Data Processing Agreement

Table of contents

Appendix: Processing stipulations

Userlike UG (haftungsbeschränkt)
Probsteigasse 44-46
D-50670 Cologne, Germany

– the Processor – enters into a contractual relationship with:

_____ **(Company name)**

_____ **(Street / building no.)**

_____ **(Postcode / town or city)**

– hereinafter referred to as the Customer or Controller –

in accordance with the following provisions:

1. Processing assignment and stipulations

1.1. This Data Processing Agreement (hereinafter referred to as “DPA”) sets out the rights and obligations of the Parties with regard to data protection that arise from contracts already in place between the Parties or to be concluded in future between the Parties (hereinafter referred to as the “principal contract”) regarding the processing of personal data by the Processor on behalf of the Controller.

1.2. This DPA and all of its components shall apply whenever the **Controller** engages the **Processor** in processing personal data (hereinafter referred to as “**data**”) on his behalf in accordance with Art. 28 of the General Data Protection Regulation (GDPR). As such, this DPA forms the framework for a number of different data processing procedures.

1.3. In the event of any discrepancies, the provisions of this DPA and all of its components shall take precedence over the provisions of the corresponding principal contract.

1.4. The specific data protection stipulations applicable to individual processing procedures (hereinafter referred to as “**stipulations**”) shall be set out in appendices to the DPA (hereinafter referred to as “**Appendices**”) before processing commences. These shall particularly refer to the subject matter, duration, nature and purpose of the processing, the categories of data, the categories of data subjects, and technical and organisational measures (hereinafter referred to as “**TOM**”).

1.5. The Appendices form an integral part of the DPA. In the event of any discrepancies, the Appendices shall take precedence over the more general provision in the DPA. If reference is made to the DPA in the following or in the Appendices, such reference shall be deemed to pertain to the DPA and all of its components.

2. Responsibility and processing on instruction

2.1. Within the scope of this DPA, the Controller shall be solely responsible for compliance with the applicable statutory provisions, in particular the legality of disclosure to the Processor and the legality of processing (“controller” as per Art. 4 (7) GDPR).

2.2. For the purposes of data processing, the Processor shall act solely on the instructions given by the Controller, unless an exemption applies as per Art. 28 (3)(a) GDPR (other statutory processing obligation). Any verbal instructions must be confirmed in writing without undue delay. In such a case, the Processor shall inform the Controller of these legal requirements before processing, unless the law giving rise to the exemption prohibits such notification on important grounds of public interest. If the Controller acts as data processor on behalf of a third party, the Controller's obligations under the data processing agreement with the third party shall be deemed to constitute direct instructions from the Controller in the relationship with the Processor if such obligations are stricter than those set out in this DPA. The Controller shall inform the Processor in writing of such third-party data processing requirements.

2.3. The Controller shall be entitled to issue the Processor with extensive instructions as regards the processing of data under this Agreement. The Controller's instructions may, in particular, cover: the subject matter of the processing, the purpose of the processing, the concrete nature of the processing, the data, the location of the processing, the duration of the processing, the correction and erasure of data, the restriction of processing, and the technical and organisational measures to be implemented.

2.4. The Processor shall ensure that he exclusively processes the data in accordance with the applicable law, the provisions of this Agreement and the Controller's instructions, as long as the Processor is not obligated to process the data in another way on account of the law of the European Union or of a member state to which the Controller is subject (e.g. investigations by law enforcement or protective authorities); in such a case, the Processor shall inform the Controller of these legal requirements before processing, unless the law in question prohibits such notification on important grounds of public interest (Art. 28 (3)(2)(a) GDPR). The Processor shall ensure that the aforementioned obligation is complied with by all persons acting under his authority (Art. 29 GDPR).

2.5. The Parties shall both name – in writing – one or more points of contact for data protection matters, including their appointed data protection officers. Should there be any change to a point of contact, the Party in question must inform the other Party in writing.

2.6. The Processor guarantees that the persons authorized to process the data (a) are aware of and shall comply with the Controller's instructions and (b) have undertaken to maintain confidentiality or are subject to an appropriate legal

duty of confidentiality. The obligation to maintain confidentiality and secrecy shall continue to apply once the processing has ended.

2.7. If the Controller acts as data processor on behalf of a third party, the Processor's obligations under this DPA shall also apply directly to the relationship between the third party and the Processor. This applies to all services that the Processor renders for the third party on behalf of the Controller. In particular, the third party shall directly hold the monitoring and information rights set out in Section 8 vis-à-vis the Processor.

2.8. The Processor shall not process the data for any purpose other than that stipulated in the specifications; in particular, the Processor shall not be entitled to process the data covered by this Agreement for his own purposes.

3. Security of processing

3.1. The Parties shall agree TOMs as per Art. 32 GDPR in order to ensure adequate protection of data (hereinafter referred to as "Appendix-TOM").

3.2. The Processor reserves the right to make changes to the TOMs, however in such a case it must be ensured that the overall level of protection never falls below that which was contractually agreed. Significant changes must be communicated to the Controller in writing, and require prior written consent from the same. Further, the Processor shall examine, assess and evaluate the effectiveness of the technical and organisational measures on a regular basis.

4. Notification of data breaches and errors in processing

4.1. The Processor shall, without undue delay, inform the Controller if he becomes aware of breaches of the security of the data entrusted to him by the Controller within the meaning of Art. 4 (12) GDPR in the scope of his organisation, or if he has concrete grounds to suspect such a data breach.

4.2. Should the Controller identify errors in the processing, he must inform the Processor without undue delay.

4.3. The Processor shall, without undue delay, implement the measures necessary to remedy a data breach identified as per Section 4.1or to rectify an error identified as per Section 4.2, and to minimize any adverse consequences, for instance for the data subjects. He shall consult with the Controller on this matter. Verbal notifications of data breaches as set out in

Section 4.1 or errors as set out in Section 4.2 must additionally be documented and submitted in writing without undue delay.

5. Transfer of data to a recipient in a third country or an international organisation

Transfer of data to a recipient in a third country outside of the EU or EEA is permissible if the conditions set out in Art. 44 et seqq. GDPR are met. Details shall be set out in one or more appendices if necessary.

6. Subcontracting of further processors

6.1. The Processor may have the processing of personal data performed in full or in part by other processors (hereinafter referred to as "**subcontractors**").

6.2. The Processor shall inform the Controller in writing and in good time of the commissioning of subcontractors or of changes to subcontracting arrangements. If he has just cause to do so, the Controller may object to subcontracting by declaring his objection in writing within four weeks of being notified of the subcontracting. Just cause shall particularly be deemed to exist if circumstances suggest that the subcontractor will breach the applicable legal provisions on data protection or contradict this DPA. In the event of justified objection by the Controller, he shall grant the Processor a reasonable period of time to replace the subcontractor under dispute with another subcontractor. If the Processor is unable to do so, or if this cannot reasonably be expected of the Controller, the relevant Party shall be entitled to terminate the principal contract extraordinarily for just cause.

6.3. The Processor shall agree on the same regulations as set out in this DPA with the subcontractor. In particular, the TOMs agreed with the subcontractor must provide an equal level of protection.

6.4. Services that the Processor uses exclusively as ancillary services to support his business activity outside of the scope of data processing shall not be considered subcontracting within the meaning of this provision. Nevertheless, the Processor undertakes to take appropriate precautions in order to guarantee the security of data when using such ancillary services.

6.5. In addition, subcontractors in third countries may only be commissioned if the specific prerequisites of Art. 44 et seqq. GDPR are met (e.g. adequacy decision from the Commission, standard protection clauses, approved codes

of conduct). Evidence of such must be provided to the Controller on request.

7. Rights of data subjects and assistance to the Controller

Should a data subject assert claims against one of the Parties in accordance with Chapter III GDPR, the Party in question shall inform the other Party without undue delay. The Processor shall assist the Controller to the best of his ability in handling such claims and in complying with the duties set out in Art. 33 to 36 GDPR.

8. Controller's monitoring and information rights

8.1. The Processor shall provide the Controller with appropriate evidence of compliance with his obligations. The Controller shall check that such evidence is satisfactory.

