Contract for the processing of data on behalf

1. General

(1) The Contractor (desk.ly Gmbh) processes personal data on behalf of the Client (you, your company) within the meaning of Art. 4 No. 8 and Art. 28 of Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). This contract regulates the rights and obligations of the parties in connection with the processing of personal data.

(2) If the term "data processing" or "processing" (of data) is used in this contract, the definition of "processing" within the meaning of Art. 4 No. 2 GDPR shall apply.

2. Subject of this contract

The subject matter of the processing, type and purpose of the processing, the type of personal data and the categories of data subjects are set out in Annex 1 to this contract.

3. Rights and obligations of the Client

(1)The Client is the person responsible within the meaning of Art. 4 No. 7 GDPR for the processing of data on behalf of the Contractor. Pursuant to No. 4 paragraph 5, the Contractor shall have the right to notify the Client if data processing, which is considered to be legally inadmissible, is the subject of the order and/or an instruction.

(2) The Client, as the person responsible, is in charge of safeguarding the data subject rights. The Contractor shall inform the Client immediately if data subjects assert their data subject rights in connection with processing of data on behalf of the Contractor.

(3) The Client has the right to issue supplementary instructions to the Contractor at any time regarding the type, scope and procedure of data processing. Instructions must be provided in written form (e.g. e-mail).

(4) Regulations on any remuneration of additional expenses incurred by the Contractor due to supplementary instructions of the Client shall remain unaffected.

(5) The Client may appoint persons authorised to issue instructions. If the persons authorised to issue instructions are to be named, they shall be named in **Annex 1**. In case these persons authorised to issue instructions change, the Client shall inform the Contractor of this in written form.

(6) The Client shall inform the Contractor immediately if he discovers errors or irregularities in connection with the processing of personal data by the Contractor.

(7) In case there is an obligation to inform third parties pursuant to Art. 33, 34 GDPR or any other statutory notification obligation applicable to the Client, the Client shall be responsible for their compliance.

(8) Where the processor processes guest booking data on behalf of the customer, responsibility for compliance with any statutory archiving obligations lies exclusively with the customer. The processor provides export functions (CSV export, REST API) for this purpose

but does not assume an archiving function. The customer is obligated to independently and promptly secure any required data.

4. General obligations of the Contractor

(1) The Contractor shall process personal data exclusively within the scope of the agreements made and/or in compliance with any supplementary instructions issued by the Clients. Exceptions to this are legal regulations which may require the Contractor to process data in a different manner. In such a case, the Contractor shall notify the Client of these legal requirements prior to processing, unless the relevant law prohibits such notification due to an important public interest. The purpose, nature and scope of the data processing shall otherwise be governed exclusively by this contract and/or the Client's instructions. The Contractor is prohibited from processing data in a manner deviating from this unless the Client has consented to this in written form.

(2) The Contractor is obliged to carry out data processing on behalf of the Client only in member states of the European Union (EU) or the European Economic Area (EEA). Processing of personal data in a third country requires the prior consent of the Client, which must be given at least in written form (e.g. e-mail). The Clients consent shall only be considered if it is ensured that the respective legal provisions to be complied with pursuant to Art. 44 - 49 of the GDPR are observed in order to ensure an adequate level of protection for the personal data.

(3) In the area of the processing of personal data in accordance with the order, the Contractor shall ensure that all agreed measures are carried out in accordance with the contract.

(4) The Contractor shall be obliged to organise his company and his operating procedures in such a way that the data which he processes on behalf of the Client are secured to the extent necessary in each case and protected against unauthorised access by third parties. The Contractor shall coordinate changes in the organisation of data processing on behalf of the Client that are significant for the security of the data with the Client in advance.

(5) The Contractor shall inform the Client immediately, if, in their opinion, an instruction issued by the Client violates statutory regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Client. If the Contractor can demonstrate that processing in accordance with the Client's instructions may lead to liability on the part of the Contractor pursuant to Art. 82 GDPR, the Contractor shall be entitled to suspend further processing in this respect until the liability between the parties has been clarified.

