This Data Processing Agreement ("Agreement") is by and between the responsible party **Customer listed on the applicable order form** (hereinafter referred to as "Customer") and the contract processor, Ungerboeck Systems International GmbH, Kaiserstrasse 72, 76137 Karlsruhe, Germany (hereinafter referred to as "Provider").

Preamble

This Agreement sets out in concrete terms the data protection obligations of the contracting parties, which arise from the contractual relationship between the parties and is hereby incorporated into any existing and currently Order Form/Offer/Service Agreement including Provider's Master Subscription Terms and Conditions, Maintenance Agreement, and/or Cloud Hosting Agreement; hereinafter collectively referred to as "Service Agreement".

This Agreement shall apply to all activities wherein employees of the Provider or persons commissioned by the Provider process Personal Data of the Customer. In order to ensure compliance with Applicable Data Protection Laws regarding transfers of Personal Data from a Controller or Processor within the European Economic Area ("EEA"), Switzerland, or United Kingdom ("UK") to a Processor outside the EEA, Switzerland, or UK, and to reflect changes in the law in Europe, Switzerland and the UK following the approval of the new Standard Contractual Clauses by the European Commission and the UK Addendum by the UK's Information Commissioner's Office, the parties hereby amend their data transfer mechanisms, as established in the Agreement, as follows:

1. SUBJECT MATTER AND DURATION OF THE ORDER/CONTRACT

(1) Subject matter

The subject matter of this order is defined in the Service Agreement.

(2) Duration

The duration of the order (term of the order processing) shall correspond to the term of the associated Service Agreement.

2. SPECIFICATION OF THE SUBJECT MATTER OF THE CONTRACT

(1) Type and purpose of the intended processing of data

The scope, type and purpose of the collection, processing and/or use of Personal Data by the Provider for the Customer are specifically described in the Service Agreement. These are in particular:

- Cloud services (hosting) of the database for the use of the software solution
- Processing of related web servers' data stored in databases by the Provider for the performance of support, maintenance, and further development (e.g., support tickets, troubleshooting, operational support, remote meetings (GoToMeeting), etc.)
- Handling of Personal Data for the assignment of rights (exclusively for the web servers) after being commissioned by the Customer.
- Access to log files for error detection and correction.
- Implementation of import, export, and migration processes, including Personal Data (technical and operational support).
- Development and implementation of interfaces for data transfer between systems.

(2) Nature of the data

The processing of Personal Data entails the following types/categories of data:

- Personal master data, such as first name, last name, title/gender, academic title, department/position
- Communication data, e.g., telephone number, e-mail, fax, mobile number

- Contract master data (contractual relationship, product or contractual interest, market segment)
- Customer history
- Contract billing and payment data
- Planning and control data
- Authorizations and system access rights
- Passwords
- Statistical data
- User activities (log files)
- Data entered by the web user
- IP addresses of users

(3) Categories of persons concerned

The categories of persons concerned by the processing include:

- Users of the Customer's web portals (e.g., prospective customers, customers, contractual partners, contact persons)
- Customers
- Prospects and potential prospects
- Subscribers
- Contractual partners
- Employees
- Suppliers
- Contact persons

3. TECHNICAL AND ORGANIZATION MEASURES

(1) The Provider undertakes to comply vis-à-vis the Customer with the technical and organizational measures required to comply with the applicable Personal Data protection regulations. This includes in particular the requirements of Art. 32 of the GDPR. The Provider also undertakes to comply with its obligations under Art. 32(1)(d) of the GDPR to implement a procedure for the regular review of the effectiveness of the technical and organizational measures to ensure the safety of the processing.

(2) The Provider shall establish safety pursuant to Art. 28 (3) c), 32 of the GDPR, particularly in connection with Art. 5 (1), (2) of the GDPR. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability, and the resilience of the systems. In this context, the state of the art, the implementation costs and the nature, scope, and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR shall be taken into consideration.

(3) The status of technical and organizational measures existing at the time of the conclusion of the Service Agreement is attached as **Annex 1**.

(4) The technical and organizational measures are subject to technical progress and further development. In this respect, the Provider shall be permitted to implement alternative adequate measures. In doing so, the security level of the specified measures may not be undercut. Significant changes shall be documented. The Customer may request an up-to-date version of the technical and organizational measures taken by the Provider at any time.

4. CORRECTION, RESTRICTION AND DELETION OF DATA

(1) The Provider shall only process the Personal Data (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from the Customer, including with regard to any transfers, and (iii) as needed to comply with law (in which case, the Provider shall provide prior notice to the Customer of such legal requirement, unless that law prohibits this disclosure).