8.2. The Processor may refer to relevant certifications or other suitable test records as evidence of compliance with the agreed safeguards and of the effectiveness thereof. Certifications as stipulated in Art. 40 GDPR or records as stipulated in Art. 42 GDPR, in particular, may be deemed appropriate. The following may also be relevant, among others: certification in accordance with ISO 27001 or ISO 27017, ISO 27001 certification for basic IT security, certification according to recognized and appropriate industry standards, or an audit certificate issued in accordance with SOC / PS 951. Certification and test procedures must be performed by a recognized, independent third party. The Processor must submit his certificates or test records. Further suitable documents (e.g. activity reports from the data protection officer or excerpts from auditors' reports) may be provided to the Controller as evidence of compliance with the agreed safeguards. The Controller's right of inspection, as set out in Section 8.3, shall not be affected thereby.

8.3. The Controller shall be entitled to perform inspections on the Processor's premises in order to check compliance with data protection provisions; such inspections shall take place during normal business hours but without disrupting operations, normally following prior notification and with reasonable notice. The Processor may make the inspection conditional upon signature of a non-disclosure agreement regarding the data of other customers and upon his TOMs.

8.4. The Parties shall agree any measures to be implemented to remedy issues identified during an inspection.

8.5. Should a supervisory authority exercise its powers as set out in Art. 58 GDPR, the Party in question shall inform the other Party without undue delay. The Parties shall support one another, within their area of responsibility, in meeting their obligations towards the supervisory authority.

9. Liability and compensation

9.1. Should a data subject assert claims for compensation against a Party on account of a breach of data protection provisions, the Party in question shall inform the other Party without undue delay.

9.2. The Controller and the Processor shall be liable towards data subjects in the manner set out in Art. 82 GDPR.

9.3. The Parties shall mutually support one another in defending against claims for compensation from data subjects, unless this would jeopardize the legal position of one Party in relation to the other Party, to the supervisory authority or to third parties.

10. Term

The DPA and the Appendix shall terminate when the corresponding principal contract ends, without requiring separate notice of termination of the Appendix. In this event, the Processor must – without undue delay and at the Controller's choice – hand over the data processed under the Appendix or erase the data in accordance with the data protection provisions and provide the Controller with written confirmation that erasure has taken place. If the Processor is subject to a legal obligation to store the data, he must inform the Controller of such in writing.

11. Continuation and transfer of old contracts

The DPA shall replace the existing contracts – drafted in accordance with Section 11 of the German Federal Data Protection Act (BDSG) – as soon as it is signed. If the Parties have agreed to stipulations as per Section 1 before conclusion of this DPA, these shall continue to apply accordingly under the

DPA unless they are replaced by appendices referring to the same subject matter.

12. Information for end customers

The Processor shall allow the Controller to personalize the chat widget and to expand the functional scope of the service. All settings shall be stored in the Controller's customer account. The activation of optional chat functions is not necessary to operate the core chat service, and is voluntary for the Controller.

Depending on the function used, the activation of these optional functions can lead to personal data belonging to the Controller's end customers being forwarded on to third-party providers for further processing. These third-party providers are not considered (further) processors of the Processor.

13. Final provisions

13.1. Should the data belonging to the Controller and held by the Processor be jeopardized by seizure, confiscation, insolvency or settlement proceedings, or other events or measures implemented by third parties, the Processor shall inform the Controller in writing without undue delay. The Processor shall, without undue delay, inform all persons responsible in this context that the responsibility for the data lies exclusively with the Controller.

13.2. No verbal side agreements have been made. Changes and additions to the DPA must be in writing and refer expressly to the DPA in order to be effective. Any deviating verbal agreements between the Parties shall be ineffective. The same shall apply to any changes to this clause.

13.3. Should a single provision of this DPA be fully or partially legally ineffective or invalid, this shall not affect the rest of the DPA. The ineffective or invalid provision shall be deemed replaced by the law, if the resulting loophole cannot be closed by supplementary contractual interpretation as set out in Sections 133, 157 of the German Civil Code (BGB). However, both Parties undertake, without undue delay, to enter into negotiations with the aim of agreeing a replacement provision for the ineffective or invalid provision that comes as close as possible to the legal and economic meaning and purpose of the ineffective or invalid provision, in particular taking account of the nature

of the agreement as a means of regulating continuing obligations with regard to data protection matters.

13.4. German law shall apply, to the exclusion of conflict of laws provisions; Art. 3 (3)(4) of the Rome I Regulation shall not be affected.

Controller:

_____

Date and location (mandatory)

_____

Signature (mandatory)

_____

Print name (mandatory)

_____

Role within company (optional)

Processor:

Cologne, 10th May 2019 

Timoor Taufig / CEO

Appendix: Processing stipulations

The Parties agree the following stipulations with regard to the Data Processing Agreement:

1. Subject matter of the processing

The subject matter of the processing is the provision of the Userlike services set out in Userlike's Terms & Conditions (hereinafter referred to as the "principal contract") by the Processor for the Controller.

2. Duration of the processing

The duration of the processing is as set out in the principal contract.

3. Purpose of the processing

The processing shall take place continuously throughout the term of the principal contract.

The Processor offers a live chat function for web and mobile support. The software-based chat communication solution offers customer support in real time and helps to expand the customer service offering.

The Processor shall fully process personal data from within the Controller's domain within the meaning of Art. 4 (2) GDPR, exclusively in order to fulfil the former's obligations under the principal contract in conjunction with the provision of Userlike services; this shall particularly include the collection, storage, modification, export, access, use, disclosure, comparison, linkage and erasure of data.

4. Categories of data

The categories of data affected by the processing depend on the use of Userlike services by the Controller. The possible categories of data that fall within the subject matter of the processing are:

End user

- Chat transcript
- E-mail address
- Browser
- Operating system
- Device
- Number of page requests
- Number of page visits
- Referrer
- URL (where the chat originated)
- Questionnaire before and after the chat
- Chat topic
- Chat status (new, pending, closed)
- Chat evaluation after the chat
- Duration of the chat
- Date of the chat
- Screenshot of the browser tab into which Userlike is integrated
- Optional data fields that the company passes on to Userlike
- IP addresses (in the context of IT security, for the purposes of attack analysis and control and protection of customers; in order to respond to queries from the prosecutor's office in the context of criminal investigations)

Company data

- Company name
- Language

- Time zone
- Country
- Service hours
- Payment information (e.g. credit card, PayPal, bank details)
- Analytics figures for chat performance

Operator's profile settings

- Username
- First name
- Surname
- Alias name
- Email address
- Language
- Time zone
- Operator group
- Profile photo
- Chat transcripts
- Analytics figures on chat performance
- IP addresses (in the context of IT security, for the purposes of attack analysis and control and protection of customers; in order to respond to queries from the prosecutor's office in the context of criminal investigations)

Whether the Processor's Userlike services are suitable for the processing of special categories of personal data as per Art. 9 (1) GDPR is a matter that requires a risk assessment by the Controller.

5. Categories of data subjects

The categories of data subjects affected by the processing depend on the use of Userlike services by the Controller. Possible categories of data subjects are:

- Customers
- Website visitors
- Interested parties
- Employees

6. Subcontractors

The Processor shall employ the following subcontractors for the processing:

Service provider	Processing of personal data	Explanation and purpose
Hetzner Online GmbH Industriestr. 25 D-91710 Gunzenhausen, Germany	Yes	Hosting of the servers. Data: Appendix, Items 4 and 5
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg	Yes	The following personal data – exclusively – shall be processed by AWS for export of technical components (such as DNS, website images, JavaScript code, style sheet files) within the scope of use of the AWS Content Delivery Network, and erased after 24 hours: ● IP address ● Browser ● Operating system ● Time stamp ● Encryption algorithm ● Encryption protocol

7. Disclosure of data to recipients in third countries or international organizations

There shall be no disclosure of personal data to recipients in third countries or international organizations.

