Data Processing Agreement

The Customer as defined in the Master Service Agreement in the role of the Controller – hereinafter referred to as the Customer – and keylight GmbH, Fasanenstr. 77, 10623 Berlin, Germany in the role of the Processor – hereinafter referred to as the Supplier – – each a 'party'; together 'the parties' – HAVE AGREED on the following Data Processing Agreement (the "DPA") in order to fulfil their obligation according to Art. 28 (3) GDPR.

Preamble

The Parties have concluded a Master Service Agreement under which the Supplier performs services for the Customer. For the performance of the services, it is necessary that the Supplier processes personal data for and on behalf of the Customer. The purpose of this agreement is to stipulate the obligations of the parties in connection with any processing of personal data by Supplier as data processor on behalf of Customer as data controller.

1 Application of the Standard Contractual Clauses

1.1 Where the Customer resides in the EU, the Parties conclude the Standard Contractual Clauses between controllers and processors as agreed upon by the European Commission in its Commission Implementing Decision (EU) 2021/915 of June 4 2021 and attached to this DPA as APPENDIX 1 (the "EU-Standard Contractual Clauses").

1.2 The Parties agree upon including Clause 5 of the Standard Contractual Clauses and use OPTION 2 of Clause 7.7 regarding the general authorization of sub processors, whereas the time period in Clause 7.7 shall be 2 weeks. Regarding any other OPTIONS to choose from in the Clauses of the Standard Contractual Clauses, the Parties in each case agree upon OPTION 1.

1.3 Where the Customer resides outside of the EU, the Parties conclude the Module 4 of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as agreed upon by the European Commission in its Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and attached to this DPA as APPENDIX 2 (the "International Standard Contractual Clauses"). ANNEX 1 and 2 of APPENDIX 1 apply accordingly, whereas Data exporter shall be the Supplier and Data importer the Customer.

1.4 The EU-Standard Contractual Clauses and International Standard Contractual Clauses will be supplemented by the provisions of this DPA.

1.5 If any clause from this DPA or the Master Service Agreement or any other related agreement between the Parties directly or indirectly contradicts the EU-Standard Contractual Clauses or International Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

2 Instructions of the Customer

2.1 The Customer's initial instructions shall be set out by the provisions of the Master Service Agreement, its Annexes and Appendices and any related agreement.

2.2 The Customer shall be entitled to modify, amend or replace such individual instructions by issuing new instructions to the point of contact designated by the Supplier. The instruction shall be given either in written form (email to suffice). In case of an oral instruction, the Customer shall immediately confirm this instruction in written form (email to suffice).

2.3 Instructions not foreseen in or covered by the Agreement shall be treated as requests for change in performance. The Customer shall immediately confirm in writing or in text form any instruction issued orally.

3 International Transfers

3.1 The Supplier shall ensure that access of Customer production data for remote support and technical operations outside the EU is granted only at the Customer's request and with prior notification to the Customer.

3.2 The Supplier ensures that the keylight service is deployed and hosted in the EU with the exception of the sub processor's that reside outside the EU and are named in Annex IV. On the Customer's specific request Supplier shall perform the hosting outside of the EU.

4 Technical and Organisational Measures

In Cases where the EU-Standard Contractual Clauses apply, the Supplier has the right to amend or modify the technical and organisational measures that are set out in the DPA and its APPENDICES and ANNEXES at any time, provided, however, that the level of security shall not fall below the level initially agreed upon.

5 Obligations of the Customer

5.1 The Customer shall notify the Supplier without undue delay of any defect or irregularity of the services with regard to the processing of personal data detected by the Customer.

5.2 The Customer shall notify the Supplier's point of contract for any issue related to data protection arising out of or in connection with the Agreement.

6 Inspections

6.1 In cases where the EU-Standard Contractual Clauses apply, the Customer shall give the Supplier reasonable notice before conducting an audit according to Clause 7.6 of the EU-Standard Contractual Clauses unless such notice is impossible to provide or would defeat the purpose of the audit.

6.2 In cases where the EU-Standard Contractual Clauses apply, Supplier shall be entitled to request a remuneration for Supplier's support in conducting audits in accordance with the respective SOW or Order Form for support and consulting services..

7 Remuneration for Supporting Obligations

In cases where the EU-Standard Contractual Clauses apply and Insofar as Supplier may claim compensation to the Customer for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

on behalf of the Customer	on behalf of the Supplier
.....	.....
Name	Name
.....	.....
Title	Title
.....	.....
Date	Date
.....	.....
Signature	Signature

APPENDIX 1

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with [choose relevant option: OPTION 1: Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data] / [OPTION 2: Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data].

