Data Protection Addendum

I. Introduction

Data Processing Addendum pursuant to Art. 28 GDPR between oculavis GmbH, Vaalser Str. 259, 52074 Aachen, Germany hereinafter referred to as "*contractor*" and the customer hereinafter also referred to as "*client*".

This Data Protection Addendum forms a part of the agreement between Customer and oculavis covering Customer's use of the Services ("Agreement") and applies automatically to customers who have active service agreements with us ("oculavis"). If there are any changes to this agreement, customers will be informed accordingly.

Definitions

- ***"Personal data"*** means any information relating to an identified or identifiable natural person ("data subject") such as a name, email or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- ***"Contractor"*** *means* the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In this case "oculavis".
- ***"Service Agreement"*** means customer or client agreement is a legal agreement between customer and oculavis GmbH to use our software and to provide related services.
- ***"Customer data"*** means any client content that is personal data that oculavis processes on behalf of Client in the course of providing the Services.
- ***"Services"*** means the software and services provided by oculavis GmbH, as applicable, that are used by the customer.
- ***"oculavis Privacy Policy"*** means the privacy policy for the services, the current version of which is available at https://oculavis.de/en/imprint/

II. Details of processing

1. **Nature and Purpose of the Processing**

oculavis will process personal data as necessary to provide the services under the service agreement.

The software platform oculavis SHARE serves the remote support of technicians or customers with data glasses, smartphones, and tablets. In addition, technical documentation such as instructions can be provided, and documentation can be created in a process-integrated

manner. Personal data is stored and processed on the platform for user identification, documentation, platform management and maintenance purposes.

The use of the oculavis SHARE software platform requires processing of personal data on the platform.

1.1. Legal basis for the processing of personal data (legal provisions, agreement or agreement initiation with the data subject, consent of the data subject, reconciliation of interests, etc.)

The following agreements are made between oculavis GmbH and the SHARE user for the use of the oculavis SHARE software:

- Service Agreement
- General terms and conditions of oculavis GmbH and oculavis SHARE https://oculavis.de/en/gtc/
- Data Processing Addendum

2. Type of Data, Categories of data subjects

The following data can be recorded in the oculavis SHARE software:

- Master data: First name, surname/last name, email, telephone number, company name, department, username
- Pictures
- Videos
- Documents (PDFs, pictures, videos, etc.)
- Online status
- Chat messages (participant, time, message)
- Time and participants of video calls: Metadata (Creation date, Start and end, participants)
- The data mentioned are partly linked together in the software and are entered/collected/generated by the users of the software platform themselves
- The following data is collected in the backend of the software platform:
  - Login data (times, frequency of logins)
  - History of chat messages, metadata of video calls

The performance of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. of the GDPR are fulfilled. The appropriate level of protection is established by binding internal data protection regulations (Art. 46 para. 2 lit. b in conjunction with 47 GDPR) and by standard data protection clauses (Art. 46 para. 2 suffered c and d GDPR).

3. Duration of Processing

The duration of this agreement corresponds to the duration of the service agreement(s). An automatic or semi-automatic deletion of personal data does not take place during the agreement period. At the end of the agreement, the client is given the opportunity to save data from his software platform SHARE. All personal data will be deleted and/or destroyed in a controlled manner at the end of the retention period (usually 90 days) or at the request of the client or after the termination of the agreement. When data is deleted, responsibilities for this agreement ends.

III. Rectification, limitation and erasure of data

(1) oculavis is not permitted to correct, delete or restrict the processing of data processed on behalf of the client without authorization but only in accordance with documented instructions from the client. As far as a concerned person directly contacts oculavis in this regard, the oculavis will immediately forward this request to the client.

(2) In so far as the scope of services includes a deletion concept, the right to delete the data, data correction, data portability and information in accordance with the documented instructions of the client shall be ensured by oculavis.

