Data Processing Agreement pursuant to Art. 28 GDPR

between the customer

- hereinafter referred to as **Customer** -

and

alfaview gmbh, Kriegsstraße 100, 76133 Karlsruhe
(alfaview® Video Conferencing Systems)

- hereinafter referred to as **Contractor** -

Preamble

The Contractor provides the Customer with the alfaview® application and in this context provides services based on an Agreement concluded between the parties consisting of the order form and the Terms and Conditions (hereinafter referred to as "**Main Agreement**"). As part of this service provision, it is necessary, or at least it cannot be excluded, that the Contractor will handle personal data for which the Customer acts as the responsible body within the meaning of the data protection provisions (hereinafter referred to as "**Order Data**"). This Agreement specifies the data protection rights and obligations of the contracting parties in connection with the Contractor's handling of Oder Data for the performance of the Main Agreement.

Clause 1 Scope, subject-matter and duration of the processing

(1) This Data Processing Agreement applies to all activities that are related to the Main Agreement and where employees of the Contractor or third parties commissioned by the Contractor may treat personal Order Data within the scope of this commissioned processing. The Data Processing Agreement does not apply if the Customer uses the alfaview® application as a natural person in the course of a purely personal or household activity.

(2) In providing the alfaview® application and the services defined in the Main Agreement, the Contractor processes personal data on behalf of the Customer; details hereto are listed in the Main Agreement (subject-matter of the processing). Personal data for the purpose of providing the alfaview® application and the services as defined in the Main Agreement is processed, as well as data that users enter and/or collect in the online meetings while using alfaview® (scope, nature and purpose of the processing).

(3) Duration of processing: The duration of the processing is determined by the term of the Main Agreement.

(4) The following data types and categories are subject to the processing of personal data:

- Personal data necessary to provide the alfaview® application and to establish communication (user profile): access data of registered users, such as name and e-mail address; users can also provide further information in their user profiles, such as title, initials, location. In case of invitations via guest links, only the guest user's name or pseudonym is required or, in case of so-called individualised guest links, the guest user's name and e-mail address.

- Personal data collected and processed by the users during the communication in online meetings using the alfaview® application: text messages (chats), video and audio data

containing images and voices of the users; this video and audio data as well as text messages in chats may contain other personal master data, communication data and other personal data exchanged by users of alfaview® in the context of communication. Audio, video and chat messages are in principle not stored or only temporarily stored until the end of communication, unless the Customer manually creates a recording.

(5) The categories of data subjects affected by the processing include the Customer (if the application is used by individuals), the Customer's employees or other authorised users on the part of the Customer (e.g. freelancers, lecturers, contract teachers) and the communication partners of authorised users as well as the persons communicated about.

(6) The contractually agreed data processing shall take place exclusively within a Member State of the European Union, or in another state that is party to the Agreement on the European Economic Area.

Clause 2 Responsibility for data processing

(1) Within the framework of this Agreement, the Customer is solely responsible for the legality of the processing of Oder Data and for the protection of the rights of the data subjects in line with Art. 12 to 22 GDPR ("Controller" within the meaning of Art. 4 [7] GDPR). The Contractor shall process personal data on behalf of the Customer only on the Customer's instruction.

Clause 3 Technical and organisational measures

(1) The Contractor is obliged to comply with the legal data protection provisions and to not disclose or expose Order Data to unauthorised third parties. Documents and data must be secured against unauthorised access, taking into account the state of the art.

(2) Within their area of responsibility, the Contractor shall design the internal organisation in such a way that it meets the special requirements for data protection. He shall take all technical and organisational measures necessary for appropriate protection of the Oder Data in accordance with Art. 32 GDPR, in particular at least the measures indicated in Annex 1.

(3) The technical and organisational measures are subject to technical progress and development. In this respect, the Contractor is permitted to implement alternative adequate measures, ensuring that the security level of the specified measures is not undercut.