8. Contact details of data protection officer

Dr. Jochen Notholt

Lindwurmstr. 10

80337 Munich

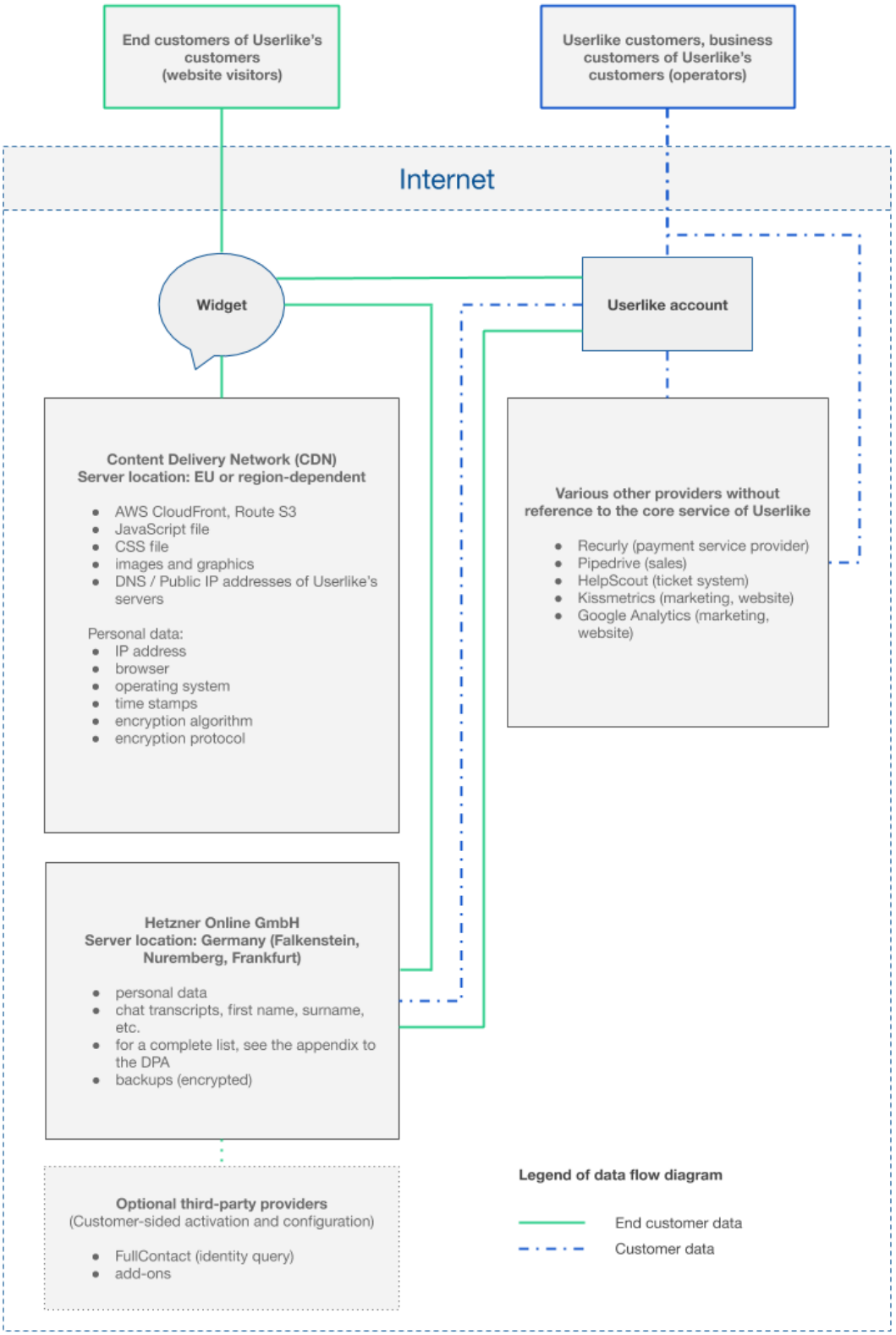
Germany

E-mail: privacy@userlike.com

Technical and organisational measures for data processing as per Art. 32 GDPR

1. Data flow diagram

The general flow of data is shown on the following chart:



2. Organisational control

Objective: The processor's staff must be obligated to maintain data secrecy and to comply with confidentiality provisions. Commitment to this obligation must be documented in personnel files so that it can be produced as evidence at any time.

Corresponding documents are stored in personnel files.

- There is a text module set out in the standard contract for all employees.
- Employees are informed of their duties again in training sessions.

3. Physical access control

Objective: Unauthorized persons must be prevented from gaining (physical) access to data processing systems on which personal data is processed or used. The processor shall install an entry control system for this purpose.

Description of entry control systems in the office (including physical precautions):

- Mechanical locking system on main entrance and office entrances
- Electronic alarm system and unlocking with 24/7 site security
- Cameras

Description of surveillance systems:

- Alarm system with link to site security – Wachschutz Berger, Cologne
- 3 x Ubiqity cameras + external server

4. System access control

Objective: Use of data processing systems by unauthorized persons must be prevented. To this end, access to DP systems must be monitored and logged (e.g. prevention of system login, unauthorized upload to and intrusion into DP system).

Intrusion of unauthorized persons into the DP systems must be prevented.

Description of the authentication mechanisms implemented (e.g. password complexity, change cycles, SSH keys):

- SSH: Public private keys
- Maintenance work: OpenVPN (certificates) S2S communication: IPSec
- C2S communication: TLS 1.2

Description of measures upon temporary inactivity of users (e.g. when an employee leaves their desk):

- Hot Corners are configured in the MacOS X system; this allows users to quickly swipe the cursor to a corner in order to bring up the lock-out screensaver. Otherwise, the monitor locks out after 30 seconds.
- All employees are encouraged to always lock their screens.

Description of technical safeguards for your network environment:

- iptables rules on external interfaces
- Services only listen in on internal cards
- IPSec communication for servers
- Weekly nmpa, nikto scans
- Monthly OpenVAS scans
- Daily monitoring with Grafana
- Daily audit of new critical errors
- Anti-DDoS in the data centre
- OpenVPN tunnel to internal services

5. Data access control

Objective: It must be ensured that persons authorized to use a data processing system are only able to access the data for which they have access authorization and that personal data cannot be read, copied, modified or erased without authorization during processing or use or after storage.

Personal data must be encrypted in the case of persistent storage.

Needs-oriented design of the authorization concept and access rights, as well as monitoring and logging thereof:

Description of the prevention of unauthorized activity in DP systems outside of granted authorizations (roles and authorizations according to the need-to-know principle):

- Rights and role management

Description of measures to prevent unauthorized access (e.g. brute force, SQL injection, login validation):

- SSH: fail2ban
- Checks in the backend with native django security precautions

Description of mechanisms to ensure that only personalized user accounts are used to access the systems (one account per user):

- 1 account per user
- 1 VPN account per user
- 1 account on a computer

Description of encryption measures implemented for personal data:

- Hard drive encryption with LUKS default settings
- Transport encryption with TLS 1.2
- IPSec
- OpenVPN
- SSH safeguards: GPG

5.1. Transfer control

Objective: It must be ensured that personal data cannot be read, copied, modified or erased without authorization during electronic transfer or during transport or storage on data carriers, and that it is possible to check and identify where transfer of personal data by data transfer systems is expected to take place.

Personal data must be encrypted for transfer (transport encryption).

Description of transport encryption:

- Transport encryption with TLS 1.2
- IPSec
- OpenVPN
- SSH

Description of the logging of personal data transfer:

- Not applicable. Personal data is not downloaded or transferred from servers. Back-ups are the exception. Back-ups are logged. Manually checked on a daily basis.

Description of transport protection for physical transport:

- Not applicable. Personal data is not physically transported from servers.

5.2. Input control

Objective: It must be ensured that it is possible to check and establish at a later date whether personal data was entered into, modified in or erased from data processing systems, and by whom.

A detailed logging system for the input, modification and erasure of personal data (e.g. log files) must be implemented and assessed on a regular basis.

Description of the logging/monitoring system for monitoring access:

- The customer has an audit log available to them. The audit log is a log listing all changes to the customer's account. This data is personal and can only be viewed and checked by the customer in exceptional circumstances, and with consent from the processor's employees.
- Various logs are kept on server level; these are compiled upon login of employees during maintenance work. These logs are checked on a random basis.
- In addition, various logs showing the technical status of the system are generated.

