Data processing agreement

1. Preamble

1.1 straiv GmbH, Industriestraße 23, 70565 Stuttgart (hereinafter the "**Processor**" or the "**Contractor**") shall provide the Client (hereinafter the "**Client**") with the services (hereinafter the "**Software**") agreed in the individual agreement / the additionally included General Terms and Conditions and product-specific contractual terms (hereinafter referred to jointly as the "**Main Agreement**").

1.2 The **object of the contract** is the provision of software in a data center for access and use via the Internet as a software-as-a-service solution and the facilitation of the storage of data by the Client on servers operated on behalf of the Contractor. The Processor shall process personal data for the Client within the meaning of Art. 28 GDPR on the basis of this contract.

1.3 The contractually **agreed provision of services** shall be provided exclusively in a Member State of the European Union or in a contracting state to the Agreement on the European Economic Area. Any relocation of the service or parts thereof to a third country shall require the prior consent of the Client and may only take place if the special requirements of Art. 44 et seq. GDPR are met (e.g. adequacy decision of the Commission, standard data protection clauses, approved codes of conduct).

1.4 The **duration of this order** (term) corresponds to the term of the Main Agreement. The term and termination of this contract are governed by the provisions on the term and termination of the Main Agreement. Termination of the Main Agreement shall automatically result in termination of this contract. Isolated termination of this contract is excluded.

2. Purpose, scope, and type of processing; categories of data subjects and type of personal data

2.1 The contract processing of personal data shall be conducted exclusively for a specific purpose. **The purpose, scope, and type of processing** are detailed in the Main Agreement. The collection and/or processing and/or use of the Client's data shall serve the performance of the Contractor's services within the meaning of the Main Agreement.

2.2 The **categories of data subjects** whose personal data will be transferred.

- Users or employeesof the Client ("hotel staff")
- End users or customers of the Client ("hotel guests")

2.3 The **type of personal data** which will be transmitted depending on the selected software package and individual settings of the Client

- Users or employees of the Client ("hotel staff")
    - Master and communication data (e.g. first/last name, e-mail address, telephone number)
    - Usage data (e.g. duration of use, feature used)
    - Image data (e.g. profile picture)

- End users or customers of the Client ("hotel guests")
    - Master and communication data (e.g. first and last name, email address, telephone number)
    - Address data (e.g. street, house number, postcode, city, country)
    - Booking or travel data (e.g. arrival and departure date, booking number, room number)
    - Registration form data (e.g. nationality, date of birth, passport number, digital signature)
    - Billing data (e.g. billing address, prices, services booked (e.g. parking, fitness studio))
    - Image data (e.g. ID card image)
    - Usage data (e.g. start, duration, and end of use, feature used, language used, browser and operating system used)
    - Geodata (e.g. GPS position)

3. Obligations and powers of instruction of the Client

3.1 The Client shall be solely responsible for assessing the permissibility of the processing and safeguarding the rights of the data subjects. Nevertheless, the Processor shall be obliged to forward all requests to the Client without delay if they are recognizably addressed exclusively to the Client.

3.2 The Contractor shall process the Client's personal data only on the Client's documented instructions. As a rule, the Client shall issue all instructions in writing or in a documented electronic format. Oral instructions must be confirmed immediately in writing or in a documented electronic format.

3.3 The Client shall be entitled to verify in an appropriate manner compliance with the technical and organizational measures implemented by the Processor and the obligations set out in this Agreement before the start of the processing and thereafter at regular intervals. The Client shall inform the Processor immediately if it discovers any errors or irregularities during the assessment.

4. Obligations of the Processor

4.1 The Processor shall process personal data exclusively within the framework of the agreements made and in accordance with the Client's instructions, including with regard to the transfer of personal data to a third country or an international organization, unless it is obliged to process the data in a different manner by the laws of the Union or the Member States to which the Processor is subject (e.g. investigations by law enforcement or state security authorities). In such a case, the Processor shall notify the Client of these legal requirements prior to the processing, unless the law in question prohibits such notification due to an important public interest (Art. 28(3) sentence 2 point a) GDPR).

4.2 The Processor shall not use the personal data provided for processing for any other purposes, in particular for its own purposes. Copies or duplicates of personal data shall not be created without the Client's knowledge. The Contractor is entitled to anonymize the data processed by way of contract processing and to use it for its own purposes, e.g. analysis of its own products.

