Stand: Januar 2023

Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO

zwischen

dem Kunden

- nachstehend **Auftraggeber** genannt -

und

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

- nachstehend **Auftragnehmer** genannt -

Präambel

Der Auftragnehmer stellt dem Auftraggeber die Anwendung alfaview® zur Verfügung und erbringt in diesem Zusammenhang Leistungen auf Grundlage einer zwischen den Parteien geschlossenen Vereinbarung bestehend aus dem Bestellformular und den Allgemeinen Geschäftsbedingungen (nachfolgend „**Hauptvertrag**“ genannt). Im Rahmen dieser Leistungserbringung ist es erforderlich oder zumindest nicht auszuschließen, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Auftragsdaten**“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftragsdaten zur Durchführung des Hauptvertrags.

§ 1 Anwendungsbereich, Gegenstand und Dauer der Verarbeitung

(1) Diese Datenschutzvereinbarung findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Auftragsdaten im Rahmen dieser Auftragsverarbeitung in Berührung kommen können. Keine Anwendung findet diese Datenschutzvereinbarung, wenn der Auftraggeber als natürliche Person die Anwendung alfaview® zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten einsetzt.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers bei der Zurverfügungstellung der Anwendung alfaview® und der Erbringung der im Hauptvertrag definierten Leistungen; Details hierzu ergeben sich aus dem Hauptvertrag (Gegenstand der Verarbeitung). Es werden hierbei personenbezogene Daten zum Zweck der Bereitstellung der Anwendung alfaview® und Dienste entsprechend des Hauptvertrages verarbeitet als auch personenbezogene Daten, welche die Nutzer bei Verwendung von alfaview® in den Online-Meetings eingeben oder erfassen (Umfang, Art und Zweck der Verarbeitung).

(3) Dauer der Verarbeitung: Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrags.

(4) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenbezogene Daten, welche zur Bereitstellung der Anwendung alfaview® und Herstellung der Kommunikation erforderlich sind (Nutzerprofil): Zugangsdaten von registrierten Benutzern wie Name und E-Mail-Adresse; optional können die Nutzer im Nutzerprofil auch weitere Angaben machen wie etwa Titel, Initialen, Ort. Bei Einladungen über Gastlinks ist nur die Eingabe eines Namens oder eines Pseudonyms des Gastnutzers erforderlich bzw. im Falle sog. individualisierter Gastlinks Name und E-Mail-Adresse des Gastnutzers.

- Personenbezogene Daten, welche von den Nutzern während der Kommunikation in Online-Meetings über die Anwendung alfaview® erhoben und verarbeitet werden: Textnachrichten (Chats), Video- und Audiodaten, welche Bildnisse und Stimmen der Nutzer enthalten; diese Video- und Audiodaten als auch Textnachrichten in Chats können auch weitere, zwischen den Nutzern von alfaview® im Rahmen der Kommunikation ausgetauschte Personenstammdaten, Kommunikationsdaten und andere personenbezogene Daten enthalten. Audio-, Video- und Chatnachrichten werden grundsätzlich nicht gespeichert bzw. nur bis zum Ende der Kommunikation zwischengespeichert, es sei denn, der Auftraggeber erstellt manuell eine Aufzeichnung.

(5) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen den Auftraggeber (bei der Nutzung der Anwendung durch Privatpersonen), Mitarbeiter oder sonstige nutzungsberechtigte Personen auf Seiten des Auftraggebers (z.B. freie Mitarbeiter, Dozenten, Lehrbeauftragte) und die jeweiligen Kommunikationspartner der nutzungsberechtigten Personen sowie Personen, über die kommuniziert wird.

(6) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

§ 2 Verantwortlichkeit für die Datenverarbeitung

Der Auftraggeber ist im Rahmen dieses Vertrages für die Rechtmäßigkeit der Verarbeitung der Auftragsdaten sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verarbeitet personenbezogene Daten nur im Auftrag des Auftraggebers auf dessen Weisung hin.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die Auftragsdaten nicht an unbefugte Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftragsdaten gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen

umzusetzen, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat Auftragsdaten nur nach Weisung des Auftraggebers unter Beachtung von § 6 dieser Vereinbarung zu verarbeiten. Der Auftragnehmer hat die Auftragsdaten ausschließlich nach Weisung des Auftraggebers zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten oder Auskunft über die gespeicherten Daten des Auftraggebers wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung und -nutzung in seinem Verantwortungsbereich, der Unterauftragnehmer nach § 9 dieser Vereinbarung einschließt, in Übereinstimmung mit den Bestimmungen dieser Vereinbarung erfolgt.