(2) To the extent covered by the scope of Services, the deletion concept, right to be forgotten, correction, data portability and information shall be ensured directly by the Provider in accordance with documented instructions from the Customer.

5. QUALITY ASSURANCE AND OTHER OBILGATIONS OF THE PROVIDER

In addition to compliance with the provisions in this Order, the Provider shall have statutory obligations pursuant to Art. 28 to 33 of the GDPR; in this respect, the Provider shall, in particular, ensure compliance with the following requirements:

- Written appointment of a chief privacy officer who shall carry out his works in accordance with Art. 38 and 39 of the GDPR. The contact details of the external data protection officer can be viewed at any time on the Provider's website at https://gomomentus.com/privacy-policy which is subject to change for time to time.
- The maintenance of confidentiality pursuant to Art. 28 para. 3 s. 2 lit. b, 29, 32 para. 4 of the GDPR. When carrying out the work, the Provider shall only use employees who have been obligated to maintain confidentiality and have been familiarized in advance with the data protection provisions relevant to them. The Provider and any person subordinate to the Provider who has access to Personal Data may process this data exclusively in accordance with the Customer's instructions, including the powers granted in this Agreement, unless they are legally obliged to process these.
- The implementation of and compliance with all technical and organizational measures required for this order in accordance with Art. 28 para. 3 p. 2 lit. c, 32 of the GDPR (see Annex 1).
- The participation in inquiries from the supervisory authority towards the Customer, as far as they concern this order processing.
- Immediately informing the Customer about control actions and measures of the supervisory authority, insofar as they relate to this Agreement. This shall also apply insofar as a competent authority is investigating the Provider in the context of administrative offense or criminal proceedings with regard to the processing of Personal Data during the order processing.
- Insofar as the Customer is exposed to an inspection by the supervisory authority, administrative offense or criminal proceedings, liability claims by a data subject or a third party or any other claims in connection with the order processing at the Provider, the Provider shall support the Customer to the best of its ability.
- The Provider shall regularly monitor the internal processes as well as the technical and organizational measures to ensure that the Processing in its area of responsibility is carried out in compliance with the requirements of the applicable data protection law, and that the protection of the rights of the Data Subject is ensured.
- Verifiability of the technical and organizational measures taken vis-à-vis the Customer within the scope of its control powers pursuant to Section 7 of this Agreement.

6. SUB-PROCESSOR RELATIONSHIPS

(1) Sub-processor relationships within the scope of this provision shall be understood to be those services which relate directly to the provision of the main Service. This does not include ancillary services which the Provider uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Provider shall be obligated to implement appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the Customer's data even in the case of outsourced ancillary services.

(2) The Provider may, in particular, use the Services of affiliated companies or other vendors, as a sub-processor, to fulfill its obligations under this Agreement. The Provider will maintain a current list of sub-processors used throughout any Services, including the sub-processor’s name and purpose of their processing. Customer may receive notifications of new sub-processors by emailing privacy@gomomentus.com with the subject.

"Subscribe" and once subscribed in this manner Customer will receive notification of new sub-processors before those sub-processors are authorized to process Personal Data on behalf of the Provider. Customer may reasonably object to Provider's use of a new sub-processor by notifying the Provider in writing within 14 days of receiving the notice of intent to authorize via privacy@gomomentus.com. This notice shall explain the reasonable grounds for objection (e.g., if the use of this sub-processor would violate applicable laws or weaken protections for the applicable Personal Data). The Provider will make commercially reasonable efforts to resolve the objection by the Customer.

(3) The Provider shall not transfer any Personal Data (and shall not permit its sub-processors to transfer any Personal Data) without the prior consent of the Customer. The Provider understands that the Customer must approve and document that adequate protection for the Personal Data will exist after the transfer, using contracts that provide sufficient guarantees (such as standard contractual clauses) unless another legal basis for the transfer exists. The Customer hereby consents to the Provider's transfer of Personal Data to the sub-processors described in this Section 6. Additionally, the Customer understands, acknowledges and agrees that the Provider is (and its sub-processors may be) based in the United States, United Kingdom, Australia, New Zealand or India and that the Provider provides (and the sub-processors may provide) Services from the such countries, and the Customer hereby consents to the transfer of Personal Data to such countries for processing by the Provider and its sub-processors in accordance with this Agreement. The Customer hereby approves the commissioning of the sub-processors listed in **Annex 2**.

7. THE CUSTOMER'S CONTROL RIGHTS

(1) The Customer shall have the right, in consultation with the Provider, to carry out inspections or to have them carried out by inspectors to be designated in individual cases by emailing privacy@gomomentus.com.