4.3 In the area of personal data processing in accordance with the contract, the Processor shall ensure that all agreed measures are carried out in accordance with the contract. The Processor must cooperate to the extent necessary in the fulfillment of the data subjects' rights pursuant to Art. 12 to 22 GDPR by the Client, in the preparation of the records of processing activities, and in the necessary data protection impact assessments of the Client and, as far as possible, provide the Client with appropriate support (Art. 28(3) sentence 2 points e) and f) GDPR).

4.4 The Processor shall inform the Client immediately if, in its opinion, an instruction issued by the Client violates statutory provisions (Art. 28(3) sentence 3 GDPR). The Processor is authorized to suspend the implementation of the instruction in question until it is confirmed or amended by the controller at the Client after a review.

4.5 The Processor must rectify, erase or restrict the processing of personal data from the contractual relationship if the Client requests this by means of an instruction and this does not conflict with the legitimate interests of the Processor. The Processor may only provide information about personal data from the contractual relationship to third parties or the data subject upon a prior instruction of the Client or with its prior consent.

4.6 The Processor agrees that the Client is entitled—generally after an appointment has been made—to check compliance with the data protection and data security regulations and the contractual agreements to an appropriate and necessary extent, either itself or through third parties commissioned by the Client, in particular by obtaining information and inspecting the stored data and the data processing programs, as well as through on-site checks and inspections (Art. 28(3) sentence 2 point h) GDPR). The commissioned third party may not be in a direct competitive relationship with the Contractor. The Processor warrants that it will assist with these checks where necessary.

4.7 The Contractor may claim remuneration for support services that are not included in the service description or are attributable to misconduct on the part of the Contractor.

4.8 The Processor undertakes to maintain confidentiality when processing the Client's personal data in accordance with the order. This shall continue to apply even after termination of the contract. The Processor warrants that it will familiarize the employees engaged in the performance of the work with the data protection provisions applicable to them before they commence their work and that they will be bound to secrecy in an appropriate manner for the duration of their work and after termination of the employment relationship (Art. 28(3) sentence 2 point b) and Art. 29 GDPR).

4.9 The Processor shall monitor compliance with data protection regulations in its operations. The Processor has appointed an external data protection officer: IITR Datenschutz GmbH, Marienplatz 2, 80331 Munich (phone: +49 89 189 173 60; e-mail: email@iitr.de).

5. Notification obligations of the Processor

The Processor shall immediately notify the Client of any malfunctions or violations by the Processor or the persons employed by the Processor or of breaches of the provisions of data protection law or the specifications stated in the order, as well as any suspicion of data protection violations or irregularities in the processing of personal data. This also applies in particular with regard to any reporting and notification obligations of the Client in accordance with Art. 33 and Art. 34 GDPR. The Processor warrants that it will, if necessary, provide the Client with appropriate support in the fulfillment of its obligations under Art. 33 and 34 GDPR (Art. 28(3) sentence 2 point f) GDPR). Notifications pursuant to Art. 33 or 34 GDPR for the Client may only be made by the Processor following prior instruction in accordance with Section 4 of this contract.

6. Subcontracting relationships with subcontractors (Art. 28(3) sentence 2 point d) GDPR)

6.1 Subcontracting relationships within the meaning of this provision are services that are directly related to the provision of the main service. This does not include ancillary services which the Contractor utilizes, e.g. as telecommunications services, postal/transport services, maintenance and user service, 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 Contractor must implement/take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security, even with regard to outsourced ancillary services.

6.2 The Client grants general approval for the commissioning of subcontractors. In particular, the Client agrees to the commissioning of the subcontractors listed in **Appendix 2**.

6.3 The engagement of additional subcontractors or changing of existing subcontractors are permitted, provided that:

- the Contractor notifies the Client of such outsourcing to subcontractors in writing or in text form a reasonable time in advance, but at least 14 days before the planned assignment, and

- the Client does not object to the planned outsourcing in writing or in text form to the Contractor within 14 days before the time the data is handed over, stating the factual reasons, and
- it is based on a contractual agreement with the subcontractor in accordance with Art. 28 (2-4) GDPR.