Clause 4 Obligations of the Contractor

(1) The Contractor shall process Order Data only as instructed by the Customer and in compliance with Clause 6 of this Agreement. The Contractor shall correct or delete Order Data or restrict the processing of this data exclusively in accordance with the Customer's instructions. If a data subject contacts the Contractor directly for the purpose of correcting or deleting their data or requesting information about the stored data of the Customer, the Contractor will forward this request to the Customer without undue delay.

(2) The Contractor shall ensure and regularly verify that the processing and use of data in their area of responsibility, which includes Subcontractors according to Clause 9 of this Agreement, is carried out in accordance with the provisions of this Agreement.

(3) Without prior consent from the Customer, the Contractor may not make copies or duplicates of the Order Data. However, this does not apply to copies, as far as they are necessary to ensure proper

data processing and proper performance of the services in accordance with the Main Agreement (including backups).

(4) The Contractor shall support the Customer regarding inspections by the supervisory authority within the scope of what is reasonable and necessary, insofar as these inspections relate to data processing by the Contractor. The Contractor may request reimbursement for the demonstrable expenses and costs incurred by these support services (pure reimbursement of expenses), unless the inspection is connected with a violation of data protection provisions or stipulations in this Agreement for which the Contractor is responsible.

(5) The Contractor shall disclose to the Customer the contact details of the company data protection officer and the contact person for data protection issues arising under the Agreement.

(6) The Contractor shall oblige the persons employed in the processing of the Customer's data to confidentiality in accordance with Art. 28 [3] [2] [b], 29, 32 [4] GDPR and secrecy in accordance with Section 203 of the German Criminal Code (StGB).

(7) The Contractor shall notify the Customer without undue delay of any disturbances and infringements of data protection provisions or the stipulations made in the order as well as of any suspected data protections violations or irregularities in the processing of personal data by the Contractor, by the Contractor's employees or a subcontractor employed in accordance with Clause 9. This shall apply in particular with regard to any notification obligations of the Customer pursuant to Art. 33 and Art. 34 GDPR. The Contractor ensures that, if necessary, they will provide the Customer with appropriate support in meeting their obligations under Art. 33 and 34 GDPR (Art. 28 [3] [2] [f] GDPR). The Contractor may only give notification for the Customer in accordance with Art. 33 or 34 GDPR upon prior instructions from the Customer.

Clause 5 Obligations of the Customer

(1) The Customer is solely responsible for the assessment of admissibility of the commissioned data processing as well as for the protection of the rights of the data subjects concerned.

(2) The Customer shall inform the Contractor immediately and in full if they find errors or irregularities regarding data protection provisions while examining the order results.

(3) The Customer is responsible for the notification obligations resulting from Art. 33 and Art. 34 GDPR.

Clause 6 Customer authority to issue instructions

(1) The Contractor processes the Customer's data exclusively in accordance with the Customer's instructions as particularly expressed in the provisions of this Agreement and the stipulations of the Main Agreement, unless he is obliged by the law of the Union or the Member States to which the Contractor is subject; in this case, the Contractor notifies the Customer of these legal requirements, unless the law concerned prohibits such notification on the grounds of an important public interest. The Customer may modify, amend or replace individual instructions in writing or in text form. The Customer is entitled to issue instructions at all times. If individual instructions entail additional costs, particularly if these go beyond the contractually agreed scope of services, these shall be reimbursed to the Contractor. There is no obligation to pay remuneration if the instruction is necessary due to a violation of data protection provisions or stipulations in this contract for which the contractor is responsible.

(2) The Customer shall immediately confirm verbal instructions in writing or in text form (e.g. by e-mail).

(3) The Contractor shall inform the Customer immediately if, in their opinion, any instructions issued by the Customer violate legal provisions (Art. 28 [3] [3] GDPR). The Contractor is entitled to suspend the implementation of the corresponding instruction until it is confirmed or modified by the person responsible at the Customer.

