Contract for Processing According to Art. 28 GDPR

The following processing agreement is concluded between

the customer using the JUMO cloud[1]

- defined as the controller, and hereinafter referred to as the Client -

and

JUMO GmbH & Co. KG

Moritz-Juchheim-Strasse 1

36039 Fulda, Germany

- defined as the processor, and hereinafter referred to as the Contractor,

pursuant to Art. 28 Section 3 of the EU General Data Protection Regulation:

---

(1) Electronic acquisition of the individual customer address

1. Introduction, scope, definitions

(1) This contract governs the rights and obligations of the Client and Contractor (hereinafter referred to as the "Parties") with respect to the processing of personal data, pursuant to Art. 4 No. 8 and Art. 28 of Regulation (EU) 2016/679 – General Data Protection Regulation (hereinafter referred to as the "GDPR").

(2) This contract applies to all tasks for which employees of the Contractor, or tier-two contractors (subcontractors) commissioned by the Contractor, process personal data belonging to the Client.

(3) The terms used in this contract are to be understood pursuant to their definition in the EU General Data Protection Regulation (hereinafter referred to as the "GDPR").

In this context, the Client is considered the "controller" and the Contractor is considered the "processor". The terms "data processing" or "processing" are based on the definition pursuant to Art. 4 No. 2 GDPR. Insofar as declarations must be made "in writing" in the following, this refers to the written form according to Art. 126 German Civil Code (BGB). Declarations may furthermore also be made in another form, provided that this form ensures an appropriate level of traceability.

2. Subject-matter and duration of processing

(1) The processing shall be based on the main contract that is in place between the Parties (maintenance contract, contract for services, etc.) or individual orders that have been placed for the provision of services in the field of servers/networks/automation or software.

(2) The Contractor shall be permitted to process personal data only within the context of the main contract, the individual order, and this processing contract – as well as when instructed to do so by the Client.

(3) The data shall be processed for an indefinite period until this contract or the main contract/contractual relationship is terminated by one of the Parties.

3. Nature and purpose of processing, type of data, categories of data subjects

The nature and purpose of the processing, the type of personal data, and the categories of the data subjects of the data processing arise from Appendix 1 (Details of processing) to this contract.

4. Obligations of the Contractor

(1) The Contractor shall process personal data only as contractually agreed or as instructed by the Client, unless the Contractor is legally obligated to process the data a certain way. If the Contractor is subject to such obligations, the Contractor shall notify the Client accordingly before processing the data, unless the Contractor is legally prohibited from sending such notification. In addition, the Contractor shall not use the data transferred for processing for any other purposes, in particular not for its own purposes.

(2) The Contractor confirms that it is familiar with the relevant, general data protection regulations. The Contractor shall observe the principles of orderly data processing.

(3) The Contractor undertakes to process the data in strict confidence.

(4) Persons who may become aware of the data processed as part of the commission must undertake in writing to maintain confidentiality, insofar as they are not already legally subject to a relevant obligation to confidentiality.

(5) The Contractor shall guarantee that the persons it deploys to process the data have become familiar with the relevant data protection provisions and with this contract before starting to process the data. Corresponding measures to train employees and raise their awareness of this topic must be repeated at appropriate intervals. The Contractor shall ensure that persons deployed to processing are appropriately instructed and monitored on an ongoing basis in order to ensure compliance with the data protection requirements.

(6) In connection with the processing that has been commissioned, the Contractor shall support the Client in creating and updating the directory of processing activities and in performing the data protection impact assessment. All necessary information and documentation must be kept available and provided to the Client upon request without delay.

(7) If the Client is subjected to an inspection by supervisory authorities or other entities or if data subjects assert rights against the Client, the Contractor undertakes to support the Client to the necessary extent insofar as the commissioned processing is affected.

(8) The Contractor shall not be permitted to pass on information to third parties or data subjects unless the Client has given its prior consent. The Contractor shall forward any requests sent directly to the Contractor on to the Client without delay.