6.4 If the Client objects to the processing of personal data by the new subcontractor for objective reasons, each contracting party shall be entitled to terminate the Main Agreement without observing a notice period, in particular if it cannot reasonably be expected to continue the contractual relationship until the agreed termination or until the expiry of a notice period for ordinary termination.

6.5 If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure that the service is permissible under data protection laws by taking appropriate measures.

7. Technical and organizational measures pursuant to Art. 32 GDPR (Art. 28(3) sentence 2 point c) GDPR)

7.1 A level of protection appropriate to the risk to the rights and freedoms of the natural persons affected by the processing shall be guaranteed for the specific contract processing. To this end, the protection objectives of Art. 32(1) GDPR, such as confidentiality, integrity, and availability of the systems and services, as well as their resilience in relation to the type, scope, circumstances, and purpose of the processing, shall be taken into account in such a way that the risk is permanently mitigated by appropriate technical and organizational measures. An appropriate and comprehensible risk assessment methodology shall be used for the processing of personal data in accordance with the contract, which takes into account the probability of occurrence and severity of the risks to the rights and freedoms of those affected by the processing.

7.2 The technical and organizational measures are subject to technical progress and further development. In this connection, the Contractor is permitted to implement alternative adequate measures. The safety level of the defined measures must not be fallen short of. Significant changes must be documented and communicated to the Client.

7.3 The current measures can be found in Appendix 1 and form a part of this contract processing.

8. Obligations of the Processor after termination of the contract (Art. 28(3) sentence 2 point g) GDPR)

Copies or duplicates of the data will not be created without the Client's knowledge. Excluded from 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. After the completion of the contractually agreed work or earlier at the request of the Client—at the latest upon termination of the service agreement—the Contractor shall, at the Client's discretion, either hand over to the Client all documents, processing, and utilization outcomes and data pertaining to the contractual relationship that have come into its possession or destroy them in accordance with data protection regulations. The same applies to test and waste material. The erasure log must be submitted on request.

9. Final provisions

9.1 Agreements on the technical and organizational measures as well as control and audit documents (also relating to subcontractors) must be kept by both contractual partners for their period of validity and subsequently for three further full calendar years. Ancillary agreements must always be made in writing or in a documented electronic format. The place of jurisdiction shall be the court with local jurisdiction for the Contractor.

9.2 If the property or the personal data of the Client to be processed is jeopardized at the Processor by third-party measures (such as seizure or confiscation), by insolvency or composition proceedings or by other events, the Processor must inform the Client immediately. The defense of the right of retention within the meaning of § 273 BGB is excluded with regard to the data processed for the Client and the associated data carriers.

9.3. The German language version of this agreement shall prevail for the interpretation of this agreement.

10. Severability clause

Should one or more clauses of this agreement be invalid or unenforceable in whole or in part, this shall not affect the validity of the remainder of the agreement. The parties shall replace the ineffective or unenforceable clause with a provision that comes as close as possible to the meaning and purpose of the ineffective clause in economic and legal terms. The same applies to any gaps in this agreement.

Appendix 1 – Technical and organizational measures

The Processor warrants that it complies with the minimum requirements described below as part of its data protection concept, which describes the measures required at the Processor for the secure handling of personal data in the context of the contract processing. This data protection concept is based on the EU General Data Protection Regulation (GDPR) and any other measures required by the interested parties. In this connection, the Processor is essentially guided by the provisions of Art. 24, 25 and 32 GDPR. Upon request, the Processor shall provide proof of compliance accordingly.

1. Confidentiality

1.1 Entry control

- Access control system/access only for authorized employees using a transponder key
- Access control at the main entrance door by means of a camera
- Documented key allocation
- Withdrawal of means of access after expiry of authorization
- Reception

1.2. Access control

- Password procedure (including minimum length)
- Server systems can only be used with a password and via an encrypted connection by users with administrator rights (SSH)
- Locking the computer when (temporarily) leaving the workplace
- Firewall/virus scanner
- Organizational instructions for issuing keys
- Immediate blocking of authorizations when employees leave the company (policy/working instructions)
- Secure transmission of authentication secrets (credentials) via HTTPS

1.3 User control

- Differentiated authorizations (e.g. in the form of profiles, roles)
- Binding authorization allocation procedure
- There is an administration concept for transparent requesting and allocation of access rights

