Data Processing Agreement

Contract for the processing of personal data in compliance to Art. 28 GDPR

This Data Processing Agreement and its annexes ("DPA") reflects the agreement on the processing of personal data within the meaning of the General Data Protection Regulation ("GDPR") by the Contractor, DeskNow GmbH, Carl-Benz-Str. 29, 48734 Reken, Germany (also referred to as "we", "us", "Service", "Data Processor", "DeskNow") on behalf of the Client (also referred to as "Client").

The Contractor shall provide services to the Client in accordance with the user agreement concluded between them (hereinafter referred to as the "Agreement" or "Main Agreement") and in accordance with the General Terms and Conditions. In order to fulfill the requirements of the GDPR for such constellations, the parties conclude the following Data Processing Agreement, which comes into effect upon signing the Main Agreement.
The Client and Contractor are hereinafter also referred to as "Party" and jointly as "Parties".

We will update these terms at regular intervals. If you have an active DeskNow subscription, we will notify you by email (if you have opted in to receive email updates) notifications or inform you via in-app notification when we do so.

§ 1 Object/scope of the assignment

(1) As part of the cooperation between the parties in accordance with the main contract, the Contractor shall have access to the Client's personal data (hereinafter "Client Data"). The Contractor processes this Client Data on behalf of and in accordance with the instructions of the Client within the meaning of Art. 4 No. 8 and Art. 28 GDPR.

(2) The processing of client data by the contractor is carried out in the following manner and to the extent and for the purpose specified therein. The group of persons affected by the data processing is limited to the groups of persons involved in the software development at the Client and is presented accordingly. The duration of the processing corresponds to the term of the main contract.

a. Purpose of the processing

- User management for access control and contacting
- Support in the implementation of contracts or orders

b. Categories of affected persons

- Employees including former employees, trainees and interns.
- External service providers and consultants and freelancers

c. Categories of personal data

- Booking data (information about actions and interactions of individual bookings/reservations in the booking process, such as log data and log files, in particular time stamps and locations).
- Names and user IDs
- Organizational information on divisional affiliations
- E-mail address and cell phone number

(3) In principle, the processing of the client data takes place exclusively in the territory of the Federal Republic of Germany or in a member state of the European Union. Should there be a relocation of the order processing to a third country, this requires the prior consent of the client and only takes place if the special

requirements of Art. 44 to 49 GDPR are met. The client already consents to the processing of personal data by the subcontractors named below upon conclusion of this order processing contract.

(4) The provisions of this contract shall apply to all activities related to the main contract. The same shall apply to all activities in which the Contractor and its employees or persons commissioned by the Contractor come into contact with Client Data.

§ 2 Authority of the client to issue instructions

(1) The Contractor shall process the Client Data within the scope of the assignment and on behalf of and in accordance with the instructions of the Client within the meaning of Art. 28 GDPR (commissioned processing). The Client has the sole right to issue instructions regarding the type, scope and method of processing activities (hereinafter also referred to as "right to issue instructions"). If the Contractor is obliged by the law of the European Union or the Member States to which it is subject to carry out further processing, it shall inform the Client of these legal requirements prior to processing.

(2) Instructions shall generally be issued by the client in writing or in electronic form (e-mail is sufficient); verbal instructions must be confirmed by the contractor in electronic form.

(3) If the Contractor is of the opinion that an instruction from the Client violates data protection regulations, it must inform the Client of this. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Client.

§ 3 Protective measures of the contractor

(1) The Contractor is obliged to observe the statutory provisions on data protection and not to disclose the information obtained from the Client's area to third parties or expose it to their access. Documents and data must be secured against unauthorized access, taking into account the state of the art.

(2) Furthermore, the Contractor shall oblige all persons entrusted by it with the processing and fulfillment of this contract (hereinafter referred to as "employees") to maintain confidentiality (obligation of confidentiality, Art. 28 para. 3 lit. b GDPR). At the Client's request, the Contractor shall provide the Client with written or electronic proof of the employees' obligation.

(3) The Contractor shall design its internal organization in such a way that it meets the special requirements of data protection. The Contractor undertakes to take all appropriate technical and organizational measures to adequately protect the Client Data in accordance with Art. 32 GDPR, in particular the measures listed in Annex 1 to this Agreement, and to maintain these for the duration of the processing of the Client Data.