(9) Insofar as legally required, the Contractor shall designate an expert, reliable person to act as the data protection officer. It must be ensured that this officer is not subject to any conflicts of interest. In cases of doubt, the Client shall be able to contact the data protection officer directly. The Contractor shall inform the Client without delay of the data protection officer's contact details or shall explain why no such officer has been designated. The Contractor shall notify the Client without delay in the event that a different person takes up the role or the officer's internal duties change.

(10) As a basic principle, processing shall occur within the EU or the EEA. Any transfer to a third country shall be permitted only with the Client's express consent and under the conditions stated in Section V GDPR and subject to compliance with the provisions of this contract.

5. Technical and organizational measures

(1) Before starting to process the data, the Contractor shall document the implementation of the necessary technical and organizational measures set out prior to the order being awarded, in particular with respect to the specific execution of the order, and shall submit this information to the Client for review. If the Client accepts the measures, the documented measures shall become the basis of the order. Insofar as the review/an audit by the Client reveals a need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Contractor shall provide the security set out in Art. 28 Section 3(c), Art. 32 GDPR, in particular in connection with Art. 5 Section 1, Section 2 GDPR. In overall terms, the measures to be taken are measures to ensure data security and to ensure a level of security appropriate to the risk with respect to the confidentiality, integrity, availability, and resilience of the systems. In this regard, it is necessary to take into account the state of technology, the costs of implementation, and the nature, scope, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons pursuant to Art. 32 Section 1 GDPR (the specifics set out in Appendix 2 shall apply).

(3) The technical and organizational measures shall be subject to technical progress and further development work. In this respect, the Contractor shall be permitted to implement alternative adequate measures. In this case, the minimum level of security provided by the specified measures must always be achieved. Any significant changes shall be documented.

(4) The Contractor shall guarantee that the data processed as part of the commission shall be strictly segregated from other data sets.

6. Rectification, restriction, and erasure of data

(1) The Contractor shall not be permitted to independently rectify, erase, or restrict the processing of the data processed as part of the commission. It shall only be permitted to do so after having received a documented instruction from the Client. Insofar as a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request on to the Client without delay.

(2) Insofar as these aspects are covered by the scope of service, the Contractor shall, after having received a documented instruction from the Client, directly ensure the erasure concept and the right to be forgotten, to rectification, to data portability, and to access.

7. Sub-contractual relationships

(1) The term "sub-contractual relationships" pursuant to this provision shall be understood to mean services which relate directly to the provision of the main service. It shall not include ancillary services used by the Contractor e.g. as telecommunications services, postal/transportation services, maintenance and user services, or the disposal of data carriers, or other measures to ensure the confidentiality, availability, integrity, and resilience of the hardware and software in data processing equipment. However, in order to ensure the protection and security of the Client's data, the Contractor shall be obligated to also conclude appropriate and legally compliant contractual agreements and carry out inspections in the event that ancillary services are outsourced.

(2) The Contractor shall be permitted to commission subcontractors (other processors) only once the Client has granted its express written/documented consent beforehand.

a) ☐ Subcontracting is not permitted.

b) ☒ The Client consents to the commissioning of the following subcontractors under the condition that a contractual agreement is concluded as specified in Art. 28 Sections 2-4 GDPR:

Subcontractor	Address/country	Service
narz systems GmbH & Co. KG	36358 Herbstein, Germany	Data storage and support

c) ☐ Outsourcing to subcontractors
or

☐ A change to the existing subcontractor
are admissible provided that:

- the Contractor notifies the Client of such outsourcing to subcontractors in writing or in text form and with a reasonable notice period, and
- the Client does not object to the planned outsourcing to the Contractor in writing or in text form by the time the data is transferred, and
- a contractual agreement as specified in Art. 28 Sections 2-4 GDPR forms the basis thereof.

(3) The Client's personal data shall not be permitted to be forwarded to the subcontractor, and the subcontractor shall not be permitted to start work for the first time, until all prerequisites for subcontracting have been fulfilled.

