

# Data Processing Addendum

Status: July 2, 2026

The following Data Processing Terms (hereinafter referred to as the “Terms”) apply to all services provided by aucentiq solutions GmbH (hereinafter referred to as “Processor”) in connection with the use of the Android, iOS, or browser-based app Klubraum (hereinafter also referred to as “Klubraum”).

Any organization that makes the Klubraum app available to its members or otherwise uses the services of the Klubraum app (hereinafter “Controller”) is deemed to have fully accepted these Terms. For the purpose of these Terms, the Controller is the data controller and aucentiq solutions GmbH is the data processor.

## Preamble

---

The following Terms specify the data protection obligations of the contracting parties arising from the use of the Klubraum app in accordance with the general terms of use. They apply to all activities related to the contract in which employees of the Processor or persons appointed by the Processor may come into contact with the Controller's personal data. The basis of the Terms is Article 28 of Regulation (EU) 2016/679 (GDPR).

## §1 Subject Matter, Duration, and Specification of Data Processing

---

The subject matter and duration of the contract, as well as the scope and type of data collection, processing, or use, result from the contract concluded through the use of Klubraum within the framework of the general terms of use. Specifically, the following data, in particular, are part of the data processing:

Type of Data	Purpose of Data Collection, Processing, or Use	Category of Data Subjects
Inventory data (e.g., names, addresses)	Identification and administration of users within a Klubraum group	all users of Klubraum invited and registered by the Controller
Content data (e.g., chats, uploads, appointments, appointment confirmations, ride-sharing)	Improvement of communication, coordination, and organization of Klubraum users	all users of Klubraum invited and registered by the Controller
Contact data (e.g., email addresses)	Invitation and identification of a user to/in a group within Klubraum	all registered users of Klubraum invited by the Controller
Pseudonymized usage data (e.g., features used)	Improvement of the functional scope and user experience of Klubraum	all registered users invited by the Controller; users can object at any time and easily

The term of these Terms is governed by the term of use. The data processing ends upon termination of the usage relationship, at the latest upon termination of the usage contract. The deletion obligations under § 3 and other expressly surviving obligations remain unaffected.

## **§ 2 Scope of Application and Responsibility**

---

1. The Processor processes personal data on behalf of the Controller. This includes activities specified in the terms of use and, if applicable, in a further service description. Within the scope of this contract, the Controller is solely responsible for compliance with the statutory provisions of data protection laws, in particular for the lawfulness of data transfer to the Processor and for the lawfulness of data processing ("Controller" within the meaning of Art. 4 No. 7 GDPR).
2. The instructions are initially laid down in the terms of use and can subsequently be modified, supplemented, or replaced by the Controller in written form or in an electronic format (text form) to the contact point designated by the Processor through individual instructions (individual instruction). Instructions of the Controller relating to data-protection-compliant processing within the meaning of Art. 28 (3) GDPR may be issued by the Controller at any time and without restriction; the Processor shall comply with them. Only instructions that go beyond the contractually agreed scope of services and require a change in service will be treated as a request for a change in service. Oral instructions must be confirmed immediately in writing or in text form.

## **§ 3 Obligations of the Processor**

---

1. The Processor may process data of data subjects only within the framework of the contract and the instructions of the Controller, unless an exception within the meaning of Article 28 (3) (a) GDPR exists. The Processor shall inform the Controller immediately if it is of the opinion that an instruction violates applicable laws. The Processor may suspend the implementation of the instruction until it has been confirmed or modified by the Controller.
2. The Processor will design its internal organization in its area of responsibility in such a way that it meets the specific requirements of data protection. It will take technical and organizational measures for the adequate protection of the Controller's data that meet the requirements of the General Data Protection Regulation (Art. 32 GDPR). The Processor shall take technical and organizational measures that permanently ensure the confidentiality, integrity, availability, and resilience of the systems and services in connection with the processing. The technical and organizational measures taken are described in more detail in the TOM documentation (Annex 2).
3. Security measures include, among other things, the ability to restore the availability of and access to personal customer data in a timely manner after an incident, the ability to ensure the ongoing availability, integrity, and confidentiality of the processing systems and services.
4. The Processor ensures that its employees involved in the processing of the Controller's data and other persons working for the Processor are prohibited from processing the data outside of the instructions. Furthermore, the Processor ensures that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of secrecy. The obligation of confidentiality/secrecy shall continue to apply after the termination of the contract.