(4) The contractor reserves the right to change the technical and organizational measures taken, whereby he shall ensure that the contractually agreed level of protection is not undercut.

(5) At the request of the Client, the Contractor shall provide the Client with evidence of compliance with the technical and organizational measures.

§ 4 Information and support obligations of the contractor

(1) In the event of disruptions, suspected data protection violations or breaches of contractual obligations of the Contractor, suspected security incidents or other irregularities in the processing of the Client Data by the Contractor, persons employed by the Contractor within the scope of the order or by third parties, the Contractor shall inform the Client immediately, but at the latest within 48 hours, in writing or in electronic form. The same applies to audits of the contractor by the data protection supervisory authority. These notifications should contain at least the information specified in Art. 33 (3) GDPR.

(2) In the above-mentioned case, the Contractor shall assist the Client in fulfilling its duty to provide information in this regard, remedial and information measures within the scope of what is reasonable.

(3) The Contractor undertakes to provide the Client with all information and evidence required to carry out an inspection within a reasonable period of time at the Client's request.

§ 5 Other obligations of the Contractor

(1) If the requirements of Art. 30 GDPR apply, the contractor is obliged to keep a list of all categories of processing activities carried out on behalf of the client in accordance with Art. 30 (2) GDPR. The list must be made available to the client upon request.

(2) The contractor is obliged to support the client in the preparation of a data protection impact assessment in accordance with Art. 35 GDPR and any prior consultation with the supervisory authority in accordance with Art. 36 GDPR. (3) The Contractor confirms that it has appointed a data protection officer - insofar as there is a legal obligation to do so. The client must be informed of any change in the person of the company data protection officer/contact person for data protection.

(3) In accordance with this agreement, the Contractor confirms that it stores the personal data separately from the actual SaaS solution, i.e. the software. The personal data is stored exclusively on the MongoDB database in Frankfurt am Main, which is hosted on Azure servers. The SaaS solution, on the other hand, is also hosted on AWS servers in Frankfurt am Main.

(4) Should the Client Data be jeopardized at the Contractor by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Client of this immediately, unless it is prohibited from doing so by court or official order. In this context, the Contractor shall immediately inform all competent bodies that the decision-making authority over the data lies exclusively with the Client as the "controller" within the meaning of the GDPR.

§ 6 Subcontractor relationships

(1) Within the scope of its contractual obligations, the Contractor is authorized to establish subcontracting relationships with subcontractors ("subcontractor relationship"). The Contractor shall ensure that the provisions agreed in this contract also apply to the subcontractors commissioned by it, whereby the Client shall be granted all control rights vis-à-vis the subcontractor in accordance with this contract.

(2) A subcontractor relationship within the meaning of these provisions shall not exist if the Contractor commissions third parties to provide services that are to be regarded as purely ancillary services.

This includes, for example, postal, transportation and shipping services, cleaning services, security services, telecommunications services with no specific reference to services that the Contractor provides for the Client and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The Contractor's obligation to ensure compliance with data protection and data security in these cases remains unaffected.

(3) The Contractor has established subcontractor relationships with the following companies, which the Client consents to by concluding this data processing agreement:

- Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg
- MongoDB Ltd, Building Two, Number One Ballsbridge, Ballsbridge, Dublin 4, Ireland

(4) If the Contractor establishes a further subcontracting relationship involving the Client's data, it shall inform the Client of this in writing at least 14 days in advance. The Client shall have the right to reject the subprocessor in the event of justified doubts as to compliance with data protection regulations. Reasonable doubts must be explained to the Contractor. Should it be impossible for the Contractor to continue to provide the service as agreed in such a case, there shall be a special right of termination.

§ 7 Control rights

(1) The Client is entitled to regularly verify compliance with the provisions of this contract. For this purpose, it may, for example, obtain information from the Contractor, have existing certificates from experts, certifications or internal audits presented to it or have the Contractor's technical and organizational measures checked personally or by a competent third party during normal business hours, provided that the latter is not in a competitive relationship with the Contractor.