(4) If the subcontractor is to provide the agreed service outside of the EU/EEA, the Contractor shall take corresponding measures to ensure that this is admissible under the data protection regulations. The same shall apply if service providers pursuant to Section 1(2) are to be deployed.

(5) The subcontractor shall not be permitted to outsource the work further. All contractual regulations in the contractual chain shall also be imposed on the additional subcontractor.

8. Quality assurance and other obligations of the Contractor

(1) In addition to complying with the regulations of this order, the Contractor is subject to legal obligations according to Articles 28 to 33 GDPR; in this respect the Contractor shall guarantee compliance with the following stipulations in particular:

a) ☒ Designation in writing of a data protection officer, who shall perform their duties according to Articles 38 and 39 GDPR.
   - ☐ The Client shall be informed of the data protection officer's contact details so that the Client can contact the officer directly. The Client shall be informed of any changes to the data protection officer without delay.
   - ☐ The Contractor has designated the following data protection officer: Mr./Ms. [please enter: first name, surname, organizational unit, telephone, email]. The Client shall be informed of any changes to the data protection officer without delay.
   - ☒ The data protection officer's current contact details are provided on the Contractor's website in a readily accessible form.

b) ☐ The Contractor is not obligated to designate a data protection officer. The Contractor has appointed the following contact person: Mr./Ms. [please enter: first name, surname, organizational unit, telephone, email].

c) ☐ Since the Contractor's headquarters are located outside of the European Union, it has appointed the following representative in the European Union pursuant to Art. 27 Section 1 GDPR: [please enter: first name, surname, organizational unit, telephone, email].

(2) The requirement to maintain confidentiality according to Art. 28 Section 3(2)(b), Art. 29, and Art. 32 Section 4 GDPR shall be complied with. When performing its work, the Contractor shall only deploy employees who have committed themselves to confidentiality and have familiarized themselves with the data protection provisions relevant to them beforehand. The Contractor and any person reporting to the Contractor who has access to personal data, shall only be permitted to process this data in accordance with the Client's instructions, including the powers granted under this contract, unless they are legally obligated to process the data.

(3) The implementation of and compliance with all technical and organizational measures required for this order according to Art. 28 Section 3(2)(c), Art. 32 GDPR (for specifics see Appendix 2) shall have been ensured.

(4) Upon request, the Client and the Contractor shall work together with the supervisory authority in the fulfilment of their tasks. This shall include notifying the Client without delay of any inspections or measures by the supervisory authority insofar as they relate to this order. This shall also apply insofar as a responsible authority opens an investigation into the Contractor as part of infringement or criminal proceedings relating to the treatment of personal data during processing.

(5) Insofar as the Client is subjected on its part to an inspection by the supervisory authority, infringement or criminal proceedings, a liability claim from a data subject or a third party, or another claim in connection with the processing by the Contractor, the Contractor shall support the Client to the best of its ability.

(6) The Contractor shall regularly inspect the internal processes and the technical and organizational measures in order to ensure that the processing performed within its area of responsibility meets the requirements set out in the applicable data protection legislation and that the protection of data subjects' rights is being ensured.

(7) The ability to prove the implemented technical and organizational measures to the Client as part of its inspection powers according to Section 9 in this contract.

9. Rights and obligations of the Client

(1) The Client alone shall assume responsibility for assessing whether the processing that has been commissioned is admissible and for safeguarding the rights of data subjects.

(2) The Client shall place/issue all orders, partial orders, and instructions in documented form. In urgent cases it shall be possible to issue instructions verbally. The Client shall confirm such instructions in documented form without delay.

(3) The Client shall inform the Contractor without delay if it discovers errors or irregularities when inspecting the results of the order.

(4) The Client shall be entitled to perform inspections in consultation with the Contractor or have these performed by inspectors who shall be appointed on a case-by-case basis. By means of spot checks, which shall generally be announced in good time, the Client shall be entitled to make sure that the Contractor is complying with this agreement in its business operations.

(5) The Contractor shall ensure that the Client is able to verify that the Contractor's obligations are being complied with according to Art. 28 GDPR. The Contractor undertakes to provide the Client with the necessary information upon request, and in particular to furnish proof of the implementation of the technical and organizational measures.

