.g. logged-in operator, shift);
- access and log data (login times, IP addresses, system logs);
- content in documents, drawings and attachments, insofar as they contain personal data;
- support and communication content.

(2) Data subjects are employees of the Controller, other users authorised by the Controller and contact persons of the Controller's customers and suppliers, insofar as their data is stored in the EVOMECS software.

(3) The processing of special categories of personal data (Art. 9 GDPR) is not intended. The Controller will not introduce such data into the EVOMECS software.

5. Instructions

(1) EVOMECS processes personal data only on documented instructions from the Controller, including with regard to transfers to third countries, unless EVOMECS is required to do so by Union or Member State law. In such a case, EVOMECS informs the Controller of that legal requirement before processing, unless that law prohibits this.

(2) The instructions are set out in the Main Contract and this DPA. The Controller may supplement or change them in text form.

(3) If EVOMECS considers that an instruction infringes data protection provisions, EVOMECS informs the Controller without undue delay and may suspend its execution until the Controller confirms or changes it.

(4) Instructions that go beyond the contractually agreed scope of services are remunerated by the Controller in accordance with the

IT Services Terms, unless they become necessary due to a breach by EVOMECS.

6. Confidentiality

EVOMECS ensures that all persons who have access to the Controller's personal data have committed themselves to confidentiality or are under a statutory obligation of confidentiality and have been familiarised with the relevant data protection provisions. Access is limited to persons who require it to provide the services. The obligation continues after the end of their activity.

7. Technical and Organisational Measures

(1) EVOMECS takes the technical and organisational measures described in Annex 1 pursuant to Art. 32 GDPR in order to ensure a level of protection appropriate to the risk.

(2) The measures are subject to technical progress. EVOMECS may replace them with equivalent or better measures; the level of protection must not fall below the agreed level. EVOMECS documents material changes.

(3) Allocation of responsibilities:

- In cloud operation, EVOMECS is responsible for the security of the application, data storage and data backup, together with the infrastructure provider named in Annex 2.
- In every operating model, the Controller is responsible for managing its user accounts and authorisations, protecting access data and the security of its end devices, networks and machine connections.
- In on-premise operation, the Controller is additionally responsible for the security of its servers, systems and data backups.

8. Sub-processors

(1) The Controller grants EVOMECS general authorisation to engage further processors (sub-processors). The sub-processors engaged at the time of conclusion of the contract are listed in Annex 2 and are deemed approved.

(2) EVOMECS informs the Controller in text form at least four (4) weeks before engaging or replacing a sub-processor. The Controller may object within this period for good cause relating to data protection. If the parties cannot reach agreement, the Controller may terminate the affected contract with effect from the date of the change. The removal of a sub-processor is merely notified.

(3) In the event of imminent danger, in particular if a sub-processor must be replaced at short notice for security reasons, EVOMECS may shorten the period under paragraph 2; the right to object and terminate remains in place.

(4) EVOMECS contractually obliges each sub-processor to data protection obligations that essentially correspond to those of this DPA and remains responsible to the Controller for compliance with these obligations.

(5) Ancillary services without access to the Controller's personal data, such as telecommunications services or cleaning services, do not constitute sub-processing within the meaning of this Clause.

9. Processing Outside the EU/EEA

(1) In cloud operation, data is stored exclusively in data centres within the EU or EEA.

(2) Processing outside the EU or EEA, for example through access by a sub-processor named in Annex 2 in the context of support or communication, is only permitted if the requirements of Art. 44 et seq. GDPR are met, in particular on the basis of an adequacy decision of the EU Commission (e.g. EU-U.S. Data Privacy Framework) or standard contractual clauses.

(3) EVOMECS informs the Controller of the respective legal basis upon request.

10. Assistance Obligations

(1) EVOMECS assists the Controller with appropriate technical and organisational measures in fulfilling the rights of data subjects (Art. 12 to 22 GDPR). If a data subject contacts EVOMECS directly, EVOMECS forwards the request to the Controller without undue delay and does not respond to it itself.

(2) Taking into account the information available, EVOMECS assists the Controller in complying with the obligations under Art. 32 to 36 GDPR, in particular with data protection impact assessments and consultation of the supervisory authority.

(3) In cloud operation, the Controller can generally fulfil requests for access, rectification and erasure itself using the functions of the EVOMECS software. Insofar as further assistance by EVOMECS is required and is not based on a breach by EVOMECS, EVOMECS may charge the effort in accordance with the IT Services Terms.