Clause 7 Obligation of assistance

(1) If, by virtue of applicable data protection laws, the Customer is obliged vis-à-vis an individual to provide information or particulars on the processing of this person's data or to guarantee the rights of data subjects in accordance with Chapter III (Articles 12 to 23) of the GDPR, the Contractor shall assist the Customer in the fulfilment of these obligations with suitable technical and organisational measures in accordance with Art. 28 [3] [e] GDPR.

(2) The Contractor shall assist the Customer in complying with the obligations set out in Art. 32 to 36 GDPR in accordance with Art. 28 [3] [f] GDPR.

(3) The demonstrable costs incurred (pure reimbursement of expenses) for providing the assistance according to paragraphs 1 and 2, shall be reimbursed by the Customer, unless the assistance is connected with a violation of data protection provisions or stipulations in this Agreement for which the Contractor is responsible.

Clause 8 Inspection rights of the Customer

The Contractor agrees that the Customer - in principle by appointment, that may only be waived in exceptional cases - is entitled to audit compliance with the data protection and data security provisions and with the contractual Agreements to an appropriate and necessary extent, either himself or through third parties commissioned by the Customer, in particular by obtaining information and inspecting the stored data and the data processing programs as well as by on-site audits and inspections (Art. 28 [3] [2] [h] GDPR). The Contractor guarantees that he will assist in these audits if necessary. The costs for the performance of the inspection shall be borne by the Client, unless the inspection is connected with a violation of data protection provisions or stipulations in this Agreement for which the Contractor is responsible.

Clause 9 Other processors in accordance with Art. 28 [2] and [4] GDPR

(1) The Customer hereby grants general authorisation to use other processors (hereinafter referred to as "**Subcontractors**"). The Subcontractors involved at the time of the Agreement being concluded are listed in Annex 2; the Customer grants authorisation to use these Subcontractors upon signature of this Agreement. The Contractor shall inform the Customer in advance of any intended change with regards to the addition or replacement of Subcontractors, giving the Customer the opportunity to object to this change (Art. 28 [2] GDPR). If no objection is made within 14 days of the announcement, the consent to the change shall be deemed to have been given. If the Customer objects, the Contractor is entitled to terminate the Main Agreement and this Agreement with a notice period of 3 weeks.

(2) The Contractor is obliged to carefully select their Subcontractors according to their qualification and reliability. When using Subcontractors, the Contractor shall oblige them in accordance with the provisions of this Agreement and thereby ensure that the Customer is able to exercise its rights under this Agreement (in particular its audit and inspection rights) directly against the Subcontractors. In

particular, the Contractor shall oblige such subcontractors to maintain secrecy in accordance with Section 203 of the German Penal Code (StGB) to which private secrets of the Customer could be disclosed in accordance with Section 203 of the StGB.

Clause 10 Deletion of data and return of data carriers

Upon completion of the contractual work or earlier upon request by the Customer - at the latest on termination of the Main Agreement - the Contractor shall, upon the Customer's option hand over or destroy according to data protection requirements all obtained documents, generated results of processing and use as well as datasets associated with the contractual relationship. The deletion log must be presented upon request.

Clause 11 Liability

A liability provision between the contracting parties in the Main Agreement also applies to commissioned processing, unless the contracting parties have expressly agreed otherwise.

Clause 12 Final provisions

(1) Insofar as no special provisions are contained in this Agreement, the provisions of the Main Agreement apply. In case of contradictions between this Agreement and provisions from other contractual agreements, in particular from the Main Agreement, the provisions from this Agreement take precedence.

(2) Changes and additions to this Agreement and all of its components – Including any assurances given by the Contractor or changes to the annex – require a written Agreement and an express reference to the fact that it is a change or supplement to these terms. This also applies to the waiver of this form requirement.

(3) The rights and obligations of the contract shall remain in force as long as the contractor processes the customer's data.

(4) Exclusive place of jurisdiction for all disputes arising from this Agreement is the Contractor's registered office.

(5) German law applies.

Annex 1

Overview of the technical and organisational measures

I. Confidentiality (Art. 32 [1] [b] GDPR)

1. Equipment access control

Unauthorised persons are to be denied access to data processing facilities where personal data is processed and used.