5.3. Availability control

Objective: It must be ensured that personal data is protected against accidental loss or destruction.

Description of the data security concept (e.g. back-up procedure, redundancies, UPS, emergency plans):

- 3 data centres (system available in triplicate)
- 2 different sites/data centres
- UPSs and diesel generators
- Mirrored hard drives
- Enterprise hard drives
- Auto failover for web nodes
- Auto failover for statistical data
- Automated monitoring
- Daily back-ups of all data
- Back-ups in 2 different locations
- Several employees managing the process

5.4. Separation rule

Objectives: It must be ensured that personal data collected for different purposes can be processed separately. The processor shall ensure demonstrable logical separation of the client's data, i.e. data from different controllers must be processed separately. Mutual access must be excluded. In addition, data must only be processed for a specific purpose.

Description of implementation for multi-client capability:

- Data is processed for a specific purpose and is separated logically by client on database level (multi-client capability).

Description of mechanisms to ensure the separation of development, testing and productive systems:

Physical separation (different servers) in 3 environments:

- Development
- Staging
- Production

5.5. Information security

Description of the information security management system (ISMS):

Various processes:

- IT security process
    - Input: Scans, messages, logs
    - Processing: Evaluation
    - Output: Measures
    - Tools: nmap, nikto, rkhunter, maldet, OpenVAS
- Responsibility:
    - IT Security: security@userlike.com
    - Data Privacy: privacy@userlike.com
- Regular training
    - IT security
    - Data protection
    - Fixed processes
    - Onboarding
    - Offboarding
- Rights and role management

5.6. Miscellaneous

Description of mechanisms to ensure confidential storage and erasure or destruction of test and scrap materials containing personal data (e.g. paper):

- Not applicable. No paper used. Excluding bookkeeping and contracts. Documents are shredded.

6. Use of subcontractors

The technical and organizational measures implemented by the other processors that we use at the point at which this agreement is concluded are enclosed with this document as an appendix. We regularly verify the appropriateness and effectiveness of the measures implemented by our subcontractors.

7. Processor's assurance

The processor guarantees that all information provided in this document is truthful.

Appendix:

TOMs for Hetzner Online GmbH
TOMs for Amazon Web Services SARL

Appendix 2 of the Agreement Pursuant to Art. 28 GDPR: Technical and Organizational Measures in Accordance with Art. 32 GDPR and Amendments

I. Confidentiality

- Physical access control
  - Data center parks in Nürnberg and Falkenstein
    - electronic physical entry control system with log
    - high security perimeter fencing around the entire data center park
    - documented distribution of keys to employees and colocation customers for colocation racks (each Client only for his rack)
    - policies for accompanying and designating guests in the building
    - data center staff present 24/7
    - video monitoring at entrances and exits; security door interlocking systems and server rooms
    - For people outside of the employment of Hetzner Online GmbH (data center visitors), entrance to the building is only permitted in the company of a Hetzner Online employee.
  - Monitoring
    - electronic physical access control system with log
    - video surveillance for all entrances and exits
- Electronic access control
  - for dedicated root server, colocation server, and cloud server principal commissions
    - server passwords, which, after the initial deployment, can only be changed by Client and are not known to the Supplier
    - The Client's password for the administration interface is determined by the Client himself; the password must comply with predefined guidelines. In addition, the Client may employ two-factor authentication to further secure his account.
  - for managed server, web hosting, and storage box principal commissions
    - Access is password-protected and only employees of the Supplier have access to the passwords. Passwords must meet a minimum length, and new passwords shall be changed on a regular basis.
- Internal access control
  - for the Supplier's internal administration systems
    - The Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
    - a revision-proof, compulsory process for allocating authorization for Supplier employees
  - for dedicated root server, colocation server, and cloud server principal commissions

Hetzner Online GmbH
CEO: Martin Hetzner
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

        - The responsibility for access control is incumbent upon the Client.
    - for managed server, web hosting, and storage box principal commissions
        - The Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
        - a revision-proof, compulsory process for allocating authorization for Supplier employees
        - Only the Supplier is responsible for transferred data/software with regard to security and updates.
- Transfer control
    - Data center parks in Nürnberg and Falkenstein
        - Drives that were in operation on canceled servers will be swiped multiple times (deleted) in accordance with data protection polices upon termination of the contract. After thorough testing, the swiped drives will be reused.
        - Defective drives that cannot be securely deleted shall be destroyed (shredded) directly in the Falkenstein data center.
- Isolation control
    - for the Supplier's internal administration systems
        - Data shall be physically or logically isolated and saved separately from other data.
        - Backups of data shall also be performed using a similar system of physical or logical isolation.
    - for dedicated root server, colocation server, and cloud server principal commissions
        - The Client is responsible for isolation control.
    - for managed server, web hosting, and storage box principal commissions
        - Data shall be physically or logically isolated and saved separately from other data.
        - Backups of data shall also be performed using a similar system of physical or logical isolation.
- Pseudonymization
    - The Client is responsible for pseudonymization.

II. Integrity (Art. 32 Para.1 Clause b GDPR)

- Data transfer control
    - All employees are trained in accordance with Art. 32 Para. 4 GDPR and are obliged to ensure that personal data is handled in accordance with data protection regulations.
    - Deletion of data in accordance with data protection regulations after termination of the contract.
    - Encrypted data transmission options are provided within the scope of the service description of the principal commission.

Hetzner Online GmbH
CEO: Martin Hetzner
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

- Data entry control
  - for the Supplier's internal administration systems
    - Data is entered or collected by the Client.
    - Changes in data are logged.
  - for dedicated root server, colocation server, and cloud server principal commissions
    - The responsibility for input control is incumbent upon the Client.
  - for managed server, web hosting, and storage box principal commissions
    - Data is entered or collected by the Client.
    - Changes in data are logged.

III. Availability and Resilience (Art. 32 Para. 1 Clause b GDPR)

- Availability control
  - for the Supplier's internal administration systems
    - backup and recovery concept with daily backups of all relevant data
    - professional employment of security programs (virus scanners, firewalls, encryption programs, spam filters)
    - employment of disk mirroring on all relevant servers
    - monitoring of all relevant servers
    - employment of an uninterruptible power supply system or emergency power supply system
    - permanently active DDoS protection
  - for dedicated root server, colocation server, and cloud server principal commissions
    - Data backup is incumbent upon the Client.
    - employment of an uninterruptible power supply system or emergency power supply system
    - permanently active DDoS protection
  - for managed server, web hosting, and storage box principal commissions
    - backup and recovery concept with daily backups of all relevant data depending upgon the services booked for the principal commission
    - employment of disk mirroring
    - employment of an uninterruptible power supply system or emergency power supply system
    - employment of software firewalls and restricted ports
    - permanently active DDoS protection
- Rapid recovery measures (Art. 32 Para. 1 Clause c GDPR)
  - For all internal systems, there is a defined escalation chain which specifies who is to be informed in the event of an error in order to restore the system as quickly as possible.

Hetzner Online GmbH
CEO: Martin Hetzner
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

IV. Procedures for regular testing, assessment, and evaluation (Art. 32 Para. 1 Clause d GDPR; Art. 25 Para. 1 GDPR)

- The data protection management system and the information security management system have been combined into a DIMS (data protection information security management system).
- Incident response management is available.
- Data-protection-friendly default settings are taken into account for software development (Art. 25 Para. 2 GDPR).

- Agreement or contract control
  - Hetzner Onling GmbH employees are regularly instructed in data protection law and are familiar with the procedural instructions and user guidelines for data processing on behalf of the Client also with regard to the Client's right of instruction. The General Terms and Conditions contain detailed information on the type and scope of the commissioned data processing and use of the Client's personal data.
  - The General Terms and Conditions contain detailed information about the purpose limitation of Client's personal data.
  - Hetzner Online GmbH has appointed a company Data Protection Officer and an Information Security Officer. The data protection organization and the information security management systems integrate both officers into the relevant operational procedures.