(6) The processing of data on behalf of the Client outside the Contractor's premises or subContractors is only permitted with the consent of the Client in writing or text form. Processing of data on behalf of the Client in private residences is only permitted with the consent of the Client in writing or text form on a case-by-case basis.

(7) The Contractor shall process the data, which are processed on behalf of the Client, separately from other data. Physical separation is not mandatory.

(8) The Contractor may identify the person(s) authorised to the Client to receive instructions from the Client. If the persons authorised to receive instructions are to be named, they shall be named in **Annex 1**. If the persons authorised to receive instructions change at the Contractor, the Contractor shall inform the Client of this in written form.

5. Contractor's Data Protection Officer

(1) The Contractor confirms that he has appointed a Data Protection Officer in accordance with Art. 37 GDPR. The Contractor shall ensure that the Data Protection Officer has the necessary qualifications and expertise. The Contractor shall inform the Client of the name and contact details of its data protection officer separately in text form.

(2) The obligation to appoint a data protection officer in accordance with paragraph 1 may be waived at the Client's discretion if the Contractor can demonstrate that it is not legally obliged to appoint a data protection officer and the Contractor can prove that operational rules exist to ensure the processing of personal data in compliance with the legal provisions, the rules of this contract and any further instructions of the Client.

6. Reporting obligations of the contractor

(1) The Contractor shall be obliged to notify the Client immediately of any breach of data protection regulations or of the contractual agreements made and/or the instructions issued by the Client which has occurred in the course of the processing of data by the Contractor or other persons involved in the processing. The same shall apply to any breach of the protection of personal data processed by the Contractor on behalf of the Client.

(2) The Contractor shall also inform the Client immediately if a supervisory authority takes any action to the Contractor pursuant to Art. 58 GDPR, which may also concern control of the processing carried out by the Contractor on behalf of the Client.

(3) The Contractor is aware that the Client may be obliged to a notification obligation pursuant to Art. 33, 34 GDPR, which provides a notification to the supervisory authority within 72 hours of the notification. The Contractor shall support the Client in the implementation of the reporting obligations. In particular, the Contractor shall notify the Client of any unauthorised access to personal data processed on behalf of the Client without undue delay, but at the latest within 48 hours of becoming aware of the access. The notification by the Contractor to the Client shall in particular include the following information:

- a description of the nature of the personal data breach, including, to the extent possible, the categories and approximate number of data subjects concerned, the categories concerned and the approximate number of personal data records concerned;
- a description of the measures taken or proposed by the Contractor to remedy the personal data breach and, where applicable, measures to mitigate its possible adverse effects.

7. Cooperation obligations of the Contractor

(1) The Contractor shall support the Client in its duty to respond to requests for the exercise of data subject rights pursuant to Art. 12-23 GDPR. The provisions of Section 12 of this contract shall apply.

(2) The Contractor shall participate in the preparation of the directories of processing activities by the Client. It shall provide the contracting authority with the information required in this respect in an appropriate manner.

(3) The Contractor shall support the Client in complying with the obligations set out in Art. 32-36 GDPR, taking into account the nature of the processing and the information available to it.

8. „Home Office“- regulations

(1) The Client hereby consents, that the Contractor can allow its employees who are commissioned to process personal data for the Client to process personal data in private residences ("home office").

(2) The Contractor shall ensure that compliance with the covenant technical and organisational measures are also guaranteed in the "home office" of the Contractor's employees. Deviations from individual covenant technical and organisational measures shall be agreed with the Client in advance and approved by the Client in written form.

(3) The Contractor shall in particular ensure that if personal data are processed in the "home office", the storage locations are configured in such a way that local storage of data on IT systems used in the "home office" is excluded. If this is not possible, the Contractor shall ensure that local storage is exclusively encrypted and that other persons in the household do not have access to this data.