IV. Technical and Organisational Measures

The Contractor shall establish security in compliance with Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR and must be able to provide evidence that these requirements have been met. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. In doing so, the state of the art, the implementation costs and the type, scope and purpose of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR shall be taken into account.

The full text of oculavis's technical and organizational security measures (TOMs) to protect customer data *_available soon_. These measures are the basis of the service agreement. If the client's inspection/audit reveals a need for adjustment, this shall be implemented by mutual agreement.

The following table provides more information regarding the technical and organizational security measures set forth below.

Technical and Organizational Security Measures (TOMs)	**Evidence of Technical and Organizational Security Measures**
Measures of pseudonymization and encryption of data	The databases that store customer data are encrypted using AES-256 encryption. Backups are also encrypted (AES-256). Customer data is encrypted when in transit (DTLS 1.2, SRTP, HTTPS, TLS 1.2).
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Regular backups of customer data are done. Customer data that is backed up is retained (retention period is usually 90 days) and encrypted in transit and at rest using the advanced encryption standard. Operational resilience strategies and capability results are incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan. *_More information will be available soon._
Measures for ensuring the ability to restore the availability and access to	See above information *_More information will be available soon._

personal data in a timely manner in the event of a physical or technical incident	
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	oculavis maintains a security framework based on ISO 27001 Information security management system and effectiveness of TOMs is regularly tested and evaluated (at least annually)
Measures for user identification and authorisation	To minimize the risk of data exposure, oculavis follows the principles of least privilege through access-control model when provisioning system access. Authorizations and accesses are assigned and granted based on the need-to-know principle, taking into account the sensitivity and criticality of data processing, and the employee's responsibilities within the company. **More information will be available soon.*
Measures for the protection of data during transmission	The databases that store customer data are encrypted using AES-256 encryption. Backups are also encrypted (AES-256). Customer data is encrypted when in transit (DTLS 1.2, SRTP, HTTPS, TLS 1.2). **More information will be available soon.*
Measures for the protection of data during storage	Strict separation of test/development data/platforms and production data/platforms. Only the software's administrators group has access to the customer instances (production environment) and only for backup, update, or data recovery purposes**More information will be available soon.*
Measures for ensuring physical security of locations at which personal data are processed	**More information will be available soon on our website.*
Measures for ensuring events logging	Security-related events are identified and monitored within applications and the underlying infrastructure. A process is defined and implemented to communicate alerts to responsible stakeholders based on security events and their corresponding metrics. **More information will be available soon.*
Measures for internal IT and IT security governance and management	Annual review, assessment, and evaluation of the effectiveness of the technical and organizational measures is annually performed. Based on ISO 27001, all relevant standards, regulations, legal/contractual, and statutory requirements are identified and documented at oculavis**More information will be available soon.*

Measures for certification/assurance of processes and products	oculavis is ISO 27001 certified.
Measures for ensuring data minimisation	Data is collected only for business purposes. The type of data collected can be found in Section II. (Details of Processing). Face anonymization is also done on mobile apps for people not involved in the call.
Measures for ensuring data quality	The databases that store customer data are encrypted using AES-256 encryption. Backups are also encrypted (AES-256*). *More information will be available soon.*
Measures for ensuring limited data retention	oculavis stores personal data only for the operation of business operations. Customer data is accessed after getting consent of the customer and accessed with four eyes principle. A deletion concept has been implemented which guarantees retention periods for personal data. An automatic or semi-automatic deletion of personal data does not take place during the agreement period. At the end of the agreement, the customer is given the opportunity to save data from his SW platform SHARE. All personal data will be deleted and/or destroyed in a controlled manner at the end of the retention period (usually 90 days) or at the request of the customer. Log files are deleted after 30 days.
Measures for allowing data portability and ensuring erasure	At the end of the agreement, the customer is given the opportunity to save data from his SW platform SHARE. All personal data will be deleted and/or destroyed in a controlled manner at the end of the retention period (usually 90 days) or at the request of the customer. Data Privacy requests can be submitted via this email. *(email will be available soon).*

The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures, provided that such alternative measures maintain at least the level of security provided by the measures agreed in TOMs.