- Use of magnetic or chip cards for authorised users
- Video surveillance
- Determination of persons with access authorisation
- Closed shop operation
- Capacity for revision regarding access authorisation
- Use of an access control system
- Key regulation and current key list
- Logging of entry and exit
- Reception/gatekeeper
- Office doors and windows locked during periods of absence

2. User control and data access control

The objective of user control is to prevent data processing systems from being used by unauthorised persons. Data access control must ensure that authorised users of a data processing system can access data exclusively referring to their access rights and that data cannot be read, copied, modified or removed unauthorised during processing, use and after storage.

- Identification and authentication of users/password protection
- Automated verification of authorisations
- Introduction of access-restrictive measures (e.g. read-only authorisation)
- Time limitation of access options
- User-related logging of (failed) access
- Use of encryption procedures
- Central registry of user rights

3. Separability

It must be ensured that data collected for different purposes can be processed separately.

- Separation of testing and production systems
- Client separation—logical separation of the data (e.g. different file directories)

- Use of different types of encryption

4. Pseudonymisation

Personal data is processed in such a way that the data can no longer be assigned to a specific data subject without additional information being provided, given that such additional information is kept separately and is subject to appropriate technical and organisational measures.

- Definition of the pseudonymisation rule, possibly based on personnel, customer or patient identification numbers (use of UUID v4)
- Authorisation: Determination of persons authorised to manage the pseudonymisation process, carry out pseudonymisation and, if necessary, de-pseudonymisation
- Random generation of assignment tables or secret parameters used in an algorithmic pseudonymisation
- Protection of assignment tables or secret parameters, both against unauthorised access and against unauthorised use
- Separation of data to be pseudonymised into identifying information to be replaced and further information

II. Integrity (Art. 32 [1] [b] GDPR)

1. Disclosure control

It must be ensured that personal data cannot be read, copied, modified, or removed by unauthorised parties during electronic transmission, during transport or during storage to data carriers and that it can be verified to which locations or sites a transmission of personal data is provided for by means of data transfer.

- Documentation of retrieval and transmission processes
- Determination of the persons authorised for transmission or transport
- Regulations regarding dispatch method and determination of transport route
- Use of safe transport containers
- Securing of the transmission and transport route
- Data encryption
- Monitoring of transportation time
- Completeness and correctness check (after the transfer)
- Use of a VPN

2. Input control

The possibility to subsequently verify and determine whether, and by whom, personal data was entered into, changed or removed from data processing systems must be ensured.

- Definition of entry authorisation
- Logging of logins

III. Availability, resilience (Art. 32 [1] [b] GDPR) and rapid recoverability (Art. 32 [1] [c] GDPR)

1. Availability

Personal data must be protected against accidental destruction or loss.

- UPS (uninterrupted power supply)
- Redundant power supply
- Emergency power system
- Fire protection and disaster regulations
- Fire detector
- Spatially separated storage of the data backups created
- Redundant server structure
- Securing of property, in particular of server rooms
- Virus protection concept
- Climate control

2. Rapid recoverability

Appropriate measures must be taken to restore data in the event of loss, destruction or undesired changes to personal data.

- Backup systems to restore lost data
- Testing of restoration
- Emergency concept with recovery plan

3. Resilience

Appropriate measures must be taken to maintain the functionality of the systems in the event of an incident.

- Update or patch management
- Intrusion detection and response system
- Training employees to identify incidents and avoid future incidents
- Switch to fail-safe mode in the event of an incident

IV. Procedure for regular review, assessment and evaluation (Art. 32 [1] [d] GDPR; Art. 25 [1] GDPR)

1. Processing control

Commissioned data processing in accordance with the order and the instructions must be guaranteed.