(2) Following receipt of this request, the parties will discuss and agree in advance on the reasonable scope, start date and duration of this audit, as well as any applicable security and confidentiality controls that may be required. The Provider may charge a fee (based on the Provider's reasonable costs) for any such audit. The Provider will provide the Customer with additional details of this fee including the basis of its calculation, in advance of the audit. Additionally, the Customer will be responsible for any fees charged by any third-party auditor appointed by the Customer for this audit.

8. NOTIFICATION OF VIOLATIONS BY THE PROVIDER

(1) The Provider shall support the Customer in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, data breach notification obligations, data protection impact assessments and prior consultations. These include, among others

a) Ensuring an appropriate level of protection through technical and organizational measures that take into consideration the circumstances and purposes of the processing, as well as the predicted likelihood, and severity of a potential security breach, and allowing for the prompt detection of relevant breach events
b) The obligation to notify personal data breaches to the contracting authority without undue delay
c) The obligation to assist the contracting authority in its duty to inform the data subject and, in this context, to provide it with all relevant information without undue delay
d) The support of the Customer for its data protection impact assessment
e) The support of the Customer in the context of prior consultations with the supervisory authority.

(2) The Provider may claim reasonable remuneration for support services which are not included in the service description, or which are not due to misconduct on the part of the Provider.

9. AUTHORITY OF THE CUSTOMER TO ISSUE INSTRUCTIONS

(1) The Customer shall have the right to issue instructions to the Provider at any time regarding the type, scope, and procedure of data processing. Instructions from the Customer shall initially be stipulated by the Service Agreements and may thereafter be amended, supplemented, or replaced by the parties in an amendment.

(2) Regulations concerning possible remuneration of additional expenses incurred by the Provider due to supplementary instructions from the Customer shall remain unaffected. The Provider shall inform the Customer without delay if the Provider is of the opinion that an instruction violates data protection regulations

or is unable to comply. The Provider shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or changed by the Customer or Customer may suspend its transfer of Personal Data to Provider and/or if applicable terminate its Service Agreement with Provider (in accordance with the terms of the Service Agreements).

10. DELETION AND RETURN OF PERSONAL DATA

(1) Copies or duplicates of the data shall not be made without the knowledge of the Customer. Exceptions to this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data that is required in order to comply with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the Customer - at the latest upon termination of the service agreement - the Provider shall hand over to the Customer all documents that have come into the Provider's possession, created processing and utilization results, as well as data files that are related to the contractual relationship, or destroy them in accordance with data protection requirements after prior consent of Customer.

(3) Documentation which serves as proof of the proper data processing in accordance with the Agreement shall be kept by the Provider beyond the end of the Service Agreement in accordance with the respective retention periods. The Provider may hand them over to the Customer at the end of the Service Agreement, to relieve the Provider.

(4) The Provider may store personal data processed in connection with the order beyond the termination of the Service Agreement, if and to the extent that the Provider is subject to a legal obligation to retain the data. In such cases, the data may only be processed for the purpose of implementing the respective statutory retention obligations. After expiry of the retention obligation, the data must be deleted immediately and if requested, certify to the Customer that this has been done.

11. EU SCCS AND UK ADDENDUM

(1) If Provider Processes Personal Data covered from the EEA, Switzerland, or UK in a country outside of the EEA, Switzerland, or UK that has not received an adequacy decision from the appropriate authorities, such transfer shall take place on the basis of the EU SCCs and/or UK Addendum, as applicable. In the event the EU SCCs and/or UK Addendum are not applicable, parties agree to work in good faith without undue delay to implement an appropriate alternative transfer mechanism authorized under Applicable Data Protection Laws.

(2) To the extent Provider Processes Personal Data covered by the EU Data Protection Laws, FADP, and/or UK Data Protection Laws, as applicable, in a country that has not received an adequacy decision from the European Commission or Swiss or UK authorities, as applicable, the parties hereby incorporate the EU SCCs (for Personal Data covered by EU Data Protection Laws or FADP, as applicable) and the UK Addendum (for Personal Data covered by UK Data Protection Laws), by reference.