(4) The Contractor shall be obliged to ensure that an effective control of the processing of personal data on behalf of the Client in the "home office" is possible. In doing so, the personal rights of the employees as well as the other persons living in the respective household shall be adequately taken into account.

(5) If employees of subcontractors are also to be deployed in the "home office", the provisions of paragraphs 1 to 4 shall apply accordingly.

9. Controlling authorities

(1) The Client shall have the right to monitor the Contractor's compliance with the statutory provisions on data protection and/or compliance with the contractual provisions agreed between the parties and/or compliance with the Client's instructions at any time to the extent required.

(2) The Contractor shall be obliged to provide information to the Client, insofar as this is necessary for the performance of the inspection in terms of paragraph 1.

(3) The Client may request to inspect the data processed by the Contractor for the customer as well as the data processing systems and programmes used.

(4) The Client may, after prior notification with a reasonable period of notice, carry out the checks referred to in paragraph 1 with the Contractor’s premises during normal business hours. In doing so, the Client shall ensure that the checks are carried out only to the extent necessary to ensure that the checks do not unduly disturb the Contractor's business operations.

(5) The Contractor is obliged, in the case of measures taken by the supervisory authority against the Client, to Article 58 GDPR, in particular with regard to information and inspection obligations, to provide the Client with the necessary information and to enable the relevant supervisory authority to carry out on-site inspections. The Client shall be informed by the Contractor of any measures planned.

(6) The Parties agree that the control measures for the processing of personal data in the "home office" to protect the personal rights of the Contractor's employees and any other persons in the respective household shall primarily be carried out by controlling the assurance of the measures to be taken by the Contractor in accordance with Clause 8 paragraph 2 and 3. If necessary, the Client shall also be enabled by the Contractor to carry out checks in the "home office" of employees.

10. Subcontracting relationships

(1) The commissioning of subcontractors by the Contractor is only permissible with the consent of the Client in text form. The Client grants such consent for the subcontractors listed in **Annex 2** upon conclusion of this contract as a general written authorisation within the meaning of Art. 28 (2) GDPR; Section 10.2 shall apply to the engagement of additional subcontractors or the replacement of existing ones.

(2) The Contractor shall carefully select the subcontractor and check before commissioning that the subcontractor can comply with the agreements made between the Client and the Contractor. In particular, the Contractor shall check in advance and regularly during the term of the contract that the subcontractor has taken the technical and organisational measures required under Article 32 GDPR to protect personal data. The result of the inspection shall be documented by the Contractor and transmitted to the Client upon request.

(3) The Contractor is obliged to obtain confirmation from the subcontractor that the subcontractor has appointed an operational data protection officer in accordance with Art. 37 GDPR. In the event that no data protection officer has been designated by the subcontractor, the Contractor shall point this out to the Client and provide information to the effect that the subcontractor is not legally obliged to appoint a data protection officer.

(4) The Contractor shall ensure that the regulations agreed in this contract and, if applicable, supplementary instructions of the Client also apply to the subcontractor.

(5) The Contractor shall conclude a contract processing agreement with the subcontractor that complies with the requirements of Art. 28 GDPR. In addition, the Contractor shall impose the same personal data protection obligations on the subcontractor as are laid down between the client and the Contractor. A copy of the commissioned data processing contract shall be provided to the Client upon request.

(6) The Contractor shall in particular be obliged to ensure by contractual arrangements that the control powers (Clause 9 of this contract) of the Client and of supervisory authorities also apply to the subcontractor and that corresponding control rights of the Client and supervisory authorities are agreed. It must also be contractually agreed that the subcontractor must tolerate these control measures and any on-site inspections.