V. Subprocessors

Sub-processing relationships within the meaning of this provision are those services which relate directly to the provision of the main service. This does not include additional services which the contractor uses, e.g. as telecommunications services, postal/transport services, maintenance and user services or the disposal of data carriers. However, the contractor shall be obliged to take appropriate and legally compliant contractual agreements and control measures to guarantee the data protection and data security of the Client's data even in the case of sub-processors.

a) The contractor may only engage sub-processors (further contract processors) with the prior express written or documented consent authorization of the Client. The client agrees to the assignment of the sub-processors mentioned here *(*available soon)* (in accordance with Art. 28 para. 2-4 GDPR).
b) Notifications and changes of existing subprocessors are permitted, as far as:

- the contractor notifies the client of such outsourcing to sub-processors in writing or in text form a reasonable period in advance typically 14 days, and
- the client does not object to the planned outsourcing in writing or in text form to the contractor up to the time the data is transferred.

c) Data Subject Rights:
   (1) a contractual agreement in accordance with Art. 28 para. 2-4 GDPR is applied. The contractor controls that the data protection obligations specified in this agreement are also enforced on the sub-processor for the relationship between client and the contractor, including a right of client to monitor and inspect the sub processor(s) on its own or by independent auditors; the contractor will provide to client upon written request information on the essential content of the contract with the sub-processor as well as information on the implementation of the data protection obligations within the sub processing relationship. The passing on of personal data of the client to the sub-processor are only permitted when all requirements for subcontracting have been met.
   (2) If the sub-processors render the agreed service outside the EU/EEA, the contractor shall ensure that it is permissible under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be used.
   (3) Any further outsourcing by the sub-processor shall require the express consent of the client (at least in text form).
   (4) All contractual regulations in the agreement chain must also be imposed on the further on the sub-processors.
   (5) Client and the contractor, including a right of client to monitor and inspect the subprocessor(s) on its own or by independent auditors; the contractor will provide to client upon written request information on the essential content of the agreement with the sub-processor as well as information on the implementation of the data protection obligations within the subprocessing relationship.

VI. Quality Assurance and other obligations of the contractor

In addition to compliance with the provisions of this agreement, the contractor shall have statutory obligations pursuant to Art. 28 to 33 GDPR; to this extent, the contractor shall in particular ensure compliance with the following requirements:

a) Written appointment of a data protection officer who carries out his duties in accordance with Art. 38 and 39 GDPR. You can find the contact details of appointed Data Protection Officer here: https://oculavis.de/en/imprint/. The contractor shall inform the Client about any related changes without delay. The changes do not affect the current agreement with the client.
b) **Confidentiality of processing:** The maintenance of confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. When performing the work, the contractor only uses employees who are obliged to maintain confidentiality and who have been familiarised beforehand with the data protection provisions relevant to them. The contractor and any person subordinate to the contractor who has access to personal data may only process these data in accordance with the instructions of the client, including

the authorizations granted in this agreement. The duty of confidentiality shall continue to apply even after the agreement has ended. The contractor shall regularly train its employees in data protection and adequately inform them about their obligations under this agreement.

c) The implementation of and compliance with all technical and organisational measures required for this agreement pursuant to Art. 28 para. 3 sentence 2 lit. c, 32 GDPR [details in Annex 1].
d) The client and the contractor will cooperate, on request, with the supervisory authority in the performance of their tasks.
e) Informing the client without delay of control measures and measures taken by the supervisory authority in so far as they relate to this Agreement. This shall also apply where a competent authority, in the course of administrative or criminal proceedings, investigates the processing of personal data during the processing of the agreement by the contractor.
f) If the client is itself subject to control by the supervisory authority, administrative or criminal proceedings, the liability of a person concerned or a third party or any other claim in connection with the processing of the agreement with the contractor, the contractor shall support it to the best of its ability.
g) The contractor must regularly monitor internal processes and technical and organisational measures in order to ensure that processing within his sphere of responsibility is carried out in accordance with the requirements of the applicable data protection legislation and that the rights of the data subject are protected.
h) The contractor will execute regular reviews in relation to the performance of his / her contractual obligations under this agreement, in particular compliance and any necessary amendment to provisions and measures laid down to carry out the commission.