Hetzner Online GmbH
CEO: Martin Hetzner
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

Annex 1

AWS Security Standards

1. **Information Security Program.** AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

   1.1 **Network Security.** The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

   1.2 **Physical Security**

      1.2.1 **Physical Access Controls.** Physical components of the AWS Network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

      1.2.2 **Limited Employee and Contractor Access.** AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

      1.2.3 **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. **Continued Evaluation**. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

[Remainder of Page Intentionally Left Blank]

Vertrag über die Auftragsverarbeitung

Inhaltsverzeichnis

Userlike UG (haftungsbeschränkt)
Probsteigasse 44-46
D-50670 Köln

verpflichtet sich als Auftragnehmer gegenüber:

_____ **(Unternehmen)**

_____ **(Straße / Haus-Nr.)**

_____ **(PLZ / Ort)**

- nachfolgend als Kunde oder Auftraggeber,

nach Maßgabe der folgenden Bestimmungen:

1. Auftrag und Festlegungen zur Verarbeitung

1.1. Dieser Vertrag über die Auftragsverarbeitung (nachfolgend „AVV“) konkretisiert für alle Verarbeitungen die datenschutzrechtlichen Rechte und Pflichten der Parteien, welche sich aus den zwischen den Parteien bereits bestehenden oder künftig abzuschließenden Verträgen (nachfolgend „Hauptvertrag“) ergeben, unter denen es zu einer Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber kommt.

1.2. Dieser AVV kommt mit all seinen Bestandteilen zur Anwendung, wenn der **Auftraggeber** den **Auftragnehmer**, zur Verarbeitung personenbezogener Daten (nachfolgend „**Daten**“) im Auftrag gemäß Art. 28 DSGVO verpflichtet hat. Dabei bildet dieser AVV den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung.

1.3. Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV mit all seinen Bestandteilen den Regelungen des zugehörigen Hauptvertrages vor.

1.4. Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (nachfolgend „**Festlegungen**“) werden vor Beginn der Verarbeitung in Anlagen zum AVV (nachfolgend „**Anlagen**“) geregelt. Dies sind insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorien von Daten und die Kategorien betroffener Personen sowie die technischen und organisatorischen Maßnahmen (nachfolgend „**TOM**“).

1.5. Die Anlagen sind Teil des AVV. Bei etwaigen Widersprüchen gehen die Anlagen der allgemeineren Regelung im AVV vor. Wird im Folgenden oder in den Anlagen auf den AVV Bezug genommen, so ist der AVV mit all seinen Bestandteilen gemeint.

2. Verantwortlichkeit und Verarbeitung auf Weisung

2.1. Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ gemäß Art. 4 Nr. 7 DSGVO).

2.2. Der Auftragnehmer handelt wegen der Verarbeitung der Daten ausschließlich weisungsgebunden, es sei denn es liegt ein Ausnahmefall gemäß Art. 28 Abs. 3 lit. a) DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. In einem solchen Fall

teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das den Ausnahmefall begründende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Wird der Auftraggeber als Auftragnehmer einer Auftragsverarbeitung für einen Dritten tätig, gelten die Verpflichtungen des Auftraggebers aus dieser Auftragsverarbeitung für den Dritten unmittelbar als Weisungen des Auftraggebers im Verhältnis zum Auftragnehmer, sofern diese Verpflichtungen strenger sein sollten als diejenigen aus diesem AVV. Der Auftraggeber wird den Auftragnehmer über solche Anforderungen Dritter an die Auftragsverarbeitung schriftlich in Kenntnis setzen.

2.3. Der Auftraggeber ist berechtigt, dem Auftragnehmer mit Blick auf die Verarbeitung der Daten im Rahmen dieses Vertrags umfassende Weisungen zu erteilen. Die Weisungen Auftraggebers können insbesondere umfassen: den Gegenstand der Verarbeitung, den Zweck der Verarbeitung, die konkrete Art der Verarbeitung, die Daten, den Ort der Verarbeitung, die Dauer der Verarbeitung, die Korrektur und Löschung der Daten, die Einschränkung der Verarbeitung und die einzusetzenden technischen und organisatorischen Maßnahmen.

2.4. Der Auftragnehmer stellt sicher, dass er die Daten ausschließlich in Übereinstimmung mit dem geltenden Recht, den Bestimmungen dieses Vertrags und den Weisungen des Auftraggebers verarbeitet, sofern der Auftragnehmer nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder eines Mitgliedstaates, dem der Auftraggeber unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Der Auftragnehmer stellt sicher, dass die vorstehende Pflicht durch jede, dem Auftragnehmer unterstellte Person eingehalten wird (Art. 29 DSGVO).

2.5. Die Parteien benennen gegenseitig in Textform einen oder mehrere Ansprechpartner in datenschutzrechtlichen Angelegenheiten, einschließlich der bestellten Datenschutzbeauftragten. Ergeben sich bei den Ansprechpartnern Änderungen, haben sich die Parteien hierüber in Textform zu informieren.

2.6. Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der Daten befugten Personen (a) die Weisungen des Auftraggebers kennen und diese beachten, sowie (b) sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die

Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.

2.7. Wird der Auftraggeber als Auftragnehmer einer Auftragsverarbeitung für einen Dritten tätig, gelten die Verpflichtungen des Auftragnehmers aus diesem AVV auch unmittelbar im Verhältnis zwischen dem Dritten und dem Auftragnehmer. Dies gilt für alle Leistungen des Auftragnehmers, welche dieser im Auftrag des Auftraggebers gegenüber dem Dritten erbringt. Insbesondere stehen dem Dritten die Kontroll- und Informationsrechte aus § 8 unmittelbar gegenüber dem Auftragnehmer zu.

2.8. Der Auftragsverarbeiter verarbeitet die Daten zu keinem anderen Zweck, als dem in der Spezifikation vorgegebenen; insbesondere ist der Auftragsverarbeiter nicht berechtigt, von dieser Vereinbarung umfasste Daten für eigene Zwecke zu verarbeiten.

3. Sicherheit der Verarbeitung

3.1. Die Parteien vereinbaren TOM gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten (nachfolgend „Anlage-TOM“).

3.2. Änderung der Anlage-TOM bleiben dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen und bedürfen der vorherigen Zustimmung durch den Auftraggeber in Textform. Der Auftragnehmer wird zudem die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig überprüfen, bewerten und evaluieren.

4. Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

4.1. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der ihm vom Auftraggeber anvertrauten Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Auftragnehmer besteht.

4.2. Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Auftragnehmer unverzüglich hierüber zu unterrichten.

4.3. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung gemäß § 4.1 oder der Fehler gemäß § 4.2 sowie zur Minderung möglicher nachteiliger Folgen, insbesondere für

die betroffenen Personen. Hierüber stimmt er sich mit dem Auftraggeber ab. Mündliche Unterrichtungen § 4.1 oder § 4.2 sind unverzüglich in Textform nachzureichen.

5. Übermittlung von Daten an einen Empfänger in einem Drittland oder in einer internationalen Organisation

Die Übermittlung von Daten an einen Empfänger in einem Drittland außerhalb von EU und EWR ist unter Einhaltung der in Art. 44 ff. DSGVO festgelegten Bedingungen zulässig. Einzelheiten werden bei Bedarf in einer oder mehreren Anlagen geregelt.

6. Unterbeauftragung weiterer Auftragsverarbeiter

6.1. Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachfolgend „**Unterauftragnehmer**“) erbringen lassen.

6.2. Der Auftragnehmer informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn aufgrund von Tatsachen angenommen werden kann, dass der Unterauftragnehmer die einschlägigen gesetzlichen Bestimmungen zum Datenschutz missachten wird oder dieser AVV zuwiderhandeln wird. Im Fall eines begründeten Widerspruchs des Auftraggebers räumt dieser dem Auftragnehmer eine angemessene Frist ein, um den vom Widerspruch betroffenen Unterauftragnehmer durch einen anderen Unterauftragnehmer zu ersetzen. Ist dem Auftragnehmer dies nicht möglich oder dem Auftraggeber nicht zumutbar, ist die jeweilige Partei zur außerordentlichen Kündigung des Hauptvertrags aus wichtigem Grund berechtigt.

6.3. Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden TOM ein gleichwertiges Schutzniveau aufweisen.