5. The Processor will take appropriate steps to ensure that only persons authorized to process personal data have access and that access is granted only to the extent necessary for the provision and improvement of the service.
6. The Processor shall support the Controller, to the extent possible, with appropriate technical and organizational measures in fulfilling the requests and claims of data subjects pursuant to Chapter III of the GDPR as well as in complying with the obligations mentioned in Art. 32 to 36 GDPR. The support owed under Art. 28 (3) (e) and (f) GDPR is provided free of charge.
7. The Processor shall inform the Controller immediately if it becomes aware of breaches of the protection of the Controller's personal data. The Processor shall take the necessary measures to secure the data and to mitigate possible adverse consequences for the data subjects and shall immediately coordinate with the Controller on this matter.
8. The Processor shall name the contact person for data protection issues arising within the scope of the contract to the Controller.
9. The Processor ensures compliance with its obligations under Art. 32 (1) (d) GDPR to implement a process for regularly reviewing the effectiveness of the technical and organizational measures for ensuring the security of the processing.
10. The Controller can at any time request the Processor in writing to close their account/group and/or delete all personal customer data. In this case, the Processor will delete all personal customer data without undue delay, at the latest within thirty (30) days from the request. Data contained in encrypted backups will be overwritten in the course of the regular backup cycle, at the latest within seven (7) days after deletion in the production system. Statutory retention obligations remain unaffected; data stored on this basis will be blocked from further processing and deleted after the respective retention period expires.
11. In the event that the Controller is subject to claims by a data subject regarding possible claims under Art. 82 GDPR, the Processor undertakes to support the Controller in defending the claim within the scope of its possibilities. The support owed under Art. 28 (3) GDPR is provided free of charge. Only insofar as the measures necessary for support go beyond this and involve an extraordinary amount of work for the Processor shall the Controller additionally remunerate these expenses to the Processor in a reasonable amount.

## **§ 4 Obligations of the Controller**

---

1. The Controller must inform the Processor immediately and completely if they discover errors or irregularities in the contract results with regard to data protection regulations.
2. In the event that the Controller is subject to claims by a data subject regarding possible claims under Art. 82 GDPR, § 3 Para. 11 shall apply accordingly.
3. The Controller shall name the contact person for data protection issues arising within the scope of the contract to the Processor.

## **§ 5 Requests of Data Subjects**

---

1. If a data subject contacts the Processor with demands for rectification, deletion, or information, the Processor will refer the data subject to the Controller, provided that an assignment to the Controller is possible according to the information provided by the data subject. The Processor

shall immediately forward the data subject's request to the Controller. The Processor shall support the Controller in accordance with instructions as agreed, within the scope of its possibilities. The Processor is not liable for consequences that result solely from the Controller culpably failing to answer, answer correctly, or answer in a timely manner a data subject's request that was forwarded to it by the Processor in good time.

## **§ 6 Verification Options**

---

1. The Processor demonstrates compliance with the obligations under these Terms primarily by means of suitable evidence, in particular through current certifications and audit reports of the data centers used (e.g., ISO 27001, SOC 2), the documentation of the technical and organizational measures (Annex 2), and the record of processing activities.
2. Insofar as this evidence is not sufficient for the Controller to fulfill its monitoring obligations, the Controller or an auditor commissioned by it and bound to secrecy may carry out data protection and security controls at its own expense. Such controls are permitted with reasonable advance notice (at least 30 days), during normal business hours, without disrupting operations, and at most once a year — as well as on an ad-hoc basis in the case of concrete grounds for suspicion.
3. If the controls require the disclosure of the Processor's business or trade secrets or endanger the Processor's intellectual property, the Controller must appoint an independent third-party auditor who must commit to confidentiality regarding the aforementioned secrets towards the Processor in an appropriate form.