(7) Services which the Contractor uses from third parties as a purely ancillary service in order to carry out the business activity are not to be regarded as subcontracting relationships within the meaning of paragraphs 1 to 6. This includes, for example, cleaning services, pure telecommunication services not specifically related to services provided by the Contractor to the contracting entity, postal and courier services, transport services and surveillance services. The Contractor is nevertheless obliged, also in the case of ancillary services provided by third parties, to ensure that appropriate precautions and technical and organisational measures have been taken to guarantee the protection of personal data. The maintenance and servicing of IT systems or applications constitutes a subcontracting relationship requiring consent and commissioned processing within the meaning of Art. 28 GDPR if the maintenance and testing concerns such IT systems that are also used in

connection with the provision of services for the Client and personal data processed on behalf of the Client can be accessed during the maintenance.

11. Confidentiality obligation

(1) The Contractor shall, when processing data for the contracting entity, be obliged to maintain the confidentiality of data received or acquired to the attention of the contracting entity in connection with the contract. The Contractor undertakes to observe the same secrecy safeguard regulations as those which are the responsibility of the Client. The Client is obliged to inform the Contractor of any special rules for the secrecy safeguard.

(2) The Contractor warrants that he is aware of the applicable data protection regulations and is familiar with their application. The Contractor also undertakes to familiarise its employees with the relevant provisions of data protection and to oblige them to maintain confidentiality. The Contractor shall also ensure that he has, in particular, required the employees involved in the work to be confidential and has informed them of the instructions given by the contracting entity.

(3) The obligation of the employees in accordance with paragraph 2 shall be proven to the Client upon request.

12. Safeguarding the rights of data subjects

(1) The Client shall be solely responsible for safeguarding the rights of data subjects. The Contractor is obliged to support the Client in his duty to process requests from data subjects in accordance with Art. 12-23 GDPR. In particular, the Contractor must ensure that the information required in this respect is provided to the Client without delay so the Client can fulfil its obligations under Article 12 paragraph 3 GDPR.

(2) Insofar as the cooperation of the Contractor is necessary for the protection of data subjects' rights - in particular in regard to information, correction, blocking or deletion - by the Client, the Contractor shall take the respective necessary measures according to the Client's instructions. The Contractor shall support the Client as far as possible with suitable technical and organisational measures in fulfilling its obligation to respond to requests for the exercise of data subject rights.

(3) Arrangements for any compensation for additional expenses incurred by the Contractor due to cooperation services in connection with the assertion of data subject rights vis-à-vis the Client shall remain unaffected.

(4) In the event that a data subject asserts his rights under Art. 12-23 GDPR against the Contractor, although this obviously concerns a processing of personal data for which the Client is responsible, the Contractor shall be entitled to inform the data subject that the Client is the data controller. In this context, the Contractor may inform the data subject of the contact details of the controller.

13. Confidentiality obligations

(1) Both parties undertake to treat all information received in connection with the performance of this contract as confidential for an unlimited period of time and to use it only for the performance of the contract. Neither party is entitled to use this information in whole

or in part for purposes other than those just mentioned or to make this information available to third parties.

(2) The above obligation shall not apply to information which one of the parties has demonstrably received from third parties without being required to maintain confidentiality or which is publicly known.

14. Remuneration

Any regulations on remuneration for services shall be agreed separately between the parties.

15. Technical and organisational measures for data security

(1) The Contractor undertakes vis-à-vis the Client to comply with the technical and organisational measures required to comply with the applicable data protection rules. This includes in particular the requirements of Art. 32 GDPR.

(2) The status of the technical and organisational measures existing at the time of the conclusion of the contract is attached as **Annex 3** to this contract. The parties agree that changes to the technical and organisational measures may become necessary in order to adapt to technical and legal circumstances. The Contractor shall consult with the Client in advance on any significant changes that may affect the integrity, confidentiality or availability of the personal data. Measures that only entail minor technical or organisational changes and do not negatively affect the integrity, confidentiality and availability of the personal data may be implemented by the Contractor without consultation with the Client. The Client may request an up-to-date version of the technical and organisational measures taken by the Contractor at any time.

(3) The Contractor shall check the effectiveness of the technical and organisational measures taken by him regularly and also on an ad hoc basis. If there is need for optimisation and/or modification, the Contractor will inform the Client thereof.