6.4. Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch

nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

6.5. Eine Beauftragung von Subunternehmern in Drittstaaten darf zudem nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Diese sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

7. Rechte betroffener Personen und Unterstützung des Auftraggebers

Macht eine betroffene Person Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

8. Kontroll- und Informationsrechte des Auftraggebers

8.1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Der Auftraggeber überprüft die Geeignetheit.

8.2. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit kann der Auftragnehmer auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Zertifizierungen nach Art. 40 DSGVO oder Nachweise nach Art. 42 DSGVO. Daneben kommen unter anderem in Betracht: eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards oder ein Prüfungsnachweis gemäß SOC / PS 951. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen. Der Auftragnehmer hat seine Zertifikate oder Prüfungsnachweise zur Verfügung zu stellen. Weitere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Wirtschaftsprüfer) können zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen dem Auftraggeber zur Verfügung gestellt werden. Das Inspektionsrecht des Auftraggebers aus § 8.3 bleibt hiervon unberührt.

8.3. Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter

Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Auftragnehmer zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Auftragnehmer darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen TOM abhängig machen.

8.4. Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien die umzusetzenden Maßnahmen ab.

8.5. Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.

9. Haftung und Schadenersatz

9.1. Macht eine betroffene Person gegenüber einer Partei Schadenersatzansprüche wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

9.2. Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

9.3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei, zur Aufsichtsbehörde oder gegenüber Dritten gefährden.

10. Laufzeit

Der AVV sowie die Anlage enden mit Beendigung des zugehörigen Hauptvertrags, ohne dass es einer gesonderten Kündigung dieser Anlage bedarf. Der Auftragnehmer hat in diesem Fall nach Wahl des Auftraggebers unverzüglich die nach der Anlage verarbeiteten Daten herauszugeben oder datenschutzkonform zu löschen und dies dem Auftraggeber in Textform zu bestätigen. Sofern der Auftragnehmer eine eigene gesetzliche Pflicht zur Speicherung dieser Daten hat, hat er dies dem Auftraggeber in Textform anzuzeigen.

11. Fortgeltung und Überleitung von Altverträgen

Der AVV ersetzt mit Wirkung ab seiner Unterzeichnung die bestehenden Verträge nach § 11 BDSG. Haben die Parteien vor Abschluss dieses AVV Festlegungen nach § 1 vereinbart, so gelten diese sinngemäß unter dem AVV fort, es sei denn sie werden durch Anlagen ersetzt, denen derselbe Verarbeitungsgegenstand zu Grunde liegt.

12. Unterrichtung der Endkunden

Der Auftragnehmer erlaubt dem Auftraggeber, das Chat-Widget zu individualisieren und den Funktionsumfang der Dienstleistung zu erweitern. Alle Einstellungen werden im Kundenkonto des Auftraggebers gespeichert. Das Aktivieren optionaler Chat-Funktionen ist für den Betrieb der Kerndienstleistung des Chats nicht notwendig und eine freiwillige Entscheidung des Auftraggebers.

Die Aktivierung dieser optionalen Funktionen, kann je nach genutzter Funktion dazu führen, dass personenbezogene Daten der Endkunden des Auftraggebers zur Weiterverarbeitung an Drittanbieter weitergeleitet werden. Bei diesen Drittanbietern handelt es sich nicht um (weitere) Auftragnehmer des Auftragnehmers.

13. Schlussbestimmungen

13.1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber in Textform zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.

13.2. Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

13.3. Sollte nur eine Bestimmung dieses AVV ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen unberührt. An Stelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide

Parteien sind jedoch verpflichtet, unverzüglich Verhandlungen aufzunehmen mit dem Ziel einer Vereinbarung an Stelle der rechtsunwirksamen oder nichtigen Bestimmung, die deren Sinn und Zweck in rechtlicher und wirtschaftlicher Hinsicht am Nächsten kommt, insbesondere dem Charakter der Vereinbarung als Dauerschuldverhältnis zur Regelung datenschutzrechtlicher Belange gerecht wird.

13.4. Es gilt deutsches Recht unter Ausschluss des Kollisionsrechts; Art. 3 Abs. 3, Abs. 4 ROM-I-VO bleiben unberührt.

Auftraggeber:

_____

Datum und Ort (Pflichtfeld)

_____

Unterschrift (Pflichtfeld)

_____

Name in Druckbuchstaben (Pflichtfeld)

_____

Funktion im Unternehmen (optional)

Auftragnehmer:

Köln, 10. Mai 2019 _____

Timoor Taufig / CEO

Anlage: Feststellung zur Auftragsverarbeitung

Die Parteien treffen zum Vertrag über die Auftragsverarbeitung ergänzend folgende Festlegungen:

1. Gegenstand der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung der in den Allgemeinen Geschäftsbedingungen von Userlike (nachfolgend „**Hauptvertrag**“) bezeichneten Userlike Services durch den Auftragnehmer für den Auftraggeber.

2. Dauer des Auftrags

Die Dauer der Verarbeitung ergibt sich aus dem Hauptvertrag.

3. Zweck der Verarbeitung

Die Verarbeitung erfolgt fortlaufend über die Laufzeit des Hauptvertrags.

Der Auftragnehmer bietet eine Live-Chat-Funktion für den Web- und Mobilsupport. Die softwarebasierte Lösung zur Chat-Kommunikation bietet einen Kundensupport in Echtzeit und hilft den Kundenservice auszubauen.

Ausschließlich zur Erfüllung der Pflichten des Auftragnehmers aus dem Hauptvertrag im Zusammenhang mit der Bereitstellung der Userlike Services werden personenbezogene Daten aus dem Herrschaftsbereich des Auftraggebers durch den Auftragnehmer vollumfänglich i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet, insbesondere erhoben, gespeichert, verändert, ausgelesen, abgefragt, verwendet, offengelegt, abgeglichen, verknüpft und gelöscht.

4. Kategorien von Daten

Die von der Verarbeitung betroffenen Kategorien von Daten hängen von der Nutzung der Userlike Services durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind:

Endnutzer

- Chat-Transkript
- Email-Adresse
- Browser
- Betriebssystem
- Endgerät
- Anzahl der Seitenaufrufe
- Anzahl der Seitenbesuche
- Referrer
- URL (wo der Chat gestartet ist)
- Umfrage vor und nach dem Chat
- Chat-Thema
- Chat-Status (new, pending, closed)
- Chat-Bewertung nach dem Chat
- Dauer des Chats
- Datum des Chats
- Screenshot des Browser-Tabs auf dem Userlike integriert ist
- Optionale Datenfelder, die das Unternehmen an Userlike übergibt
- IP-Adressen (im Kontext der IT-Security, zum Zweck der Angriffsanalyse und Angriffsbekämpfung und Schutz der Kunden; zur Beantwortung von Anfragen seitens der Staatsanwaltschaft im Kontext von strafrechtlichen Ermittlungen)

Unternehmensdaten

- Firma
- Sprache
- Zeitzone

- Land
- Service-Zeiten
- Zahlungsinformationen (z. B. Kreditkarte, Paypal, Bankverbindung)
- Analytics-Kennzahlen zur Chat-Performance

Profileinstellungen des Operators

- Username
- Vorname
- Nachname
- Alias-Name
- Email-Adresse
- Sprache
- Zeitzone
- Operator-Gruppe
- Profilfoto
- Chat Transkripte
- Analytics-Kennzahlen zur Chat-Performance
- IP-Adressen (im Kontext der IT-Security, zum Zweck der Angriffsanalyse und Angriffsbekämpfung und Schutz der Kunden; zur Beantwortung von Anfragen seitens der Staatsanwaltschaft im Kontext von strafrechtlichen Ermittlungen)

Ob die Userlike Services des Auftragnehmers für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO geeignet ist, bedarf einer Risikobewertung durch den Auftraggeber.