(3) Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber keine Kopien oder Duplikate der Auftragsdaten anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die Datenverarbeitung durch den Auftragnehmer betreffen. Der Auftragnehmer kann für diese Unterstützungsleistung die ihm hierdurch entstehenden, nachzuweisenden Aufwände und Kosten ersetzt verlangen (reiner Aufwandsersatz), es sei denn, die Kontrolle steht in Zusammenhang mit einem Verstoß gegen Datenschutzvorschriften oder Festlegungen in diesem Vertrag, welchen der Auftragnehmer zu vertreten hat.

(5) Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit und den Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen.

(6) Der Auftragnehmer hat die bei der Verarbeitung von Daten des Auftraggebers beschäftigten Personen gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO zur Vertraulichkeit und zur Geheimhaltung entsprechend § 203 StGB zu verpflichten.

(7) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen und Verstöße des Auftragnehmers, der bei ihm beschäftigten Personen oder eines eingesetzten Unterauftragnehmers gem. § 9 gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers durchführen.

§ 5 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von betroffenen Personen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Dem Auftraggeber obliegen die aus Art. 33 und Art.34 DSGVO resultierenden Meldepflichten.

§ 6 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Daten des Auftraggebers ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie insbesondere in den Bestimmungen dieser Vereinbarung und den Festlegungen des Hauptvertrags Ausdruck finden, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftraggeber kann in schriftlicher Form oder in Textform einzelne Weisungen ändern, ergänzen oder ersetzten (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Ziehen Einzelweisungen Mehrkosten nach sich, insbesondere wenn diese über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind diese dem Auftragnehmer zu vergüten. Eine Vergütungspflicht besteht nicht, wenn die Weisung aufgrund eines Verstoßes gegen Datenschutzvorschriften oder Festlegungen in diesem Vertrag notwendig ist, welche der Auftragnehmer zu vertreten hat.

(2) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder in Textform (z.B. per E-Mail) bestätigen.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 S. 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

§ 7 Unterstützungspflichten

(1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Informationen oder Auskünfte zur Verarbeitung von Daten dieser Person zu geben oder die Rechte von betroffenen Personen nach Kapitel III (Artt. 12 bis 23) der DSGVO zu gewährleisten, wird der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Pflichten mit geeigneten technischen und organisatorischen Maßnahmen entsprechend Art. 28 Abs. 3 lit. e DSGVO unterstützen.

(2) Der Auftragnehmer unterstützt den Auftraggeber entsprechend Art. 28 Abs. 3 lit. f DSGVO bei der Einhaltung der in den Artt. 32 bis 36 DSGVO genannten Pflichten.

(3) Bei der Erbringung der Unterstützungsleistungen nach Abs. 1 und 2 dem Auftragnehmer entstehende und nachzuweisende Aufwände und Kosten (reiner Aufwandsersatz) sind vom Auftraggeber zu ersetzen, es sei denn, die Unterstützungsleistungen stehen in Zusammenhang mit einem Verstoß gegen Datenschutzvorschriften oder Festlegungen in diesem Vertrag, welche der Auftragnehmer zu vertreten hat.

§ 8 Kontrollrechte des Auftraggebers

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung, die nur in besonderen Ausnahmefällen entfallen darf - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Die Kosten für die Durchführung der Kontrolle trägt der Auftraggeber, es sei denn, die Kontrolle steht in Zusammenhang mit einem Verstoß gegen Datenschutzvorschriften oder Festlegungen in diesem Vertrag, welche der Auftragnehmer zu vertreten hat.