(6) Measures that do not solely affect the specific order shall be able to be verified by means of the following:

- ☐ Adherence to an approved code of conduct according to Article 40 GDPR;
- ☐ Certification according to an approved certification mechanism according to Article 42 GDPR;
- ☒ Current certificates, reports, or extracts of reports from independent entities (e.g. auditors, Auditing department, data protection officer, IT Security department, data protection auditors, quality auditors);

☐ Suitable certification by means of an IT security audit or data protection audit (e.g. according to the baseline protection ("Grundschutz") from the German Federal Office for Information Security, ISO 27001).

(7) The Contractor shall be entitled to claim for remuneration for enabling the Client to perform inspections.

10. Notification in the event of breaches by the Contractor

(1) The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 GDPR governing the security of personal data, notification obligations in the event of data breaches, data protection impact assessments, and prior consultations. This shall include, among others:

a) Ensuring an appropriate level of security by means of technical and organizational measures which take into account the context and purposes of the processing as well as the predicted likelihood and severity of a potential breach of rights as a result of security loopholes, and which enable relevant breaches to be identified immediately
b) The obligation to report breaches of personal data to the Client without delay
c) The obligation to support the Client in fulfilling its obligation to provide information to the data subject, and to provide the Client with all relevant information in this respect without delay
d) Supporting the Client in the Client's data protection impact assessment
e) Supporting the Client within the context of prior consultations with the supervisory authority

(2) The Contractor shall be entitled to claim remuneration for support services which are not included in the service description or are not attributable to misconduct on the part of the Contractor.

11. Client's authority to issue instructions

(1) If instructions are issued verbally, the Client shall confirm these without delay (at minimum in text form).

(2) The Contractor shall inform the Client without delay if it believes that an instruction would breach data protection regulations. The Contractor shall be entitled to refrain from carrying out the corresponding instruction until it is confirmed or amended by the Client.

12. Erasure and return of personal data

(1) No copies or duplicates of the data shall be created without the Client being made aware of this. This excludes backup copies insofar as they are required to ensure orderly data processing, as well as data required to comply with statutory retention obligations.

(2) Once the contractually agreed work has been completed or at an earlier point in time if so requested by the Client – but at the latest when the service agreement ends – the Contractor shall provide the Client with all documents which it has received, any results generated from the processing and usage, and any data sets relating to the contractual relationship, or shall destroy these by prior agreement and in accordance with the data protection regulations. The same shall apply to test material and waste material. The record documenting the erasure shall be presented upon request.

(3) Documentation used to prove that data processing has been carried out properly and in accordance with the order shall be retained by the Contractor beyond the end of the contract

in accordance with the respective retention periods. To relieve the burden on the Contractor, the Contractor shall be entitled to hand this documentation over to the Client when the contract ends.

13. Miscellaneous

(1) In the event that the Client's property located at the Contractor is put at risk as a result of measures taken by third parties (such as seizure or confiscation), insolvency or composition proceedings, or other events, the Contractor shall notify the Client without delay.

(2) If individual parts of this agreement are invalid, this shall not affect the rest of the agreement. The invalid agreement shall be replaced by a provision which most closely reflects the original intention of the Parties.

Fulda, 09.06.2020

Location, date

Contractor

The Client's consent will be recorded electronically.

Appendix 1 – Details of processing

1. Nature and purpose of data processing

The data is processed for the following purposes:

Software maintenance, troubleshooting, user support, installation of updates/upgrades, modifications to configurations, programming work

2. Type of personal data

The following types of data constitute the subject-matter of the order:

General data/contact details

☒	Name
☒	Data for business communications (e.g. telephone, email, company address)
☒	Data for private communications (telephone, email, private address)
☐	Nationality
☐	Identity card data/IDs (e.g. passport, driving license, social security number)
☐	Dates of birth/age
☐	(Personal) profiles/image files
☐	Other, please specify:

Contractual data

☒	General contractual data
☐	Settlement and payment data
☐	Bank details/credit card data
☐	Contract history/usage history
☐	Other, please specify:

Creditworthiness data

☐	Payment behavior
☐	Score values
☐	Information on assets
☐	Other, please specify:

Work-related data

☐	Master data
☐	Wage data/salary data/income
☐	Qualifications/development potential/occupational profiles
☐	Data concerning health/social data
☐	Working-time data
☐	Travel booking/settlement data
☐	Workflows
☐	Other, please specify:

Special categories of personal data

☐	Racial/ethnic origin
☐	Political opinions
☐	Religious/philosophical beliefs
☐	Union membership
☐	Genetic data
☐	Biometric data
☐	Data concerning health
☐	Data concerning sex life/sexual orientation
☐	Offenses, convictions, and judgments
☐	Other, please specify:

Services data and IT (usage) data

☒	Device IDs
☒	Access data
☒	Identification data/IDs
☒	Telecommunications data/content of messages
☒	Usage data and connection data/metadata
☒	Image data/video data
☒	Audio data/voice data
☐	Other, please specify:

Vehicle data, location data, and context data

☐	Vehicle identifiers/vehicle identification data/VIN
☐	Vehicle data/vehicle condition data/vehicle analysis data
☐	Context information and environmental information
☐	Location data/location-related data/movement data
☐	Other, please specify:

3. Categories of data subjects

The following categories of people are affected by the data processing:

☒	Customers
☒	Interested parties
☐	Subscribers
☒	Service users
☒	Indirectly involved persons/persons in the vicinity/occupants
☐	Visitors
☐	Attendees at events
☒	Participants in communications
☐	Applicants
☒	Employees
☒	Former employees
☒	Apprentices/interns
☐	Employees' relatives
☐	Shareholders/governing bodies
☐	Business partners
☐	Suppliers and service providers
☐	Consultants
☒	Business contact persons
☐	Sales representatives
☐	Media representatives
☐	Other, please specify:

Appendix 2 – Technical and organizational measures

1. Confidentiality (Art. 32 Section 1(b) GDPR)

- Access control
  No unauthorized access to data processing equipment:
  - Personal transponders
  - Electronic door openers at self-closing exterior doors
  - Records logging the presence of employees and visitors
  - Documented and verifiable arrangements governing keys
  - Burglar alarm system and camera footage
  - Access to data centers granted only to authorized persons
- Access control
  No unauthorized use of systems:
  - Personalized user accounts
  - Secure passwords; two-factor authentication where possible
  - Automatic blocking mechanisms
  - Encryption of mobile data carriers
- Access control
  No unauthorized reading, copying, modification, or removal within the system thanks to the use of authorization concepts and needs-based access rights and by logging access
- Segregation control
  Segregated processing of data collected for different purposes as a result of multi-tenancy

2. Integrity (Art. 32 Section 1(b) GDPR)

- Transfer control
  No unauthorized reading, copying, modification, or removal if data is transferred or transported electronically, e.g. encryption, Virtual Private Networks (VPN), electronic signature
- Input control
  Identification of whether, and by whom, personal data has been entered into, modified in, or removed from data processing systems, e.g. logging, document management

3. Availability and resilience (Art. 32 Section 1(b) GDPR)

- Availability control
  Protection against accidental or willful destruction or loss, e.g. backup strategy

(online/offline; on-site/off-site), uninterruptible power supply (UPS), anti-virus protection, firewall, reporting procedures, and emergency/recovery plans

- Ability to restore availability in a timely manner (Art. 32 Section 1(c) GDPR)

4. Process for regular testing, assessment, and evaluation (Art. 32 Section 1(d) GDPR; Art. 25 Section 1 GDPR)

- Incident management
- Data protection by default (Art. 25 Section 2 GDPR)
- Order control, by means of:

1. Contract on processing according to Art. 28 GDPR
2. Defined authority to issue instructions
3. Designation of a data protection officer by the processor
4. Ensuring the return and/or destruction of data once the order ends