(2) The Client shall only carry out inspections to the extent necessary and shall take reasonable account of the Contractor's operating procedures. The parties shall agree on the time and type of inspection in good time.

(3) The Client shall document the results of the inspection and inform the Contractor thereof. In the event of errors or irregularities that the client discovers, in particular during the inspection of order results, the client must inform the contractor immediately. If facts are discovered during the inspection that require changes to the ordered process flow to be avoided in the future, the client shall inform the contractor of the necessary procedural changes without delay.

§ 8 Rights of data subjects

(1) The Contractor shall support the Client as far as possible with suitable technical and organizational measures in fulfilling its obligations under Art. 12 to 22 and Art. 32 to 36 GDPR. The Contractor shall provide the Client with the requested information about Client data without delay, but at the latest within 14 working days, if the Client does not have the relevant information itself.

(2) If the data subject asserts their rights in accordance with Art. 16 to 18 GDPR, the contractor is obliged to correct, delete or restrict the client data immediately, at the latest within a period of 7 working days, at the instruction of the client. The Contractor shall provide the Client with written proof of the deletion, correction or restriction of the data upon request.

(3) If a data subject asserts rights, such as the right to information, correction or deletion of their data, directly against the contractor, the contractor shall forward this request to the client and await the client's instructions. The contractor will not contact the data subject without corresponding individual instructions.

§ 9 Term and termination

(1) The term of this contract corresponds to the term of the main contract. If the main contract can be terminated with notice, the provisions on ordinary termination shall apply accordingly.

§ 10 Deletion and return after the end of the contract

(1) The Contractor shall return to the Client all documents, data and data carriers provided to it after termination of the main contract or at any time at the Client's request, or delete them completely and irrevocably at the Client's request, unless there is a statutory retention period. This shall also apply to copies of the Client Data made by the Contractor, such as data backups, but not to documentation that serves as proof of the proper processing of the Client Data in accordance with the order. Such documentation shall be retained by the Contractor for a period of 6 months and returned to the Client upon request.

(2) The Contractor shall confirm the deletion to the Client electronically. The Client has the right to check the complete and contractually compliant return or deletion of the data at the Contractor in a suitable manner.

(3) The Contractor shall be obliged to treat any data it becomes aware of in connection with the main contract confidentially, even after the end of the main contract.

§ 11 Liability

(1) The liability of the parties shall be governed by Art. 82 GDPR. Any liability of the Contractor towards the Client for breach of obligations under this contract or the main contract shall remain unaffected by this.

(2) The parties shall indemnify each other against liability if a party proves that it is not responsible in any respect for the circumstance that caused the damage to a party concerned. This shall apply accordingly in the event of a fine imposed on a party, whereby the indemnification shall be made to the extent that the other party bears a share of the responsibility for the infringement sanctioned by the fine.

§ 12 Final provisions

(1) The parties agree that the Contractor's defense of the right of retention within the meaning of Section 273 BGB (German Civil Code) is excluded with regard to the data to be processed and the associated data carriers.

(2) Amendments and supplements to this agreement must be made in electronic form.

(3) In case of doubt, the provisions of this agreement shall take precedence over the provisions of the main agreement. Should individual provisions of this agreement prove to be invalid or unenforceable in

whole or in part or become invalid or unenforceable as a result of changes in legislation after the conclusion of the contract, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision that comes as close as possible to the meaning and purpose of the invalid provision.

(4) This agreement is subject to German law. The exclusive place of jurisdiction shall be the Contractor's registered office.

(5) Only the German version of this document is legally binding.

.....	.....
Signature (contractor)	Place & date
.....	.....
Signature (client)	Place & date

TOM system

Technical and organizational measures in accordance with Art. 32 GDPR

In addition to the data processing agreement, the parties shall make the following stipulations regarding the technical and organizational measures to be implemented by DeskNow:

Confidentiality (Art. 32 para. 1 lit. b GDPR) Access control

The following measures prevent unauthorized persons from gaining access to data processing systems:

- Access control system, badge reader (magnetic/chip card)
- Door locks (electric door openers, combination locks, etc.)
- Key management/documentation of key allocation
- Alarm system
- Special protective measures for the server infrastructure (certification in accordance with ISO/IEC 27001:2013, 27017:2015, 27018:2019 and ISO/IEC 9001:2015)
  - Special protective measures for the storage of backups and other data carriers
  - Non-reversible deletion or destruction of data carriers

Access control

The following measures prevent unauthorized third parties from gaining access to data processing systems:

- Personal and individual login when logging into the system/network
- Authorization process for access authorizations
- Password procedure/password policy (specification of password parameters in terms of complexity and update interval)
- Logging of access
- Automatic blocking of clients after a period of time without user activity
- Additional authorization roles for certain applications (in particular administrator rights and server administration)

  Hardware firewall

  Use of a state-of-the-art software firewall
- Use of state-of-the-art anti-virus software
- Mobile device policy

Access control

The following measures ensure that unauthorized third parties have no access to data:

- Conclusion of order processing contracts for the external care, maintenance and repair of data processing systems, insofar as the processing of data is the subject of the contractor's service in the case of remote maintenance.

- Evaluations/logging of data processing
- Encryption of data carriers
- Four-eyes principle
- Differentiated authorization concept / segregation of duties
- Number of persons with administrator status minimized
- Privacy films for mobile data processing systems
- Blocking of accounts of employees who have left the company

Separation control

The following ensure that data collected for different purposes is processed separately:

- Multi-client capability of IT systems
- Use of test data
- Separation of development and production environment

Integrity (Art. 32 para. 1 lit. b GDPR)

Transfer control

It is ensured that data cannot be read, copied, changed, removed or otherwise processed without authorization during transmission or storage on data carriers and that it is possible to check which persons or bodies have gained access to data. The following measures have been implemented to ensure this:

- Encryption of e-mail or e-mail attachments

  Encryption of data carriers

  Secure file transfer or other data transport
- Encrypted WLAN
- Logging of data transmission or data transport
- Logging of read accesses
- Logging the copying, modification or removal of data
- Encryption against AWS through DynamoDB Encription Client

Input control

The following measures ensure that it is possible to check who processed data in data processing systems and at what time:

- Access rights
- System logging

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

The following measures ensure that data is protected against accidental destruction or loss and is always available to the customer:

- Security concept for software and IT applications
- Backup procedure
- Redundant data storage
- Guarantee of data storage in the secure network
- Installing security updates as required
- Uninterruptible power supply (UPS)
- Fire and/or extinguishing water protection for the server room
- Air-conditioned server room
- Firewall & virus protection
- System resilience is ensured by oversizing

Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Data protection management

The following measures are intended to ensure that the organization meets the basic requirements of data protection law:

- Obligation of employees to maintain confidentiality
- Sufficient training of employees in data protection
- Keeping a record of processing activities (Art. 30 GDPR)
- DeskNow's data protection policy
- Privacy policy of DeskNow

Management of data breaches

The following measures are intended to ensure that reporting processes are triggered in the event of data protection breaches:

- Reporting process for data breaches to the supervisory authorities in accordance with Art. 4 (12) GDPR (Art. 33 GDPR)
- Notification process for data breaches in accordance with Art. 4 (12) GDPR vis-à-vis data subjects (Art. 34 GDPR)

Data protection-friendly default settings (Art. 25 para. 2 GDPR)

Data protection-friendly default settings must be taken into account both in the standardized default settings of systems and apps and when setting up the processing. In this phase, functions and rights are specifically configured, the permissibility or impermissibility of certain inputs or input options is determined with regard to data minimization and a decision is made on the availability of usage functions. The type and scope of the personal reference or anonymization (e.g. for selection, export and evaluation functions that are defined and

made available by default or freely configurable) or the availability of certain processing, functions or logging are also determined.

Order control

The following measures ensure that data is only processed in accordance with the customer's instructions:

- Data processing agreement with provisions on the rights and obligations of the parties

  Process for issuing and following instructions
- Designation of contact persons and/or responsible employees
- Training/instructions for all employees authorized to access DeskNow
- Obligation of employees to maintain confidentiality
- Agreement of contractual penalties for breaches of instructions

.....	.....
Signature (contractor)	Place & date
.....	.....
Signature (client)	Place & date