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional

safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss,

alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) OPTION 1: PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secrets or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in [OPTION 1] Article 32 Regulation (EU) 2016/679/ [OPTION 2] Articles 33, 36 to 38 Regulation (EU) 2018/1725.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to [OPTION 1] Article 33(3) Regulation (EU) 2016/679/ [OPTION 2] Article 34(3) Regulation (EU) 2018/1725, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to [OPTION 1] Article 34 Regulation (EU) 2016/679 / [OPTION 2] Article 35 Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under [OPTION 1] Articles 33 and 34 of Regulation (EU) 2016/679 / [OPTION 2] Articles 34 and 35 of Regulation (EU) 2018/1725.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

The Customer as defined in the DPA Master Service Agreement.

Processor(s): [*Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]*

1. Name: keylight GmbH,

Address: Fasanenstr. 77, 10623 Berlin, Germany

Telephone: +49 30 814 760 14

Email: sales@keylight.com

2. Data Protection Officer of Processor:

Name: Mr. Andrew Aitken,

Address: The DPO resides at the premises of the keylight GmbH,

Telephone: +49 30 814 760 14

Email: privacy@keylight.com

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

Employees, end customers and partners of Customer

Categories of personal data processed

First name, last name, address, telephone number, email address, order and booking data, encrypted password.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The processing of sensitive data is not part of the services rendered by the Supplier.

Nature of the processing

Supplier provides SaaS to Customer and the nature of the processing of personal data includes any processing that is required for Supplier to render these services to Customer. It specifically includes the collection, organisation, structuring, storage and making available of personal data but may also include any other operation such as the adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction of personal data

Purpose(s) for which the personal data is processed on behalf of the controller

Supplier processes personal data to render its services as defined in the provisions of the Master Service Agreement. This includes specifically the creation and management of subscriptions and accounts, provision of information about existing subscriptions and their billing

Duration of the processing

The processing endures as long as Supplier renders its services to Customer and ends with the termination of the Master Subscription Agreement.

Subject matter, nature and duration of the processing with regard to sub processors:

Please see below in ANNEX IV

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures need to be described concretely and not in a generic manner.

Technical and organisational measures

pursuant to Art. 32 General Data Protection Regulation ('GDPR')

1 Physical Access Control

The following measures are implemented to protect against unauthorised physical access to premises, buildings or rooms where data processing systems are located which process and/or use Personal Data:

a) Physical components of the data centre facilities, servers, networking equipment, and host software are housed in nondescript facilities.

b) Physical barrier controls are used to prevent unauthorised entrance to these facilities both at the perimeter (e.g., fencing, walls) and at building access points.

c) Physical access points to server locations are managed by electronic access control devices and are secured with intrusion detection devices that sound alarms if the door is forced open or held open.

d) Establishing access authorizations for employees and third parties, including the respective documentation.

e) All visitors are required to present identification and are signed in.

f) Use of video cameras (CCTV) to monitor individual physical access to data centre facilities.

g) Data centres utilise security guards 24x7, who are stationed in and around the building.

2 System Access Control

The following measures are implemented to protect against the unauthorised access to and use of data processing systems used to provide the digital services:

a) User and administrator access to the data centre facilities, servers, networking equipment, and host software is based on a role based access rights model. A unique ID is assigned to ensure proper user-authentication management for users and administrators on all system components.

b) The concept of least privilege is employed, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.

c) IT access privileges are reviewed on a regular basis by appropriate personnel.

d) Access to systems is revoked within a reasonable timeframe of the employee record being terminated (deactivated).

e) *First time passwords/passphrases are set to a unique value and changed immediately after first use.*
f) *User passwords/passphrases are changed periodically and only allow complex passwords.*
g) *Time stamped logging of security relevant actions is in place.*
h) *Automatic time-out of user terminal if left idle, with user identification and password required to reopen.*
i) *Assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection.*
j) *Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.*
k) *Firewall policies (configuration files) are pushed to firewall devices on a regular basis.*

3 Data Access Control

The following measures are implemented to control that persons entitled to use data processing systems gain access only to the Personal Data when they have a right to access, and Personal Data is not read, copied, modified or removed without authorization in the course of processing, use and stor-age.

a) *User and administrator access to the data centre facilities, servers, networking equipment, and host software is based on a role based access rights model. A unique ID is assigned to ensure proper user-authentication management for users and administrators on all system compo-nents.*
b) *The concept of least privilege is employed, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.*
c) *IT access privileges are reviewed on a regular basis by appropriate personnel.*
d) *Time stamped logging of access to and modification of Personal Data is in place.*
e) *An incident response plan is in place to address the following at time of incident:*
    - *Roles, responsibilities, and communication and contact strategies in the event of a compro-mise.*
    - *Specific incident response procedures.*
    - *Coverage and responses of all critical system components*