§ 9 Weitere Auftragsverarbeiter nach Art. 28 Abs. 2 und 4 DSGVO)

(1) Der Auftraggeber erteilt hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter (nachfolgend „**Unterauftragnehmer**“ genannt) hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen Unterauftragnehmer ergeben sich aus Anlage 2, für welche der Auftragnehmer die Genehmigung mit Abschluss dieser Vereinbarung erteilt. Der Auftragnehmer informiert den Aufraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen diese Änderung Einspruch zu erheben (Art. 28 Abs. 2 DSGVO). Erfolgt kein Einspruch innerhalb von 14 Tage ab Bekanntgabe, gilt die Zustimmung zur Änderung als gegeben. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Wochen zu kündigen.

(2) Der Auftragnehmer ist verpflichtet, Unterauftragnehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Unterauftragnehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann. Insbesondere wird der Auftragnehmer solche Unterauftragnehmer zur Geheimhaltung entsprechend §203 StGB verpflichten, welchen Privatgeheimnissen des Auftraggebers gem. §203 StGB offenbart werden könnten.

§ 10 Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im

Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber nach dessen Wahl auszuhändigen oder datenschutzgerecht zu vernichten.. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

§11 Haftung

Eine zwischen den Vertragsparteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, es sei denn, die Vertragsparteien haben ausdrücklich etwas anderes vereinbart.

§ 12 Schlussvorschriften

(1) Soweit in dieser Vereinbarung keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen dieser Vereinbarung und Regelungen aus sonstigen vertraglichen Abreden, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus dieser Vereinbarung vor.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers oder Änderungen der Anlage - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Die Rechte und Pflichten des Vertrages bleiben so lange bestehen wie der Auftragnehmer die Daten des Auftraggebers verarbeitet.

(4) Ausschließlicher Gerichtsstand für alle aus diesem Vertrag sich ergebenden Streitigkeiten ist der Sitz des Auftragnehmers.

(5) Es gilt deutsches Recht.

Anlage 1

Übersicht über die technisch-organisatorischen Maßnahmen

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. Zutrittskontrolle
Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

- Einsatz von Magnet- bzw. Chipkarten für Zutrittsberechtigte
- Videoüberwachung
- Festlegung der zugangsberechtigten Personen
- Closed Shop-Betrieb
- Revisionsfähigkeit der Zugangsberechtigungen
- Einsatz eines Zugangskontrollsystems
- Schlüsselregelung und aktuelle Schlüsselliste
- Protokollierung der Zu- und Abgänge
- Empfang / Pförtner
- Verschlossene Bürotüren und Fenster bei Abwesenheit

2.Zugangs- und Zugriffskontrolle
Bei der Zugangskontrolle ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Bei der Zugriffskontrolle ist Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

- Identifikation und Authentifizierung der Benutzer/ Passwortschutz
- Maschinelle Überprüfung der Berechtigungen
- Einführung zugriffsbeschränkender Maßnahmen (z. B. nur Leseberechtigung)
- Zeitliche Begrenzung der Zugriffsmöglichkeiten
- Benutzerbezogene Protokollierung der (Fehl-)Zugriffe
- Einsatz von Verschlüsselungsverfahren
- Zentrale Vergabestelle von Benutzerrechten

3. Trennungskontrolle
Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Trennung von Test- und Produktivsystem
- Mandantentrennung - Logische Trennung der Daten (z.B. unterschiedliche Dateiverzeichnisse)
- Einsatz unterschiedlicher Verschlüsselungen

4. Pseudonymisierung
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technische und organisatorische Maßnahmen unterliegen.

- Definition der Pseudonymisierungsregel, ggf. anknüpfend an Personal-, Kunden- oder Patienten-Kennziffern (Verwendung von UUID v4)
- Autorisierung: Festlegung der Personen, die zur Verwaltung der Pseudonymisierungs-verfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind

- zufällige Erzeugung der Zuordnungstabellen oder der in eine algorithmische Pseudonymisierung eingehenden geheimen Parameter
- Schutz der Zuordnungstabellen bzw. geheimen Parameter sowohl gegen unautorisierten Zugriff als auch gegen unautorisierte Nutzung
- Trennung der zu pseudonymisierenden Daten in die zu ersetzenden identifizierenden und die weiteren Angaben