16. Contract duration

(1) This contract shall apply for the duration of the actual fulfilment of services by the processor.

(2) It may be terminated with a three months' notice to the end of a quarter.

(3) The Client may terminate the contract at any time without notice if there is a serious breach by the Contractor of the applicable data protection provisions or of obligations under this contract, if the Contractor is unable or unwilling to carry out an instruction of the Client or if the Contractor refuses access by the Client or the competent supervisory authority in breach of the contract.

17. Termination

(1) After termination of the contract, the contractor shall return to the Client or delete, at the Client's option, all documents, data and processing or utilisation results produced in his

possession which are connected with the contractual relationship. The deletion shall be appropriately documented. Any statutory retention obligations or other obligations to store the data shall remain unaffected. In the case of deletion requested by the Client, data carriers shall be destroyed in compliance with at least security level 3 of DIN 66399; the Client shall be provided with proof of destruction with reference to the security level in accordance with DIN 66399.

(2) The Client has the right to check the complete and contractual return and deletion of the data at the Contractor. This can also be done by an on-site inspection of the data processing systems at the Contractor's premises. The Client shall give reasonable notice of the on-site inspection.

(3) The Contractor may store personal data processed in connection with the order beyond the termination of the contract if and to the extent that the contractor is subject to a statutory obligation to retain the data. In these 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.

18. Right of retention

The parties agree that the objection of the right of retention by the contractor in accordance with § 273 BGB (German Civil Code) is excluded with regard to the processed data and the associated data carriers.

19. Final Provisions

(1) Should the property of the Client with the Contractor be endangered by measures of third parties (for example by seizure or confiscation), by insolvency proceedings or by other events, the Contractor shall inform the Client without delay. The Contractor shall inform the creditors without delay of the fact that data processed under the order is involved.

(2) The written form is required for ancillary agreements.

(3) Should individual parts of this contract be invalid, this shall not affect the validity of the remaining provisions of the contract.

Annex 1 - Object of the contract

1. Object and purpose of the processing

The Client's order to the Contractor includes the following work and/or services:

Provision and support of the web-based booking software desk.ly

Purpose of order data processing:

Collection & storage of data required for the use of the services offered (e.g. booking of office seats via the online booking tool desk.ly).

2. Type(s) of personal data

The following types of data are regularly processed:

Type of data:

First and last name
E-mail address
Function / department
Anonymised IP address
Web browser used
Date/time of access
Absences of users
Profile pictures of users
External guests: first name, last name, email address, company name (optional)

3. Categories of data subject

Group of persons affected by the data processing:

Employees of the Client, as well as third parties who are granted access to the booking portal by the Client.

External guests / visitors (invited by employees of the customer to use booking functions).

4. Persons (Contractor) authorised to receive instructions

Mister Amir El Sayed (CISO)

Annex 2 - Subcontractors

For the processing of data on behalf of the Client, the Contractor shall use the services of third parties who process data on its behalf ("subcontractors").

The company or companies concerned are listed on the following URL:

https://www.desk.ly/en/list-of-subprocessors

Annex 3
Technical and organisational measures of the Contractor

The Contractor shall take the following technical and organisational measures for data security in accordance with Art. 32 GDPR.

Since the Contractor operates the desk.ly service exclusively on the infrastructure of the subcontracted processor Amazon Web Services EMEA SARL (AWS), which is specialised in external server hosting, in Frankfurt am Main (encrypted data backups are additionally stored in the AWS Ireland region within the EU) and no personal data of participants are stored or processed on the Contractor's own premises, the following TOM are limited to the security measures taken by the Contractor on its premises.

Information regarding TOM for external server hosting is available here:
https://aws.amazon.com/de/compliance/data-center/controls/

All TOMs are based on the requirements of ISO27001:2022 and GDPR.