## **§ 7 Subcontractors (Further Processors)**

---

1. The Processor shall only commission a subcontractor for processing activities in accordance with these Terms if this subcontractor is based in the European Economic Area (EEA) or, if based in a third country (in particular the United States of America), the requirements of Art. 44 et seq. GDPR are met. Suitable safeguards include, in particular, a Commission adequacy decision (e.g., the EU-US Data Privacy Framework for appropriately certified recipients), standard contractual clauses together with any additional protective measures required, or another suitable safeguard within the meaning of Art. 46 GDPR.
2. The Controller fundamentally agrees that the Processor may involve other subcontractors meeting the criteria mentioned in paragraph 1 as sub-processors for the processing of personal data in connection with the provision of the service, provided that their use does not lead to violations of applicable law or the Processor's obligations under these Terms. The Processor shall ensure that the involved subcontractors are properly qualified, have concluded a data processing agreement with the Processor, and that these data processing agreements meet the same level of protection as these Terms. The Processor is liable to the Controller for the processing of personal data by the subcontractors.
3. The sub-processors used at the time of conclusion of the contract are listed by name in the list attached as Annex 1; the Controller approves their use. Before adding or replacing a sub-processor, the Processor shall inform the Controller at least 30 days in advance in text form. The Controller may object to the change within 14 days of receipt of the information for an important reason relating to data protection. If the parties cannot resolve a justified objection by mutual

agreement, the Controller is entitled to terminate the user contract and these Terms. In addition, the Processor keeps an up-to-date list of the sub-processors available upon request.

## **§ 8 Data Transmission**

---

1. Personal data will only be processed by the Processor and/or a commissioned subcontractor: (i) within the EEA; or (ii) in a third country outside the EEA, provided that the requirements of Art. 44 et seq. GDPR are met, in particular a Commission adequacy decision (e.g., the EU-US Data Privacy Framework for appropriately certified recipients), standard contractual clauses together with any additional protective measures required, or another suitable safeguard within the meaning of Art. 46 GDPR.
2. Pseudonymized usage data will not be passed on to subcontractors (with the exception of servers rented in the name of the Processor from the hosting providers named in Annex 1) or third parties.

## **§ 9 Liability and Damages**

---

1. The Processor's liability towards the Controller for the slightly negligent breach of material contractual obligations (cardinal obligations) is limited in amount to the foreseeable damage typical for this type of contract at the time the contract was concluded. Material contractual obligations are those whose fulfillment makes the proper performance of the contract possible in the first place and on whose compliance the Controller regularly relies.
2. In the case of slightly negligent breach of non-material contractual obligations, the Processor's liability is excluded.
3. The above limitations of liability do not apply in cases of intent and gross negligence, for damages arising from injury to life, body, or health, or insofar as mandatory statutory provisions stand in the way. Liability towards data subjects under Art. 82 GDPR and the statutory apportionment between the parties in their internal relationship (Art. 82 (5) GDPR) remain unaffected.

## **§ 10 Final Provisions**

---

1. Changes and additions to these Terms and all their components – including any assurances by the Processor – require a written agreement. These changes will be presented in the form of an updated version of these Terms.
2. All disputes arising with respect to the Terms shall be brought before a court in Germany, which shall have exclusive jurisdiction in the decision, unless otherwise specified in writing by the parties.
3. German law applies.
4. Should a provision of these Terms be deemed invalid or unenforceable, the remainder of these Terms shall remain valid and legally effective. The invalid or unenforceable provision will either (i) be modified as necessary to ensure its validity and enforceability while maintaining the parties' intentions as closely as possible, or, if not possible, (ii) be interpreted as if the invalid or unenforceable part had never been included.

## Annexes

---

- **Annex 1 – Sub-processors:** List of the sub-processors used (document “Documentation of the sub-processors of aucentiq solutions GmbH”, in each case the current version).
- **Annex 2 – Technical and Organizational Measures (TOM):** Documentation of the technical and organizational measures of aucentiq solutions GmbH (in each case the current version).