5. Kategorien betroffener Personen

Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der Nutzung der Userlike Services durch den Auftraggeber ab. Als Kategorien betroffener Personen kommen dabei in Betracht:

- Kunden
- Website-Besucher

- Interessenten
- Beschäftigte

6. Unterauftragnehmer

Der Auftragnehmer setzt für die Verarbeitung folgende Unterauftragnehmer ein:

Dienstleister	**Verarbeitung personenbezogener Daten**	**Erläuterung und Zweck**
Hetzner Online GmbH Industriestr. 25 D-91710 Gunzenhausen	ja	Hosting der Server. Daten: Anlage, Ziffer 4 und 5
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg	ja	Im Rahmen der Nutzung des AWS-Content Delivery Networks zum Ausspielen der technischen Komponenten (wie DNS, Bilder der Webseite, JavaScript Code, Stylesheet-Dateien) werden ausschließlich die folgenden personenbezogenen Daten durch AWS verarbeitet und nach 24 Stunden gelöscht: • IP-Adresse • Browser • Betriebssystem • Zeitstempel • Verschlüsselungsalgorithmus • Verschlüsselungsprotokoll

7. Offenlegung von Daten an Empfänger in Drittländern oder internationalen Organisationen

Es findet keine Offenlegung von personenbezogenen Daten gegenüber Empfängern in Drittländern oder internationalen Organisationen statt.

8. Kontaktdaten Datenschutzbeauftragter

Dr. Jochen Notholt

Lindwurmstr. 10

80337 München

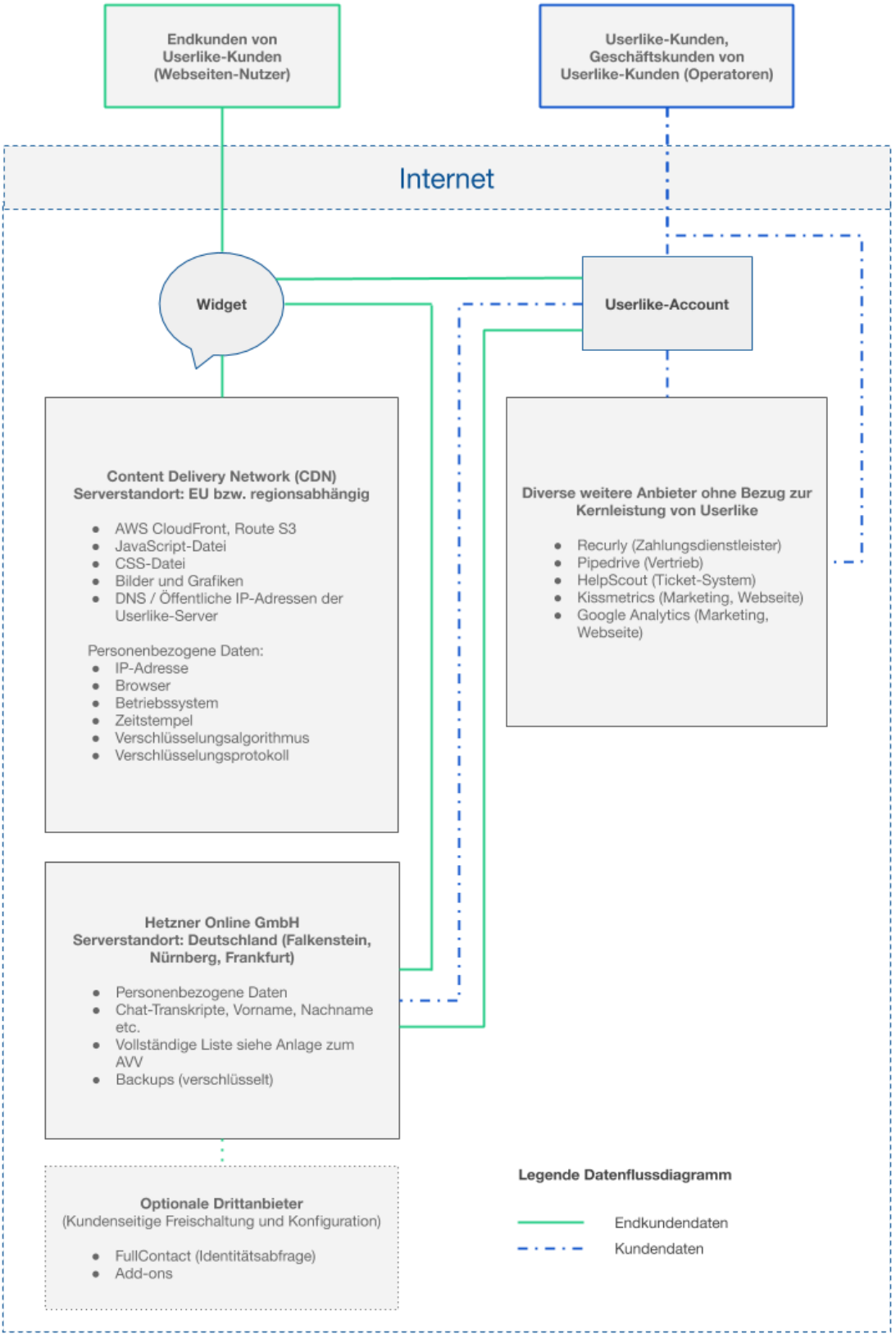
Deutschland

E-Mail: privacy@userlike.com

Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO bei der Auftragsverarbeitung

1. Datenflussdiagramm

Auf dem nachfolgenden Chart ist der grobe Datenfluss dargestellt:



2. Organisationskontrolle

Sollvorgabe: Das Personal des Auftragnehmers ist auf das Datengeheimnis und die Einhaltung der Verschwiegenheitsvorschriften zu verpflichten.Die Tatsache der Verpflichtung sollte zum Zweck eines jederzeitigen Nachweises in der Personalakte dokumentiert werden.

Entsprechende Unterlagen sind in der Personalakte hinterlegt.

- Textbaustein ist im Standardvertrag für alle Mitarbeiter hinterlegt.
- Mitarbeiter werden nochmals in Schulungen darauf hingewiesen.

3. Zutrittskontrolle

Sollvorgabe: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personen- bezogene Daten verarbeitet oder genutzt werden, zu verwehren (wobei der Begriff räumlich zu verstehen ist). Der Auftragnehmer hat zu diesem Zweck ein Zutrittskontrollsystem zu installieren.

Beschreibung der Zutrittskontrollsysteme im Büro (inklusive der physischen Schutzvorkehrungen):

- mechanische Schließanlage Haupteingang sowie Büroeingänge
- elektronische Alarmanlage und Entriegelung mit 24/7 Wachschutz
- Kameras

Beschreibung der Überwachungseinrichtungen:

- Alarmanlage mit Aufschaltung auf Wachschutz - Wachschutz Berger, Köln
- 3 x Ubiqity Cameras + externer Server

4. Zugangskontrolle

Sollvorgabe: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Zu diesem Zweck muss der Zugang zu den DV-Anlagen kontrolliert und protokolliert werden (z. B. Anmelden in System,

unerlaubtes Hochfahren und Eindringen in DV- System verhindern).

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Beschreibung der implementierten Authentifizierungsmechanismen (z.B. Passwort- komplexität, Wechselzyklen, SSH Keys):

- SSH: Public Private Keys
- Wartungsarbeiten: OpenVPN (Zertifikate) S2S Kommunikation: IPSec
- C2S Kommunikation: TLS 1.2

Beschreibung der Maßnahmen bei temporärer Inaktivität der Nutzer (z.B. Mitarbeiter verlässt den Arbeitsplatz):

- Beim MacOS X System sind Hot Corners konfiguriert, sodass die Maus in eine Ecke geschoben wird, um den Bildschirm schnell zu sperren. Andernfalls sperrt sich der Monitor nach 30 Sekunden.
- Alle MA werden aufgerufen, Bildschirme immer zu sperren.