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

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

- Dokumentation der Abruf- und Übermittlungsprogramme
- Festlegung der für die Übermittlung oder den Transport Berechtigten
- Regelungen für die Versandart und Festlegung des Transportweges
- Verwendung sicherer Transportbehälter
- Sicherung des Übertragungs- und Transportweges
- Verschlüsselung der Daten
- Überwachung der Transportzeit
- Vollständigkeits- und Richtigkeitsprüfung (nach der Übertragung)
- Nutzung eines VPN

2. Eingabekontrolle
Es ist Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Festlegung von Eingabebefugnissen
- Protokollierung der Logins

III. Verfügbarkeit, Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) und Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

1. Verfügbarkeit
Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- USV (Unterbrechungsfreie Stromversorgung)
- Redundante Leitungsversorgung
- Notstromaggregat
- Brandschutz- und Katastrophenordnung
- Brandmelder
- Räumlich getrennte Aufbewahrung der erstellten Datensicherungen
- Redundante Serverstruktur
- Objektsicherung insb. der Serverräume
- Virenschutzkonzept
- Klimatisierung

2. Rasche Wiederherstellbarkeit
Es sind geeignete Maßnahmen zu ergreifen, um im Falle eines Verlusts, einer Zerstörung oder einer nicht gewünschten Veränderung von personenbezogenen Daten die Daten wiederherzustellen.

- Backup-Systeme zur Wiederherstellung verlorener Daten

- Testen der Wiederherstellung
- Notfallkonzept mit Wiederanlaufplan

3. Belastbarkeit/ Resilienz
Es sind geeignete Maßnahmen zu ergreifen, um im Falle von Zwischenfällen die Funktionsfähigkeit der Systeme aufrechtzuerhalten.

- Update- bzw. Patchmanagement
- Intrusion-Detection-and-Response-System
- Schulung der Beschäftigten zur Erkennung von Zwischenfällen sowie zur Vermeidung zukünftiger Zwischenfälle
- Wechsel auf Fail-Safe-Modus im Falle eines Zwischenfalls

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

1. Auftragskontrolle
Es ist eine auftrags- und weisungsgemäße Auftragsdatenverarbeitung zu gewährleisten.

- Klare Vertragsgestaltung und –ausführung
- Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
- Sorgfältige Auswahl des Auftragnehmers
- Formalisierung der Auftragserteilung
- Protokollierung und Kontrolle der ordnungsgemäßen Vertragsausführung
- Sanktionen bei Vertragsverletzung
- Information über neu auftretende Schwachstellen und andere Risikofaktoren, ggf. Überarbeitung der Risikoanalyse und –bewertung
- Audits durch den Datenschutzbeauftragten

2. Externe Prüfungen, Audits, Zertifizierungen

- Es werden ausschließlich ISO 27001 zertifizierte Rechenzentren eingesetzt.
  Die ISO 27001 ist eine internationale Norm für Informationssicherheit. Sie dokumentiert die Sicherheit und Qualität des jeweiligen Rechenzentrums nach internationalen Standards unter anderem in Bezug auf das Sicherheitsmanagement, die Sicherheitspolitik, Zugriffs- und Zugangskontrollen, das IT-Störungsmanagement sowie die Einhaltung rechtlicher Verpflichtungen.

Anlage 2

Übersicht über die, die vom Auftragnehmer eingesetzten Unterauftragnehmer gem. § 10 Abs. 2

Firma Unterauftragnehmer	**Anschrift/Land**	**Beschreibung der übernommenen Teilleistung**
alfatraining Bildungszentrum GmbH	Kriegsstr. 100 76133 Karlsruhe Deutschland	Muttergesellschaft, Bereitstellung von Infrastruktur, Support und Entwicklung.
SysEleven	SysEleven GmbH Boxhagener Straße 80 10245 Berlin Deutschland	**Rechenzentrum (ISO 27001-zertifiziert)** Folgende Daten werden über SysEleven transportiert (während des Transports über das Internet verschlüsselt): - Audioströme (AES 256 verschlüsselt) - Videoströme (TLS verschlüsselt) - Realtime Events (z.B. Betreten/Verlassen des Raumes, Chatnachrichten, Benutzung des Pausebuttons) Folgende Daten werden über SysEleven verarbeitet: - Kundendatenbank - Protokoll der Metadaten (z.B. Loginzeiten oder wer wann eine Chatnachricht geschrieben hat) - Backend Services: Authentifizierungsservice, Benutzerservice (E-Mailadressen, Rechnungsdaten, Benutzerdaten)
noris	noris network AG Thomas-Mann- Straße 16 - 20 D-90471 Nürnberg Deutschland	**Rechenzentrum (ISO 27001-zertifiziert)** Folgende Daten werden über noris transportiert (während des Transports über das Internet verschlüsselt): - Audioströme (AES 256 verschlüsselt) - Videoströme (TLS verschlüsselt)