(3) Where the EU SCCs apply, they will be deemed completed as follows:

- Module 2 (Controller to Processor) will apply where Customer is a Controller of Personal Data and Provider is a Processor of Personal Data, the EU SCCs will be deemed completed as follows:
    - Clause 7 of the EU SCCs, the "Docking Clause (Optional)", shall be deemed incorporated;
    - in Clause 9(a) of the EU SCCs, the parties choose Option 2, 'General Written Authorization', with a time period of fourteen (14) days;
    - the optional wording in Clause 11 of the EU SCCs shall be deemed to not apply;
    - in Clause 12, any claims brought under the EU SCCs shall be subject to the terms and conditions set forth in the Service Agreement. In no event shall any party limit its liability with respect to any Data Subject rights under the EU SCCs; in Clause 17 of the EU SCCs, the Data Exporter and Data Importer agree that the EU SCCs shall be governed by the laws of Federal Republic of Germany and choose Option 1 to this

effect;

- in Clause 18 of the EU SCCs, the Data Exporter and Data Importer agree that any disputes shall be resolved by the courts of Federal Republic of Germany;
- Annexes I.A, I.B, II and III of the EU SCCs shall be deemed completed with the information set out in Annex I and Annex II to this Agreement the contents of which are hereby agreed by the parties; and
- for the purpose of Annex I.C of the EU SCCs, the competent Supervisory Authority is the Supervisory Authority of the country where the Data Exporter is established. If the Data Exporter is not established in the EEA, but the Processing is subject to the GDPR, the competent authority is Supervisory Authority of Federal Republic of Germany.

(4) To the extent Personal Data transfers are subject to FADP, the following shall apply:

- References to the GDPR should be understood as references to FADP and, once effective, the revised FADP insofar as Personal Data transfers are subject to the FADP/the revised FADP.
- The term 'member state', as used in the Approved EU SCCS, shall not be interpreted to limit Data Subjects in Switzerland from being able to sue for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs. Where FADP applies to Processing, the EU SCCs shall also protect the data of legal entities, until the entry into force of the revised FADP (the version enacted on 25 September 2020, as amended).
- For the purposes of Annex I.C of the EU SCCs, where Customer is the Data Exporter and the Personal Data transferred is exclusively subject to FADP, the Swiss Federal Data Protection and Information Commissioner (the "FDPIC") shall be the competent Supervisory Authority. Where the Personal Data transferred is subject to both the FADP and the GDPR, parallel supervision should apply: for the (revised) FADP, the FDPIC shall be the competent Supervisory Authority insofar as the transfer is governed by the (revised) FADP; and for GDPR, the competent Supervisory Authority is (a) the Supervisory Authority of the country where the Data Exporter is established if the Data Exporter is established in the EEA, or (b) the Supervisory Authority of Ireland if the Data Exporter is not established in EEA.

(5) Where the UK Addendum applies, it will be deemed completed as follows:

- Table 1 shall be deemed completed with the information set out in Annex I of this Addendum, as appropriate, the contents of which are hereby agreed by the parties;
- In Table 2, parties select the checkbox that reads: "Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum", and the accompanying table shall be deemed to be completed according to the parties' preferences outlined in Clause 11.4. For the purposes of clause 9 of the UK Addendum, the governing law shall be deemed to be that of England & Wales
- Table 3 shall be deemed completed with the information set out in Annex I and Annex II to this Addendum, the contents of which are hereby agreed by the parties;
- In Table 4, the parties agree that either party may terminate the Addendum as set out in Section 19 of the UK Addendum.

(6) For the avoidance of any doubt, these EU SCCs/UK Addendum shall independently apply to all EEA and UK (where clause 1.6 applies) affiliates of Customer that may use the Services provided by Provider (as defined in the Annex to these EU SCCs, which have been incorporated into this Agreement). For the purpose of the EU SCCs/UK Addendum, the aforementioned Customer EEA and UK (where clause 11(5) applies) affiliates shall each be deemed a Data Exporter and Provider shall be deemed the Data Importer.

12. CHANGES TO THE POLICIES

(1) Provider will communicate all changes to the Agreement (including reasons that justify the changes) or to the list of group members bound by the Agreement:

- to Provider's group members bound by the Agreement via written notice (which may include e-mail or posting on an internal Intranet accessible to all group members); and
- to Customer and the individuals who benefit from the Agreement via online publication on Provider's website (and, if any changes are material in nature, Provider must also actively communicate the material changes to Customer before they take effect, in accordance with paragraph 12.3 below).

(2) If Provider makes any material changes to the Agreement or to the list of group members bound by the Agreement that affect the level of protection offered by the Agreement or otherwise significantly affect the Agreement, Provider will promptly report such changes (including the reasons that justify such changes) to all other Provider group members. If a proposed change to the Agreement will materially affect Provider's processing of personal information on behalf of a Customer, Provider will also:

- actively communicate the proposed change to the affected Customer before it takes effect, and with at least 14-day notice to enable the affected Customer to raise objections; and
- the Customer may then suspend the transfer of Personal Data to Provider and/or if applicable terminate the Service Agreement, in accordance with the terms of the Service Agreement with Provider.