4 Data Transmission Control

The following measures are implemented to control that Personal Data is not read, copied, modified or removed without authorization during transfer:

a) *Prevention of unauthorised copying: The measures taken to prevent unauthorised copying of the physical storage infrastructure as such (e.g. copying your data by transferring them to an external storage medium as a hard drive) are included in the measures described above.*
b) *Use of role based access rights model: described above.*
c) *Firewall policies: described above*
d) *Implement an incident response plan: described above.*

e) *Storage Device Decommissioning: When a storage device has reached the end of its useful life, procedures implemented include a decommissioning process that is designed to prevent customer data from being exposed to unauthorised individuals. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices and applicable data protection law.*

f) *Secure Access Points: there are only a limited number of secure access points to the cloud, which allow you to establish a secure communication session with your storage or compute instances within the Services.*

g) *Connections to the network by personnel: personnel connect to the network using secure authentication that restricts access to network devices and other cloud components.*

5 Data Input Control

The following measures are implemented to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from data processing systems used to provide the digital services:

Logging User Activity: developers and administrators who need access to our systems in order to maintain them must explicitly request access. Approved personnel connect to the network using secure authentication that restricts access to network devices and other cloud components, logging all relevant activity for security review.

6 Order Control

The following measures are implemented in order to ensure that Personal Data which are processed on your behalf can only be processed in compliance with your instructions:

a) *Internal communication: various methods of internal communication are implemented at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees and regular management meetings for updates on business performance and other matters.*

b) *Corporate Segregation: Logically, the production network is segregated from the corporate network by means of a complex set of network security / segregation devices. Developers and administrators on the corporate network who need to access in order to maintain them must explicitly request access. Approved personnel then connect to the network through secure means.*

c) *Robust Compliance Program: The IT infrastructure is designed and managed in alignment with security best practices and certain IT security standards, such as ISO 27001.*

d) *Policies and Security Awareness Training: We and our Subprocessors maintain and provide periodic security awareness training to all information system users. Policies and procedures have been established based upon data security and data protection requirements.*

7 Availability Control

The following measures are implemented to protect Personal Data against accidental or unauthorised destruction or loss.

a) Fire Detection and Suppression: Automatic fire detection and suppression equipment has been installed with our data centres. The fire detection system utilises smoke detection sensors in all data centre environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms.

b) Redundant Power Systems: The data centre electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centres use generators to provide back-up power for the entire facility.

c) Climate and Temperature Control: Personnel and systems monitor and control temperature and humidity at appropriate levels at data centres.

d) Preventative maintenance: Preventative maintenance is performed to maintain the continued operability of the data centre equipment.

8 Data Separation Control

The following measures are implemented to control that Personal Data collected for different purposes can be processed separately:

Multi-tenant environment: The Platform is a virtualized, multi-tenant environment. Security management processes and security controls designed to isolate each customer from other customers are implemented. Systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. Corporate Segregation: described above.

9 Technical and organisational measures of sub processors

Supplier uses sub processors for rendering its services (see Annex IV). All sub processors implement appropriate technical and organisational measures. Please find more information under:

Amazon Web Services: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Twilio (Sendgrid): https://www.twilio.com/legal/security-overview

Zendesk: https://www.zendesk.co.uk/trust-center/

ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Subprocessor	Address	Location	Subject matter	Nature and duration

Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxembourg	EU US APAC (Customers may select a data region)	Hosting the backend and the API	The nature of the processing can include especially the collection, organisation, structuring, storage and making available of personal data but may also include any other operation such as the adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction of personal data. The processing endures as long as Supplier renders its services to Customer and ends with the termination of the Master Subscription Agreement.
Twilio Inc.	101 Spear Street, 1st Floor, San Francisco, CA, 94105, USA	US	Transactional emailing (Sendgrid)	See above.
Zendesk, Inc.	1019 Market Street, San Francisco, CA 94103 USA	EU	Third-party service provider of customer support tools	See above. does not have access to Customer Data stored or processed by the Services. only has access to Customer Data if Customer explicitly elects to share Customer Data in the course of a support case

APPENDIX 2

STANDARD CONTRACTUAL CLAUSES
MODULE FOUR: Transfer processor to controller

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  (v) Clause 13;
  (vi) Clause 15.1(c), (d) and (e);
  (vii) Clause 16(e);
  (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES
Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data[2], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 [not applicable]
Use of sub-processors

Clause 10
Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13 [not applicable]
Supervision

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 [not applicable]

Clause 15 [not applicable]

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany (specify country).

Clause 18
Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Germany (specify country).

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

[2] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.