Beschreibung der technischen Schutzmaßnahmen für Ihre Netzwerkumgebung:

- iptables-Regeln auf externen Schnittstellen
- Dienste lauschen nur auf internen Karten
- IPSec-Kommunikation für Server
- wöchentliche nmap-, nikto-Scans
- monatliche OpenVAS-Scans
- tägliches Monitoring mit Grafana
- tägliches Audit neuer kritischer Fehler
- Anti-DDoS im Rechenzentrum
- OpenVPN-Tunnel zu internen Diensten

5. Zugriffskontrolle

Sollvorgabe: Es ist zu gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der

Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Personenbezogene Daten müssen bei persistenter Speicherung verschlüsselt werden.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Beschreibung der Verhinderung unerlaubter Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen (Rollen und Berechtigungen nach dem Need-to-Know Prinzip):

- Rechte und Rollenmanagement

Beschreibeung der Maßnahmen gegen unzulässige Zugriffe (z. B. Brute Force, SQL Injection, Login Validierung):

- SSH: fail2ban
- Prüfungen im Backend mit nativen django Sicherheitsvorkehrungen

Beschreibung der Sicherstellung, dass ausschließlich personifizierte Benutzerkonten für den Zugriff auf die Systeme genutzt werden (ein Konto je Benutzer):

- 1 Konto je Nutzer.
- 1 VPN Account je Nutzer
- 1 Konto auf einem Computer

Beschreibung der implementierten Verschlüsselungsmaßnahmen der personenbezogenen Daten:

- Festplattenverschlüsselung mit LUKS Default Settings
- Transportverschlüsselung mit TLS 1.2
- IPSec
- OpenVPN
- SSH-Sicherungen: GPG

5.1. Weitergabekontrolle

Sollvorgabe: Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Personenbezogene Daten sind nur verschlüsselt zu übertragen (Transportverschlüsselung).

Beschreibung der Transportverschlüsselung:

- Transportverschlüsselung mit TLS 1.2
- IPSec
- OpenVPN
- SSH

Beschreibung der Protokollierung der Weitergabe von personenbezogenen Daten:

- Nicht anwendbar. Personenbezogene Daten werden nicht von Servern heruntergeladen oder weitergegeben. Ausnahme Sicherungen. Sicherungen werden protokolliert. Täglich manuell geprüft.

Beschreibung der Transportsicherung bei einem physikalischen Transport:

- Nicht anwendbar. Personenbezogene Daten werden nicht von Servern physikalisch transportiert.

5.2. Eingabekontrolle

Sollvorgabe: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Ein detailliertes Loggingsystem über die Eingabe, Veränderung oder Löschung von personenbezogenen Daten (z. B. Logdateien) ist zu implementieren und regelmäßig auszuwerten.

Beschreibung der Logging / Monitoringsystem zur Überwachung der Zugriffe:

- Dem Kunden steht ein Auditlog zur Verfügung. Das Auditlog ist ein Protokoll, in dem alle Änderungen am Account des Kunden verzeichnet sind. Diese Daten sind personenbezogenen und können nur vom Kunden in Ausnahmefällen und mit einer Erlaubnis durch die Mitarbeiter des AN eingesehen und kontrolliert werden.
- Auf der Ebene von Servern werden diverse Protokolle mitgeschrieben, die durch das Anmelden von Mitarbeitern bei Wartungsarbeiten erstellt werden. Diese Protokolle werden stichprobenartig kontrolliert.
- Weiterhin werden diverse Protokolle generiert, die den technischen Zustand des Systems darstellen.

5.3. Verfügbarkeitskontrolle

Sollvorgabe: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Datensicherungskonzepts (z. B. Back-Up Verfahren, Redundanzen, USV, Notfallpläne):

- 3 Datacenter (System 3-fach vorhanden)
- 2 verschiedene Standorte/Rechenzentren
- USVs und Dieselgeneratoren
- gespiegelte Festplatten
- Enterprise-Festplatten
- Autofailover für Webnodes
- Autofailover für Statiskdaten
- Automatisiertes Monitoring
- tägliche Backups aller Daten
- Backups an 2 verschiedenen Orten
- mehrere Mitarbeiter, die Prozess beherrschen

5.4. Trennungsgebot

Sollvorgaben: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Der Auftragnehmer sorgt für eine nachweislich logische Trennung der Daten des Man- danten, d. h. Daten verschiedener Auftraggeber sind getrennt zu verarbeiten. Gegenseitiger Zugriff ist auszuschließen. Ebenso werden die Daten nur zweckgebunden verarbeitet.

Beschreibung der Umsetzung zur Mandantenfähigkeit:

- Daten werden zweckgebunden verarbeitet Daten werden auf Datenbankebene logisch nach Mandanten getrennt (Mandantenfähigkeit).

Beschreibung der Sicherstellung der Trennung von Entwicklung-, Test- und Produktivsystemen:

Physikalische Trennung (verschiedene Server) in 3 Umgebungen:

- Development
- Staging
- Produktion

5.5. Informationssicherheit

Beschreibung des Informationssicherheitsmanagementsystems (ISMS):

Diverse Prozesse:

- IT-Sicherheitsprozess
  - Input: Scans, Meldungen, Protokolle
  - Verarbeitung: Bewertung
  - Output: Maßnahmen
  - Tools: nmap, nikto, rkhunter, maldet, OpenVAS
- Verantwortung:
  - IT-Security: security@userlike.com
  - Datenschutz: privacy@userlike.com
- Regelmäßige Schulungen
  - IT Security
  - Datenschutz

    - Feste Prozesse
    - Onboarding
    - Offboarding

- Rechte und Rollenmanagement

5.6. Sonstiges

Beschreibung der Sicherstellung der vertraulichen Aufbewahrung sowie der Löschung oder Vernichtung von Test- und Ausschussmaterialen mit personenbezogenen Daten (z. B. Papier):

- Nicht anwendbar. Da keine Nutzung von Papier. Ausnahme Buchhaltung, sowie Verträge. Dokumente werden geschreddert.

6. Einsatz von Unterauftragnehmern

Die von den von uns eingesetzten weiteren Auftragsverarbeiter jeweils zum Zeitpunkt des Abschlusses dieser Vereinbarung implementierten technischen und organisatorischen Maßnahmen sind diesem Dokument als Anlage beigefügt. Wir versichern uns in regelmäßigen Abständen von der Angemessenheit und Wirksamkeit der von unseren Unterauftragnehmern getroffenen Maßnahmen.

7. Versicherung des Auftragnehmers

Der Auftragnehmer garantiert, dass alle in diesem Dokument genannten Angaben der Wahrheit entsprechen.

Anlage:

TOM der Hetzner Online GmbH
TOM der Amazon Web Services SARL

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO:
Technische und organisatorische
Maßnahmen nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

- Zutrittskontrolle
  - Datacenterparks in Nürnberg und Falkenstein
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenterpark
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
  - Verwaltung
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Videoüberwachung an den Ein- und Ausgängen
- Zugangskontrolle
  - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
    - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
    - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.
  - bei Hauptauftrag "Managed Server", "Webhosting", "StorageBox"
    - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert
- Zugriffskontrolle
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
    - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
        - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
    - bei Hauptauftrag "Managed Server", "Webhosting", "StorageBox"
        - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
        - Für übertragene Daten/Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.
- Datenträgerkontrolle
    - Datacenterparks in Nürnberg und Falkenstein
        - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
        - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).
- Trennungskontrolle
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
        - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
    - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
        - Die Trennungskontrolle obliegt dem Auftraggeber.
    - bei Hauptauftrag "Managed Server", "Webhosting", "StorageBox"
        - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
        - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- Pseudonymisierung
    - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
    - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
    - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
- Eingabekontrolle
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.
  - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
    - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
  - bei Hauptauftrag "Managed Server", "Webhosting", "StorageBox"
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
    - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
    - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
    - Monitoring aller relevanten Server.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Dauerhaft aktiver DDoS-Schutz.
  - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
    - Datensicherung obliegt dem Auftraggeber.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Dauerhaft aktiver DDoS-Schutz.
  - bei Hauptauftrag "Managed Server", "Webhosting", "StorageBox"
    - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
    - Einsatz von Festplattenspiegelung.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Einsatz von Softwarefirewall und Portreglementierungen.
    - Dauerhaft aktiver DDoS-Schutz.
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
  - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

- Auftragskontrolle
  - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
  - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
  - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

Annex 1

AWS Security Standards

1. **Information Security Program.** AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

   1.1 **Network Security.** The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

   1.2 **Physical Security**

      1.2.1 **Physical Access Controls.** Physical components of the AWS Network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

      1.2.2 **Limited Employee and Contractor Access.** AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

      1.2.3 **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. **Continued Evaluation**. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

[Remainder of Page Intentionally Left Blank]