13. DEFINITIONS

(1) Applicable Data Protection Laws: means, the following data protection law(s), as applicable, including any subsequent amendments, modifications and revisions thereto: (i) the EU Regulation 2016/679 entitled "On the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data ("GDPR") and any applicable national laws implemented by EEA member countries; (ii) the Swiss Federal Act of 19 June 1992 on Data Protection (as may be amended or superseded); and (iii) the Data Protection Act 2018 (c. 12) of the United Kingdom.

(2) EU Data Protection Laws: means the European Union ("EU") legislation on the protection of Data Subjects with regard to the Processing of Personal Data and on the free movement of such data, including, in particular the GDPR (together with associated national legislation) and Directive 2002/58/EC, as amended by Directive 2009/136/EC, and as may be further amended or replaced from time to time, in those countries that are members of the EU or EEA, and other data protection or privacy legislation (including any substantially similar legislation that replaces the GDPR or associated national legislation), in force from time to time in those countries that are members of the EU or the EEA, as the case may be.

(3) EU SCCs: means the standard contractual clauses for the transfer of Personal Data, in accordance with Applicable Data Protection Law, to Controllers and Processors established in third countries approved by the European Commission from time to time, the approved version of which in force at the date of signature of this Agreement is that set out in the European Commission's Decision 2021/914 of 4 June 2021,as such standard contractual clauses are available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard- contractual-clauses-scc_en and as may be amended or replaced by the European Commission from time to time.

(4) FADP: means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1) and Ordinances SR 235.11 and SR 235.13, as amended and applicable, and, once effective on 1 September 2023 (or such other date as established by Swiss law), the revised FADP version of 25 September 2020, as amended and applicable.

(5) Personal Data: means any information relating, directly or indirectly, to an identified or identifiable natural person that is Processed by Provider or Sub-processors under the Service Agreement. Without limiting the generality of the foregoing, "Personal Data" includes but is not limited to "Personal Data," "Personal Information" and similar terms as defined under Applicable Data Protection Laws to the extent such data is Processed under the Agreement.

(6) Processor Group: means Provider and any entity which controls, is controlled by, or is under common control with, Provider.

(7) Services: means the functions that Provider performs on behalf of Customer as set forth in the Service Agreement.

(8) UK Addendum: means the UK 'International Data Transfer Addendum to the EU Commission Standard Contractual Clauses', available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as adopted, amended or updated by the UK's Information Commissioner's Office, Parliament or Secretary of State.

(9) UK Data Protection Laws: means the Data Protection Act 2018 (DPA 2018), as amended, and EU GDPR, as incorporated into UK law as the UK GDPR, as amended, and any other applicable UK data protection laws, or regulatory Codes of Conduct or other guidance that may be issued from time to time.

(10) Any other capitalized terms that are not defined herein shall have the meaning provided under the Agreement or Applicable Data Protection Laws. A reference to any term or section of Applicable Data Protection Laws means the version as amended.

IN WITNESS WHEREOF, the parties have executed this Agreement by their duly authorized representatives effective as of the date of the Service Agreement.

Annex I

This Annex describes the types of data transferred by Data Exporters and the purposes for which that Data may be Processed by the Processors/Data Importers. This Annex is subject to the terms of the Agreement. Capitalized terms not defined in this Annex will have the meaning attributed to them in the main body of the Agreement or in Applicable Data Protection Laws.

Data Exporter:

- The Data Exporter is: Customer as provided in the Service Agreement.
- Name (full legal name): As provided in the Service Agreement.
- Trading name (if different): As provided in the Service Agreement.
- Address: As provided in the Service Agreement.
- Official registration number (if any) (company number or similar identifier): As provided in the Service Agreement.
- Contact person's name, position, and contact details: As provided in the Service Agreement.
- Activities relevant to the data transferred under these Clauses: As provided in this Agreement and the Service Agreement.
- Signature and date: Executed on the same day as the Agreement, which shall be deemed executed the date it is accepted by signing through DocuSign.
- Role (controller/processor): Where the Customer determines the purposes and means of the Processing of Personal Data, its role is a Controller; where the Customer acts on behalf of and under the instructions of a Controller, its role is a Processor.

Data Importers:

- The Data Importer is: Ungerboeck Systems International GmbH or as otherwise provided in the Agreement signature block.
- Name (full legal name): Ungerboeck Systems International GmbH
- Address: c/o Baker Tilly, Cecilienallee 6, 40474 Düsseldorf Germany
- Contact person's name, position, and contact details:
    - Mr. Ken Bell, Chief Information Security Officer and Data Protection Officer (Global); privacy@gomomentus.com
    - Mr. Matthew Epps, General Counsel legal@gomomentus.com
- Activities relevant to the data transferred under these Clauses: Processing as specified in the Agreement, Service Agreement and according to documented instructions on behalf of Customer.
- Signature and date: Executed on the same day as the Agreement, which shall be deemed executed the date it is accepted by signing through DocuSign.
- Role (controller/processor): Processor

Categories of Data Subjects. This section will be deemed completed as described in the Agreement.