The contractor shall ensure that the technical and organisational measures taken can be proven to the client within the scope of its control powers pursuant to Clause 7 of this agreement.

VII. Control rights of the Client

(1) Upon mutual agreement with the contractor, the client has the right to conduct audits either personally or through appointed auditors or inspectors as necessary. Client has the right to convince himself of the observance of this agreement by the contractor in his business operations by means of spot checks, which must be notified in good time. Contractor shall grant access to client or third party auditors of the client for inspections at the Supplier's premises.
(2) The contractor shall ensure that the client can confirm compliance with the obligations outlined under Art. 28 GDPR. The contractor agrees to provide necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures to the client. The contractor shall support inspections by client or third party auditors, in particular with competent contact persons and by providing relevant information and evidence upon client's request.
(3) Evidence of measures which do not only relate to this specific Agreement, can be provided by compliance with approved rules of conduct in accordance with Art. 40 GDPR or current attestations, up-to-date attestations, certificates, reports or extracts thereof from independent bodies (e.g. auditors, auditors, data protection officer, IT security department,

data protection auditors, quality auditors). Client's right to carry out inspections remains unaffected.

(4) The contractor may claim remuneration to facilitate the client's inspection activities.

VIII. Notification of infringements by the Contractor

1. The agreement or shall support the client in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. These include:

   a) Ensuring an adequate level of protection through technical and organisational measures which take into account the nature and purposes of the processing and the predicted likelihood and severity of a potential breach of rights through security breaches, and which allow the immediate identification of relevant breaches.
   b) The obligation to immediately report infringements of personal data to the client, without undue delay, within 24 hours.
   c) the obligation to assist the client to inform the data subject and to make all relevant information available to the data subject without undue delay in this connection.
   d) assisting the client with its data protection impact assessment.
   e) Supporting the client within the framework of prior consultations with the supervisory authority.
   f) Informing the client, without undue delay, about any inspections, control activities or measures carried out by the relevant data protection authorities in relation to personal data processed on behalf of the client.

2. For support services which are not included in the service description or are not due to a misconduct of the contractor, the contractor can claim a remuneration.

IX. Authority of the Client to issue instructions

(1) The contractor shall process the data provided by client or third parties acting on behalf of client solely for client and only within the scope of this agreement and in accordance with the documented instructions from client. Any other use of such data, in particular for purposes of the contractor's own business operations or the purposes of third parties, is prohibited.

(2) Oral instructions as set forth in the agreement, in this DPA, or as directed by the client or client's end users through the services shall be confirmed by the client without delay (at least in text form).

(3) The contractor shall inform the client immediately if an instruction violates data protection regulations. The contractor shall be entitled to suspend the execution of the corresponding instruction until it has been confirmed or amended by the client.

X. Deletion and return of personal data

(1) No copies or duplicates of data processed on behalf of client may be produced or disclosed to third parties without client's prior written consent. This does not apply to backup copies as these are required to ensure appropriate security of data processing.

(2) Upon completion/termination of the service agreement or earlier upon request by the client - the contractor shall hand over all documents, processing and usage results as well as databases which have come into his possession and which are connected with the contractual relationship, or delete them in accordance with data protection laws after prior consent. The same applies to test and scrap material. The deletion protocol must be submitted upon request.

(3) Documentation evidence that data has been processed properly and in accordance with this agreement shall be retained by the contractor beyond the end of this agreement in accordance with relevant data retention periods. The contractor may handover such documentation to client after this agreement is terminated.