Physical Access Control

Measures to prevent unauthorized persons from accessing data processing facilities for the processing and use of personal data:

- The building is controlled by an external security service outside business hours with irregular checkups.
- The network room is always locked and may only be entered by authorized persons.
- The key allocation is documented by employees authorized for this purpose.
- A security lock is fitted on each door of the offices and locked outside opening hours.
- Service providers are monitored.
- Employees have access to the office complex with a personalized transponder. In the event of theft or loss, no reference to the premises of desk.ly GmbH can be established.

System Access Control

Measures to prevent data processing systems from being used by unauthorized persons:

- Employees are identified and authenticated by user ID and password.
- Passwords are managed via a password manager and only made accessible to the respective user. Passwords are randomly generated by the system in compliance with current security recommendations.
- Server systems can only be administered with console password or via password-protected, encrypted connection.
- Web servers are hardened and maintained with regular patch management.
- Only personalized user accounts are used. Group accounts are only set up in a few exceptional cases.

- Automated standard routines exist for regular updates of protection software, such as virus scanners.
- Standard organizational routines are in place to regularly update the software components used to close publicly known vulnerabilities.

Data Access Control

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use, and after storage:

- Unauthorized collection, processing, and use of personal data is prevented.
- Differentiated access authorizations to files and application programs are implemented.
- Differentiated processing options, such as read-modify-delete, have been assigned.
- It is ensured that each user can only access the data to which he or she is authorized. The data of individual users are logically separated from each other. The separation control takes place within the application layer and is ensured in the software development process.
- Access rights are only granted, changed, and withdrawn by the internal administration. The technical and organizational processes for granting or withdrawing access rights are separate from each other.
- Access to the IT system via external connections (public networks) is specially protected.
- System administration is promptly informed about employees leaving so that access rights can be deleted.
- The transfer of data between the data processing system and the user is encrypted.

Separation

Measures to ensure that data processed for different purposes is processed separately:

- Data is split into different endpoints that have been created and act in a purpose-oriented manner.
- Customer-related data is stored directly at the company.
- User information about the company is requested upon login to prevent data mixing from different customers.
- Internal company data is requested within the companies after careful checking for authorization.
- Separate instances running on different servers ensure the separation of test and production systems.
- Instances are completely independent and run on different databases with different data sets.

Pseudonymisation & Encryption

Measures for pseudonymisation or encryption of data:

- Passwords are encrypted using a specific password hashing procedure.

- Bookings are automatically and irreversibly anonymized after 90 days by default, such that no personal reference can be established, while the booking itself is retained for usage display purposes. The administrator of the customer may configure this period individually in the system. Such configuration constitutes an instruction by the customer pursuant to Clause 3 § 3 of this agreement and is the customer's own data protection responsibility.
- Company/person-related anonymization can be enabled, anonymizing data output to the user while keeping the database intact.
- Bookings are pseudonymized in the database, with a booking referring to a specific user via user ID.
- Pseudonymized logging based on user ID is implemented for actions such as deleting bookings and sending bulk emails.
- Guest booking data is anonymized automatically and irreversibly on a rolling basis after a period configurable by the customer's administrator. The period is set upon activation of the guest booking feature and constitutes an instruction by the customer pursuant to Clause 3 § 3 of this agreement. The applicable period is communicated to the invited guest in text form at the time of invitation.
- Activation of the guest booking feature by the customer's administrator constitutes an instruction pursuant to Clause 3 § 3 of this agreement. Responsibility for compliance with any statutory archiving obligations lies exclusively with the customer. desk.ly provides export functions (CSV export, REST API) for this purpose but does not assume an archiving function.

Integrity Input Control

Measures to ensure that it is possible to check and determine retrospectively whether and by whom personal data have been entered into data processing systems, changed, or removed:

- Traceability of input, modification, and deletion of data is ensured through individual usernames and login to the management system.
- The contractual restriction of work with the Client's personal data is limited to the service provider's employees working in connection with services under the contract.