Type of Personal Data. This section will be deemed completed as described in the Agreement.

Sensitive Personal Data. This section will be deemed completed as described in the Agreement.

Frequency of the processing: This Processing will be on a continuous basis.

Nature and purpose of the Processing: Provider shall collect, Process, and use all Personal Data solely for the purpose of the Processing as specified in the Agreement and according to documented instructions on behalf of Customer.

Duration. The duration of the data Processing shall depend on the term of the Service Agreement.

Retention Period. The retention period of the Personal Data is for the duration of the Agreement or as otherwise described therein.

Sub-processors. This section will be deemed completed as described in the Agreement, Annex II and amended from time to time.

Technical-Organizational Measures

For more information on security measures in the Ungerboeck cloud environment, please refer to the following pages. For more information about privacy at Ungerboeck Systems International GmbH, please see our Privacy Policy at https://gomomentus.com/privacy-policy. For more information on the security measures of Ungerboeck's cloud provider Amazon Web Services, please visit the AWS website at https://aws.amazon.com/de/compliance/gdpr-center/.

A. Technical-organizational measures at the Ungerboeck sites.

1. Confidentiality (Art. 32 para. 1 lit. b of the GDPR)

- Access management and control
  - The main entrance is locked. Those authorized to access the office premises are either in possession of a chip card or a key. Central card or key issuance including logging.
  - Video surveillance at the main entrance to the office premises.
  - Rooms worth protecting (e.g., server room) are always locked. Only employees who need access to these rooms for their professional tasks have access to these rooms.
- Electronic access management
  - When accessing the CRM system, users identify themselves with their user ID and password.
  - Available WiFi connection for the office is password protected.
  - An error condition triggered by an incorrect authorization to the system will result in the blocking of access to the system after a defined number of attempts.
  - User IDs and passwords are created in accordance with the Ungerboeck password policy (special characters, minimum length requirements and regular password changes).
  - Guidelines are in place for employees working from home, mobile devices or on-site at the customer.
  - Security policies and concepts for the measures described below are in place and are reviewed and updated annually.
- Separation control
  - Ungerboeck follows the principles of segregation of duties and the least privilege principle (as few rights as possible). This is enforced by means of access requests and reviews, among other things.
  - Development and production environments are separated, and permissions are granted per environment.
- Pseudonymization (Art. 32 para. 1 lit. a of the GDPR; Art. 25 para. 1 of the GDPR).
  - Pseudonymization for customers is possible on request at the CRM system and is performed manually, if necessary. Otherwise, data can be blocked or anonymized.
  - If Ungerboeck uses aggregated data for internal purposes, this information is pseudonymized.
  - There are security guidelines and concepts for the measures described below, and these are reviewed and updated annually.

2. Integrity (Art. 32 para. 1 lit. b DSGVO)

- Transfer control
  - There are authorized data transfer methods (MediaShuttle, SFTP). The procedures are documented.
  - The request and transmission of database copies is documented in the corresponding support ticket.

- Internet access is protected against eavesdropping via VPN and TSL/SSL encryption mechanisms. Transferred files are regularly, randomly checked for integrity.
- E-mails containing very sensitive information are encrypted (e-mail encryption in Office 365).
- Security policies and concepts for the measures described below are in place and are reviewed and updated annually.

- Input control
  - The entry and modification of master data are recorded in log files in the CRM system.
  - All records are summarized centrally via an enterprise SIEM tool.
  - Access within the CRM system is controlled by custom configuration of software settings (user roles, access rights, field encryption or masking, etc.).
  - Security policies and concepts for the measures described below are in place and are reviewed and updated annually.

3. Availability and resilience (Art. 32 para. 1 lit. b of the GDPR)

- Availability control
  - Up-to-date virus protection is installed. Firewall systems are in use.
  - Regular, random integrity tests of the backups of local servers.
- Rapid recoverability (Art. 32 Para. 1 lit. c of the GDPR).
  - Personal Data backup concept for the local servers has been implemented.
  - Global crisis plan ("Global Disaster Recovery Plan") is in place, covering all offices and data centers. RTOs and RPOs are documented in our Business Continuity and Disaster Recovery Plan.
  - Security policies and concepts for the measures described below are in place and are reviewed and updated annually.