- Clear structure and execution of Agreements
- Delimitation of responsibilities and obligations between Contractor and Customer

- Careful selection of the Contractor
- Formalisation of order placement
- Logging and monitoring of proper execution of the Agreement
- Sanctions for breach of Agreement
- Information about emerging vulnerabilities and other risk factors, if necessary revision of the risk analysis and assessment
- Audits by the data protection officer

2. External inspections, audits, certifications

- Only ISO 27001 certified data centres are used. ISO 27001 is an international standard for information security. It documents the security and quality of the respective data centre in accordance with international standards with respect to security management, security policy, access and admission controls, IT incident management and compliance with legal obligations, among other things.

Annex 2

Overview of the Subcontractors used by the Contractor in accordance with clause 10 (2)

Company Subcontractor	Address/country	Description of the partial service assumed
alfatraining Bildungszentrum GmbH	Kriegsstraße 100 76133 Karlsruhe Germany	Parent company, provision of infrastructure, support and development.
SysEleven	SysEleven GmbH Umspannwerk – Aufgang C Ohlauer Straße 43 10999 Berlin Germany	**Data centre (ISO 27001 certified)** The following data is transported via SysEleven (encrypted during transport over the internet): - Audio streams (AES 256 encrypted) - Video streams (TLS encrypted) - Real-time events (e.g. entering or leaving the room, chat messages, using the pause button) The following data is processed via SysEleven: - Customer database - Meta data log (e.g. login times or sender and sending time of a chat message) - Backend services: authentication service, user service (e-mail addresses, billing data, user data)

noris	noris network AG Thomas-Mann-Straße 16-20 90471 Nuremberg Germany	**Data centre (ISO 27001 certified)** The following data is transported via noris (encrypted during transport over the internet): - Audio streams (AES 256 encrypted) - Video streams (TLS encrypted) - Real-time events (e.g. entering or leaving the room, chat messages, using the pause button) The following data is processed via noris: - Customer database - Meta data log (e.g. login times or sender and sending time of a chat message) - Backend services: authentication service, user service (e-mail addresses, billing data, user data)

Hetzner	Hetzner Online GmbH Industriestraße 25 91710 Gunzenhausen Germany	**Data centre (ISO 27001 certified)** The following data is transported via Hetzner (encrypted during transport over the internet): - Audio streams (AES 256 encrypted) - Video streams (TLS encrypted) - Real-time events (e.g. entering or leaving the room, chat messages, using the pause button) The following data is processed via Hetzner: - Customer database - Meta data log (e.g. login times or sender and sending time of a chat message) - Backend services: authentication service, user service (e-mail addresses, billing data, user data)
1&1 IONOS SE	1&1 IONOS SE Elgendorfer Straße 57 56410 Montabaur Germany	**Data centre (ISO 27001 certified)** The following data is transported via IONOS (encrypted during transport over the internet): - Audio streams (AES 256 encrypted) - Video streams (TLS encrypted) - Real-time events (e.g. entering or leaving the room, chat messages, using the pause button)

		The following data is processed via IONOS: - Customer database - Meta data log (e.g. login times or sender and sending time of a chat message) - Backend services: authentication service, user service (e-mail addresses, billing data, user data)
Open Telekom Cloud (OTC)	Telekom Deutschland GmbH Landgrabenweg 151 53277 Bonn Germany	**Data centre (ISO 27001 certified)** The following data is processed via OTC: - Customer database If required, we use this data centre for the same services as SysEleven, noris, Hetzner and IONOS in the future.
Strato	Strato AG Pascalstraße10 10587 Berling Germany	**Data centre (ISO 27001 certified)** Not yet active, i.e. currently, no personal data is processed there. If required, we use this data centre for the same services as SysEleven, noris, Hetzner and IONOS.
sendinblue	Sendinblue GmbH Köpenicker Straße 126 10179 Berlin	**Mailing provider** When sending transactional e-mails that are necessary for establishing communication, personal data are processed. In detail these are - E-mail for creating an account: Name, e-mail address, company name - User invitation email: Name, e-mail address, company name of the host

		- Sending personalised guest links: name, e-mail address - E-mail if password has been forgotten: Name, e-mail address - E-mail for deletion of the company: Name, e-mail address, company name