Disclosure Control

Measures to ensure that personal data cannot be read, copied, altered, or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment:

- Confidential data may only be transmitted to clients in encrypted form by email.
- The data of the portal is secured within the environment of the data center operator. No transmission outside the EU takes place.
- Personal data may only be sent by email in encrypted form (by arrangement) or by SMS (e.g., passwords).

Availability and Resilience

Measures to ensure that personal data is protected against accidental destruction or loss:

- Availability control, including data backup, security updates, virus protection, firewall, and UPS, is guaranteed.
- Storage of data backup media is ensured in the bank safe.
- Virus scanners are used centrally on servers and decentrally on PCs. Incoming and outgoing emails are scanned for viruses.
- Security tests are conducted regularly at the infrastructure level by internal staff only.

Regular Review, Assessment, and Evaluation Procedures

Measures for regular internal data protection training and employee awareness:

- Regular internal data protection training and employee awareness sessions are conducted.
- Insights gained are regularly incorporated into the further development of the portal and the data processing system.
- A data protection officer has been appointed.
- Requests from data subjects are documented by the account management and processed in a timely manner.
- A processing directory in accordance with GDPR is maintained.

Measures for User Identification and Authorization

Measures to ensure user identification and authorization:

- Employees are identified and authenticated by user ID and password.
- Access rights are only granted, changed, and withdrawn by the internal administration.
- Multi-factor authentication (MFA) is enabled on the Identity Management.
- A list of all authorized VPN users is maintained.
- Infrastructure accounts are allocated within one week of request.
- Administrative account non-repudiation measures are in place.

Measures for the Protection of Data During Transmission

Measures to protect data during transmission:

- The transfer of data between the data processing system and the user is encrypted.
- Confidential data may only be transmitted to clients in encrypted form by email.
- VPNs block parallel insecure connections.

Measures for the Protection of Data During Storage

Measures to protect data during storage:

- User data in S3 is encrypted at rest.
- Proof of media/device disposal is documented.
- Production data is not used for development or testing.
- Removable media encryption is in place.

Measures for Ensuring Events Logging

Measures to ensure events logging:

- Traceability of input, modification, and deletion of data is ensured through individual usernames and login to the management system.
- Records of access requests issues are tracked.
- Incident reports or root cause analyses are maintained.

Measures for Ensuring System Configuration, Including Default Configuration

Measures to ensure system configuration:

- A network diagram is maintained.
- Secure configuration baselines are developed.

Measures for Internal IT and IT Security Governance and Management

Measures to ensure internal IT and IT security governance:

- An information security policy is in place and regularly updated.
- Management review of the ISMS is conducted regularly.
- Internal audit reports are maintained.
- Security awareness training completion is required for all employees.

Measures for Certification/Assurance of Processes and Products

Measures for certification/assurance:

- Vendor security reviews are conducted regularly.
- Supplier/vendor agreements are in place.
- A Master Service Agreement template is used for all third-party services.

Measures for Ensuring Data Minimization

Measures to ensure data minimization:

- Pseudonymization and data masking procedures are implemented.
- Production data is not used for development or testing.
- A data inventory map is maintained.

Measures for Ensuring Data Quality

Measures to ensure data quality:

- QA process documentation is maintained.
- Competence evaluations are conducted prior to offer and hiring.
- Performance evaluations are completed regularly.
- Security awareness training completion is required for all employees.

- Employee background checks are completed.
- A company organization chart is maintained.
- Contractor agreements are in place.

Measures for Ensuring Limited Data Retention

Measures to ensure limited data retention:

- An employee termination checklist is used.
- Customer data deletion records are maintained.
- Data restore tests are conducted regularly.
- Records of access requests issues are tracked.

Measures for Allowing Data Portability and Ensuring Erasure

Measures to ensure data portability and erasure:

- Customer data deletion records are maintained.
- Data restore tests are conducted regularly.
- Records of security issues being closed within deadline (SLA) are maintained.
- Incident response plans are tested regularly.