4. Procedures for regular review, assessment, and evaluation (Art. 32 (1) (d) of the GDPR; Art. 25 (1) of the GDPR).

- Personal Data protection management
  - Regular data protection training for the Provider's employees.
  - Regular cyber security training for the Provider's employees
  - Internal employee handbook consisting of internal data protection and IT policies on information security and data protection measures in the EMEA organization, including policies for employees working from home, mobile devices, or on-site at the customer.
  - In addition to the external data protection officer, an internal data protection coordinator was appointed for the EMEA organization.
  - Formation of a global data protection team to strengthen IT security and enterprise-wide data protection management.
- Incident Response Management
  - Incident Response Plan is documented and reviewed annually.
  - Incident Response Plan is tested at least annually as part of BC/DR testing.
  - There is an Incident Response Team that is aware of its responsibilities.
  - Security guidelines and concepts for the measures described below are in place and are reviewed and updated annually.
- Personal Data protection-friendly default settings (Art. 25 para. 2 of the GDPR)
  - Ungerboeck Systems International GmbH supports GDPR-compliant software solutions by means of "data protection through technology design" and "data protection through privacy-friendly default

settings". An appropriate level of data protection can be achieved through the settings in the software solution and through the individual configuration of the settings depending on the respective function (e.g., through access rights, field encryption or field masking, etc.).

- Contractual obligations
  - Further details on contractual obligations are contained in the respective Service Agreement with the Customer.
  - Obligation to follow instructions, notification obligations, and audit rights are regulated in this Agreement.
  - Employees of the Customer who may issue instructions to the Provider shall be named by the Customer's management in the Service Agreement.

B. Technical-organizational measures in the Ungerboeck Cloud environments

For Cloud Environments, Ungerboeck uses the industry leading cloud provider, Amazon Web Services ("AWS") for maximum scalability and reliability of Cloud Environments as well as offsite backup and disaster recovery.

"Under the AWS shared responsibility model, AWS provides a global secure infrastructure and foundation compute, storage, networking, and database services, as well as higher level services. AWS provides a range of security services and features which AWS customers (Ungerboeck) can use to secure their assets. AWS customers (Ungerboeck) are responsible for protecting the confidentiality, integrity, and availability of their data in the cloud, and for meeting specific business requirements for information protection."
(Source: Amazon Web Services – Security Best Practices Whitepaper)

"Amazon Web Services (AWS) operates, manages and controls the components from the host operating system and virtualization layer, down to the physical security of the facilities wherein the AWS services operate. The customer (Ungerboeck) is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS provided security group firewall and other security-related features."
(Source: Amazon Web Services – EU Data Protection Whitepaper)

Please note: The measures described below are subject to change based on the availability of AWS services and the state of the art. The following list does not contain the complete technical and organizational measures taken by the Provider but is only intended to provide the Customer with an insight into the measures taken. Further details on Ungerboeck's use of Amazon Web Services and security controls are available upon request.

1. AWS Infrastructure:
   - For more information on the security and compliance measures of the Ungerboeck's cloud provider, Amazon Web Services, please visit the AWS Website.

2. Security measures in the Ungerboeck Cloud environment:
   - Databases for EU customers are hosted in the EU.
   - Ungerboeck employs multiple layers of firewalls and network security tools to protect data boundaries.
   - All publicly accessible access points are isolated from core components by access control lists. Only necessary ports ingress and egress from hosted environments are open.
   - Application access is controlled by built-in LDAP authentication and all access points are protected by SSL/TSL encryption.
   - Access via IP systems is disconnected after a set time when not in use, the so-called session timeout. Web server sessions are terminated by the server according to a defined time period.
   - Anti-virus software and anti-malware software is deployed on all servers, updated daily, and scanned regularly.
   - All servers are protected by an industry-leading Intrusion Prevention System (IPS) that scans network

traffic and identifies methods to detect malicious files on the network.

- Sensitive data, such as password and credit card information within the database, is encrypted using 256-bit AES with split-key methods.
- Transmission of data ingress and egress to the application are protected by TLS 1.2 encryption or higher.
- Customer data is logically separated and secured on a non-shared database schema and application instance.
- Unused services and applications are removed or disabled where possible.
- The latest security updates and patches are installed in systems during regular maintenance.
- Multi-factor authentication is required to access management consoles, if available.
- Access to system components and data is limited to individuals whose jobs require such access, as well as minimal access privileges that are required to perform the corresponding tasks.
- Ungerboeck enforces complex password policies as required by PCI-DSS compliance.
- Ungerboeck uses fully managed cloud-based security and compliance services to monitor, detect and immediately respond to unwanted security incidents.
- Ungerboeck has a 24x7 log monitoring, analysis, and review, in order to collect, aggregate, and search log data from cloud, server, application, security and network assets in the Ungerboeck Cloud.
- Ungerboeck has a 24x7 vSOC that performs continuous monitoring of all production systems.
- Ungerboeck provides 24x7 monitoring of production systems using industry standard practices that alert responsible Ungerboeck personnel to system performance and resource utilization.
- Ungerboeck employs a combination of technologies such as load balancing, server farming, mirroring, and database maintenance plans to achieve high availability, redundancy, and failover.

