Data Processing Agreement

1. Preamble

1.1 Straiv GmbH, Industriestraße 23, 70565 Stuttgart (hereinafter "**Processor**" or "**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 Processor. 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.

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 employees of 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 (optional 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)
    - Usage data (e.g. start, duration, and end of use, feature used, language used, browser and operating system used)
    - Geodata (only when using the functionality “GPS settings” to restrict the services of Straiv to a radius around the hotel)

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 Processor processes personal data of the Client only on its 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. 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 than those mentioned in this contract or resulting from the Main Agreement (see

Section 2.1). 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. product analysis.

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. Unless otherwise agreed herein, the Processor shall not disclose any information obtained from the Client's area to third parties**.**

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 Processor. The Processor warrants that it will assist with these checks where necessary.

4.7 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).

4.8 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, violations by the Processor or the persons employed by the Processor, as well as breaches of data protection provisions or the specifications set out in the order, and 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 carried out by the Processor following prior instruction in accordance with Section 4 of this contract.

6. Subcontracting Relationships (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 Processor 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 Processor 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 Processor 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 Processor 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 Processor shall

ensure that the service is permissible under data protection laws by taking appropriate measures.

7. Technical and Organizational Measures (Art. 32 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 Processor 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 an integral part of this data processing agreement.

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 Processor 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 will be presented to the Client after request.

9. Liability

9.1 Liability shall be governed by the statutory provisions in accordance with Art. 82 GDPR.

9.2 The parties shall indemnify each other from liability for damages if a party proves that it is

not responsible for the circumstance. This applies accordingly to a fine imposed on a party, whereby the indemnification takes place to the extent that the other party shares responsibility for the breach sanctioned by the fine.

10. Final Provisions

10.1 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 Processor.

10.2 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.

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

11. 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 legal and economic sense and purpose of the ineffective clause. The same applies to any gaps in this agreement.

Appendix 1 – Technical and Organizational Measures (TOM)

The Processor warrants that it complies with the minimum requirements described below as part of its data protection concept. This describes the measures required at the Processor within the scope of order processing for the secure handling of personal data. The basis for this data protection concept is the EU General Data Protection Regulation (GDPR) and, if applicable, further measures required by the interested parties. In this regard, the Processor is essentially guided by the requirements of Articles 24, 25, and 32 GDPR. Upon request, the Processor shall provide corresponding proof of compliance.

1. Confidentiality

1.1 Entry Control

- Entry control system / entry only for authorized employees by means of transponder keys
- Entry control at the main entrance door by means of a camera
- Documented allocation of keys
- Return of access means after expiry of authorization
- Reception

1.2 Access Control

- Password policy (minimum length, alphanumeric with upper and lower case as well as special characters required)
- Login to server systems is exclusively possible via SSH, whereby only administrators with valid access authorized via a whitelist with RSA-SHA keys and secure passwords are permitted
- Locking of the computer when (temporarily) leaving the workplace
- Access to relevant systems via OAuth and 2-factor authentication
- Firewall/virus scanner
- Organizational instructions for the issuing of keys
- Immediate blocking of authorizations when employees leave (policy/working instruction)
- Secure transmission of authentication secrets (credentials) via HTTPS

1.3 Usage Control

- Differentiated authorizations (e.g. in the form of profiles, roles)
- Binding authorization allocation procedure
- An administration concept exists for the traceable application and allocation of access rights
- Detection and prevention of repeated failed login attempts to fend off brute-force attacks
- Logging of changes to authorizations
- Binding procedure for the recovery of data from backup (restore by IT department on instruction of the management)
- Documentation of network drive access for authorized users (user groups)
- Authorization concept is documented
- Allocation of minimal authorizations (need-to-know principle)
- The allocation of generic group IDs or passwords is not provided for in the software and is not recommended.
- The software allows for the avoidance of the concentration of functions and enables the separation of functions of administration activities among different qualified persons.
- Data protection-compliant disposal of data carriers no longer required by server

service providers

1.4 Pseudonymization

- Evaluations are pseudonymized unless the personal reference is absolutely necessary for the result.

1.5 Anonymization

- All data anonymized within the meaning of Section 4.2 are processed in such a way that it is not possible to assign them to a real person. The anonymized data are stored in a separate, delimited database. This technical procedure ensures that a personal reference cannot be subsequently restored.

1.6 Separation Control

- The authorization mechanisms available in the systems used enable the exact implementation of the specifications of the authorization concept.
- An authorization concept exists which takes into account the separate processing of the Client's data from data of other clients.
- Labeling of the recorded data (file reference, ID, customer/process number)
- Separation of functions/production/test

2. Integrity

2.1 Transmission Control

- Logging of data transmissions
- Secure transport protocols (SSL, TLS, SFTP)
- The use of private data carriers at the workplace is prohibited.
- Paper and data carriers with personal data are disposed of in a data protection-compliant manner by a qualified disposal company.
- In principle, no use of mobile data carriers. If necessary, however, use of encrypted mobile data carriers.
- Incoming and outgoing data streams are filtered by a current firewall solution corresponding to the technical standard.
- Agreement/policy on the use of third-party hardware for company purposes.
- Agreement/policy on the use of company hardware in a private environment.

2.2 Input Control

- Authorization concept
- Use of application-level firewalls and intrusion detection systems to prevent and detect attacks
- The organizational definition of responsibilities for those authorized to input data is documented.
- Every employee has only the necessary access to the data required within the scope

of their function/role (principle of minimal rights).
- Requests for and allocation of authorizations for resources worthy of protection are made traceably only by persons authorized for this purpose.

2.3 Order Control

- The contract contains detailed information on the purpose 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 use of personal data of the Client.
- The service provider has appointed a data protection officer and ensures their appropriate and effective involvement in 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 available.
- The order was placed formally (order form).
- All employees with access rights are demonstrably committed to data secrecy.
- Every employee has received work instructions/policies or leaflets informing them about measures to comply with data protection and IT security.
- In the event of errors regarding data processing or a violation 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
- Backups are secured in a different fire compartment than the source systems and are encrypted separately
- 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
- Proactive detection of anomalous behavior and events on 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

Subcontractor	Description of services	Location
Amazon Web Services EMEA SARL	Hosting Straiv Software	EU
Hetzner Online GmbH	Website hosting	EU
LINK Mobility Austria GmbH	SMS Distribution	EU
Mailgun Technologies SAS	E-Mail Distribution	EU
Bird B.V.	Whatsapp Messaging	EU
Datadog Inc.	Log evaluation	EU
Atlassian B.V.	Ticket system	EU
Google Cloud EMEA Limited	Google Workspace / Provision of Chatbot	EU

WhatsApp Ireland Limited	Whatsapp Distribution	EU
Hubspot Ireland Limited	Customer communication	EU
OpenAI Ireland Ltd	Provision of chatbot	**EU**
LangChain Inc.	Provision of chatbot	EU
n8n GmbH	Process automation	EU

As at: 30.03.2026
Version: 1.7