		- Realtime Events (z.B. Betreten/Verlassen des Raumes, Chatnachrichten, Benutzung des Pausebuttons) Folgende Daten werden über noris verarbeitet: - Kundendatenbank - Protokoll der Metadaten (z.B. Loginzeiten oder wer wann eine Chatnachricht geschrieben hat) - Backend Services: Authentifizierungsservice, Benutzerservice (E-Mailadressen, Rechnungsdaten, Benutzerdaten)
Hetzner	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	**Rechenzentrum (ISO 27001-zertifiziert)** Folgende Daten werden über Hetzner transportiert (während des Transports über das Internet verschlüsselt): - Audioströme (AES 256 verschlüsselt) - Videoströme (TLS verschlüsselt) - Realtime Events (z.B. Betreten/Verlassen des Raumes, Chatnachrichten, Benutzung des Pausebuttons) Folgende Daten werden über Hetzner verarbeitet: - Kundendatenbank - Protokoll der Metadaten (z.B. Loginzeiten oder wer wann eine Chatnachricht geschrieben hat) - Backend Services: Authentifizierungsservice, Benutzerservice (E-Mailadressen, Rechnungsdaten, Benutzerdaten)

1&1 IONOS SE	1&1 IONOS SE Elgendorfer Str. 57 56410 Montabaur Deutschland	**Rechenzentrum (ISO 27001-zertifiziert)** Folgende Daten werden über IONOS transportiert (während des Transports über das Internet verschlüsselt): - Audioströme (AES 256 verschlüsselt) - Videoströme (TLS verschlüsselt) - Realtime Events (z.B. Betreten/Verlassen des Raumes, Chatnachrichten, Benutzung des Pausebuttons) Folgende Daten werden über IONOS verarbeitet: - Kundendatenbank - Protokoll der Metadaten (z.B. Loginzeiten oder wer wann eine Chatnachricht geschrieben hat) - Backend Services: Authentifizierungsservice, Benutzerservice (E-Mailadressen, Rechnungsdaten, Benutzerdaten)
Open Telekom Cloud (OTC)	Telekom Deutschland GmbH Landgrabenweg 151 53227 Bonn	**Rechenzentrum (ISO 27001-zertifiziert)** Folgende Daten werden über OTC verarbeitet: - Kundendatenbank Bei Bedarf setzen wir dieses Rechenzentrum zukünftig auch für dieselben Dienste ein wie SysEleven, noris, Hetzner und IONOS.
Strato	Strato AG Pascalstraße 10 10587 Berlin	**Rechenzentrum (ISO 27001-zertifiziert)** Momentan noch nicht aktiv, d.h. derzeit werden dort keine personenbezogenen Daten verarbeitet.

		Bei Bedarf setzen wir dieses Rechenzentrum für dieselben Dienste ein wie SysEleven, noris, Hetzner und IONOS.
rapidmail	rapidmail GmbH Wentzingerstraße 21 79106 Freiburg im Breisgau	**Mailing-Provider** Beim Versand transaktionaler E-Mails, die für die Herstellung der Kommunikation notwendig sind, werden personenbezogene Daten verarbeitet. Im Einzelnen sind das: - E-Mail zur Kontoerstellung: Name, E-Mail-Adresse, Firmenname - E-Mail zur Benutzereinladung: Name, E-Mail-Adresse, Firmenname des Gastgebers - Versand personalisierter Gastlinks: Name, E-Mail-Adresse - E-Mail, wenn Passwort vergessen wurde: Name, E-Mail-Adresse - E-Mail zur Löschung der Company: Name, E-Mail-Adresse, Companyname