Annex 2 – Sub-Processor

Sub-processor / Country	Services
Amazon Web Services, Inc. ("AWS") United States of America	Cloud services (hosting) of the database to use the software solution, as well as test databases in the cloud for customers with appropriate Customer Success Plan. Use of AWS data centers in Europe.
Ungerboeck Affiliates • Ungerboeck Systems International, LLC; United States of America and New Zealand • Ungerboeck Software International, Pty Ltd.; Australia and New Zealand • Oletha Pyt Ltd; India • Ungerboeck Systems International GmbH; United Kingdom	Support for the contract execution: • Support services ("Follow-the-Sun") and technical services; • Alpha/Beta/Early Adopter Program; • Web sessions and online meetings; • Remote or on-site services; • Technical monitoring of the cloud environment (availability and performance monitoring, as well as troubleshooting in the event of a malfunction or outage outside of Customer's regular office hours); • Applies to non-hosted (on-premises) customers only: For support tests it may be necessary to test with the Customer's actual data, to be able to reproduce an error. For this purpose, the Customer is asked to provide a copy of his database via MediaShuttle (alternatively, the Customer can upload the database copy to the secured EU FTP server).
Zendesk, Inc. United States of America	Support center and knowledge base Ticket system for processing support tickets for Ungerboeck software, provision of the platform, servers are located in the USA.
LogMeIn, Inc. United States of America	GoToMeeting, GoToWebinar
NITOR Infotech Pvt. Ltd. India	Technical developments, quality tests
Altaa Vistaa Business Solutions Pvt Ltd, India	Customer Success Services, other contractual services (mainly assigned for, but not limited to, English speaking projects)
OuiOui Lyon France	Technical training and similar services for French-speaking customers
Datajust B.V. (Storecove), Netherlands	Integration of e-billing in Ungerboeck software (PEPPOL) / Accesspoint as a service
Stripe, Inc., United States of America	Upon subscription of the proposed services (Ungerboeck Payments / Payment Processing Services through Ungerboeck Software)
Rossum Czech Republic s.r.o., Czech Republic	Upon subscription of the proposed services (Accounts Payable Automation through Ungerboeck Software)
DocuSign Inc., United States of America	Upon subscription of the proposed services (Electronic Signature integration in Ungerboeck Software including – if applicable - envelope provision)
Jotform, Inc., United States of America	Upon subscription of the proposed services (Implementation of online forms)
Twilio Inc., United States of America	Upon customer request or approval of custom solution proposal (SendGrid Emails in Ungerboeck Software)
Signiant Inc., Unites States of America	Use of MediaShuttle service to upload and transfer database copies into the Ungerboeck Cloud Environment; used by onpremise customers upon Ungerboeck's request

Dynatrace, LLC, Unites States of America	Third party monitoring and logging platform that Ungerboeck uses for ingesting, parsing, querying, and performing analytics on Ungerboeck applications and infrastructure logs.
Azure (Microsoft), Unites States of America	Cloud service provider for hosting shared services projects across the Ungerboeck product portfolio.
Okta, Inc. Unites States of America	Identity provider
AC PM LLC (Postmark) Unites States of America	Email service provider
Spreedly, Inc., Unites States of America	Payment processing platform
84codes AB, Sweden	Cloud-managed RabbitMQ for message queuing services
AlertLogic, United States of America	MDR solutions provide single pane-of-glass visibility across public cloud, hybrid, and on-premises environments, providing vital insights on your security posture, and detecting and responding to threats to your business.
Atlassian Australia	Used to manage all development and product related activities. In some cases, support tickets and information from those tickets can make it's way into these systems.
DATADOG, INC. United States of America	Used for Application Performance Monitoring and Infrastructure Monitoring along with log ingestion to ensure proper uptime and performance.
Productboard, Inc. United States of America	Used to capture user feedback and new ideas for the product teams
DELIGHTED, LLC United States of America	Used to validate usage.
Pendo.io, Inc. United States of America	Used to capture usage information of our product offerings
Flowgear LLC United States of America	Used as a Integration Platform as a Service for custom integrations
Smartlook.com, s.r.o., Czech Republic	Product analytics and UX monitoring for websites and mobile applications.
WalkMe Inc. United States of America	Used to provide in-app help via walkthroughs.
Caffeinated Corporation- United Sates of America	Used by Customer Support to streamline and automate support processes.