11. Notification of Personal Data Breaches

(1) EVOMECS notifies the Controller of a personal data breach without undue delay, at the latest within 48 hours after becoming aware of it, at the contact address designated by the Controller.

(2) As far as known, the notification contains the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken and proposed. EVOMECS provides information that is not yet available in phases.

(3) EVOMECS takes the necessary measures to secure the data and mitigate possible adverse consequences without undue delay and assists the Controller with its notification and communication obligations under Art. 33 and 34 GDPR.

12. Evidence and Audits

(1) Upon request, EVOMECS makes available to the Controller all information necessary to demonstrate compliance with this DPA. Evidence may be provided in particular by current attestations, certificates or audit reports of independent bodies, including those of sub-processors (e.g. ISO/IEC 27001 or BSI C5 of the infrastructure provider).

(2) If such evidence is insufficient in an individual case, the Controller is entitled to carry out audits, including inspections, itself or through an auditor bound to confidentiality. Inspections must be announced at least four (4) weeks in advance, take place during normal business hours and must not disrupt operations disproportionately. They are permitted no more than once per calendar year unless there is a specific reason, in particular a personal data breach.

(3) During inspections, the confidentiality of the data of other EVOMECS customers must be maintained. Access to systems or data of other customers is excluded.

(4) Each party bears its own costs for inspections. EVOMECS may charge its effort for inspections beyond the first in a calendar year in accordance with the IT Services Terms, unless the inspection reveals a material breach by EVOMECS.

13. Return and Deletion

(1) After the end of the provision of services, EVOMECS deletes or returns all personal data at the choice of the Controller, unless Union or Member State law requires storage.

(2) In cloud operation, data is returned by way of an export in accordance with the Cloud Terms (Clause 12) in a common, machine-readable format. After expiry of the retrieval period set out there, EVOMECS deletes the data from the production systems; backups are deleted upon expiry of their 14-day retention period. EVOMECS confirms the deletion in text form.

(3) In on-premise operation, the productive data is within the Controller's area of responsibility; a return is not applicable. EVOMECS deletes data received on an ad hoc basis, for example in the context of support, as soon as it is no longer required for the respective purpose, at the latest at the end of the contract.

(4) EVOMECS may retain documentation serving as evidence of proper processing beyond the end of the contract in accordance with statutory retention periods.

14. Liability

(1) The liability provisions of the Main Contract apply to the liability of the parties towards each other. Liability towards data subjects under Art. 82 GDPR remains unaffected.

(2) Internally, each party bears the damage attributable to its own area of responsibility. EVOMECS is not liable for breaches based on instructions of the Controller or on its system and organisational sphere.

15. Final Provisions

(1) Amendments and additions to this DPA must be made in text form. EVOMECS updates Annex 2 in accordance with the procedure under Clause 8.

(2) Contact for data protection enquiries and notifications to EVOMECS: info@evomecs.com, subject "Data protection".

(3) Should any provision of this DPA be invalid, the validity of the remaining provisions shall remain unaffected.

(4) The law and place of jurisdiction agreed in the Main Contract apply.

Annex 1: Technical and Organisational Measures

The measures apply to cloud operation and to support access to on-premise systems.

AREA	MEASURES
Data centre and physical protection	Hosting with an infrastructure provider with certified data centres in the EU (see Annex 2); access control, video surveillance, fire and power failure protection by the provider; evidence via its certificates.
Access control (systems)	Individual user accounts, password policy, lockout after repeated failed attempts.
Access control (data)	Role and authorisation concept based on the need-to-know principle; administrative access only for authorised EVOMECS employees.
Separation control	Logical separation of the data of different customers (multi-tenancy separation); separation of production, test and development environments.
Transfer control	Encrypted transmission in accordance with the state of the art (TLS); secured download for data exports.
Input control	Logging of logins and administrative changes with an appropriate retention period.
Availability and recoverability	Daily data backup, 14-day retention, separate from the production system; system monitoring; regular restore tests.
Organisation	Confidentiality obligation and data protection training of employees; procedure for reporting security incidents; regular review of the measures; careful selection and monitoring of sub-processors.
Remote maintenance (on-premise)	Access only after approval by the Customer, via an encrypted connection, limited in time and logged.

Annex 2: Sub-processors

As of: 10/2026

- STACKIT (Schwarz Digits Cloud GmbH & Co. KG)
- Google (Google Workspace)
- TeamViewer
- Lovable
- Atlassian
- Grafana Labs
- Univedo