- Logging of changes made to authorizations
- Binding procedure for restoring data from backups (restore by IT department on the instructions of management)
- Documentation of network drive access for authorized users (groups)
- Authorization concept is documented
- Assignment of minimal authorizations (need-to-know principle)
- The assignment of generic group IDs or passwords is not provided for in the Software and is not recommended.
- The Software makes it possible to avoid the concentration of functions and enables the functional separation of administrator activities between different qualified persons.
- Data protection-compliant disposal of no longer required data carriers by server service providers

1.4 Pseudonymization
Analyses are pseudonymized unless a personal reference is absolutely necessary for the result.

1.5 Separation control
- The authorization mechanisms available in the systems used enable the exact implementation of the specifications of the authorization concept.

- There is an authorization concept that takes into account the separate processing of the Client's data and the data of other clients.
- Labeling of the recorded data (file number, ID, customer/process number)
- Separation of functions/production/testing

2. Integrity

2.1 Transfer control
- Logging of data transfers
- Secure transport protocols (SSL, TLS, SFTP)
- A ban on the use of private data carriers at the workplace is in force
- Paper and data carriers containing personal data are disposed of by a qualified disposal company in accordance with data protection regulations.

- Generally no use of mobile data carriers. However, if necessary, use of encrypted mobile data carriers.
- Incoming and outgoing data streams are filtered by a firewall solution which is up-to-date/in line with the technical standard.
- Agreement/guideline on the use of non-company hardware for company purposes.
- Agreement/guideline on the use of company hardware in the private environment

2.2 Input control

- Authorization concept
- Use of application-level firewalls and intrusion detection systems to prevent and recognize attacks
- The organizational definition of responsibilities for the input-authorized users is documented.
- Each employee only has the necessary access to the data required for their function/role (principle of minimum rights).
- Authorizations for resources meriting protection are only requested and granted by authorized persons in a traceable manner.

2.3 Order control

- The contract contains detailed information on the purpose limitation of the Client's personal data as well as a prohibition of use by the service provider outside the written order.
- The contract contains detailed information on the type and scope of the commissioned processing and utilization of the Client's personal data.
- The service provider has appointed a data protection officer and ensures their appropriate and effective integration into the relevant operational processes through the data protection organization.
- Contract data processing agreements have been concluded with all relevant subcontractors or have at least been requested.
- Clear contract design, offer, and order confirmation are present.
- The order has been placed in a formalized manner (order form).
- All employees with access authorization are verifiably bound to data secrecy.
- Every employee has received work instructions/guidelines or information sheets that provide information on measures for compliance with data protection and IT security.
- In the event of errors in data processing or breaches of data protection, the Client shall be informed immediately.

3. Availability and resilience

- Backup procedure/regular backup copies
- Full backup and recovery concept with daily backup
- Regular checks of the condition and labeling of data carriers for data backups
- Mirroring of hard disks, e.g. RAID procedure
- Use of protection programs (virus scanner/firewall)
- Monitoring of all relevant servers

4. Procedures for regular review, assessment, and evaluation

- All employees have been obligated and instructed in writing to maintain data confidentiality.
- All employees must complete data protection training (eLearning) once per calendar year.
- Proof of successful completion of the training by means of a corresponding certificate.

Appendix 2 - Subcontractors

Subcontractors	Description of the services	Location
makandra GmbH	Hosting straiv Software	EU
Hetzner Online GmbH	Website hosting	EU
LINK Mobility Austria GmbH	SMS Distribution	EU
Mailgun Technologies,Inc.	E-Mail distribution	EU
Bird B.V.	Whatsapp Messaging	EU
SmartBear Software Inc.	Error tracking	US
Datadog Inc.	Log evaluation	EU
PostHog Inc.	Product analysis	EU
Atlassian Pty Ltd,	Ticket system	EU
Google Cloud EMEA Limited	Google Workspace	EU
WhatsApp Ireland Limited	Whatsapp Distribution	EU
Hubspot Ireland Limited	Customer communication	EU

OpenAI Ireland Ltd	Provision of chatbot	US
LangChain Inc.	Provision of chatbot	EU

As at: 01.04.2025
Version: 1.6