Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen

Mittelschule Weidenberg, Schulstraße 2, 95466 Weidenberg

- Verantwortlicher -

und

Auctores GmbH, Amberger Straße 82, 92318 Neumarkt

- Auftragsverarbeiter -

Präambel

Der Auftragsverarbeiter betreibt und wartet für den Verantwortlichen das Videokonferenzwerkzeug 2021 und bietet dem Verantwortlichen Support und Anpassungsdienstleistungen dafür an. In diesem Zusammenhang verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen. Diese Vereinbarung regelt die Verpflichtungen der Vertragsparteien nach Art. 28 Abs. 3 DSGVO und ergänzt insoweit den Vertrag des Auftragsverarbeiters mit dem Bayerischen Staatsministerium für Unterricht und Kultus (StMUK) vom 29.03.2021 (im Folgenden "Auftrag" genannt). Sie findet Anwendung auf alle Verarbeitungen personenbezogener Daten, die mit dem Auftrag in Zusammenhang stehen und bei denen der Auftragsverarbeiter oder durch den Auftragsverarbeiter beauftragte Dritte personenbezogene Daten für den Verantwortlichen verarbeiten. Die in der vorliegenden Vereinbarung gewählten Begrifflichkeiten entsprechen den Begrifflichkeiten der DSGVO.

1. Gegenstand und Spezifizierung der Auftragsverarbeitung

1.1 Art, Zweck und Gegenstand der Verarbeitung

- Betrieb und Wartung des Videokonferenzwerkzeugs:
  Zweck der Verarbeitung ist die Bereitstellung von Videokonferenzräumen mit integrierter Chat-Funktion für die Schulen und weiteren Einrichtungen im Ressortbereich des StMUK. Das System ermöglicht den Nutzern synchrone Kommunikation in Ton und Videobild. Um die Nutzung des bereitgestellten Videokonferenzwerkzeugs kontrollieren und die Zutritte zu den Konferenzräumen gezielt steuern zu können, ist der Einsatz personifizierter Benutzerzugänge für berechtigte Nutzer erforderlich. Hierzu stellt der Auftragsverarbeiter eine Verwaltungsoberfläche zur Verfügung, die berechtigten Personen der nutzenden Schulen und weiteren Einrichtungen im Ressortbereich des StMUK zugänglich gemacht wird. Zur Bereitstellung der personifizierten Benutzerzugänge und der Verwaltungszugänge ist die Führung einer Nutzerdatenbank sowie die Implementierung eines Authentifizierungssystems erforderlich, das den Zugriff auf die Videokonferenzräume auf Nutzungsberechtigte beschränkt.
- Support hinsichtlich der Videokonferenzlösung:
  Den berechtigten Nutzern soll Nutzer-Support für das Videokonferenzwerkzeug per Telefon und Ticketsystem angeboten werden. Das Ticketsystem wird von berechtigten Nutzern per E-Mail befüllt. Tickets werden per E-Mail beantwortet.
- Anpassungsdienstleistungen gem. Nr. 10.11.2 des Auftrags nach Bedarf:
  Der AN übernimmt nach Beauftragung durch das StMUK Integrations -, Anpassungs - und Entwicklungsdienstleistungen, um das Videokonferenzwerkzeug beispielsweise in die Systemumgebung des StMUK, z. B. die Lernplattform mebis , die Nutzerdatenbank von mebis oder das Fortbildungsverwaltungssystem FIBS zu integrieren.

Art der verarbeiteten personenbezogenen Daten

- Stammdaten gemäß 3.1.1 in Nr. 7 Anlage 2 BaySchO
- Sichtbare Profilinformationen gemäß 3.1.2 in Nr. 7 Anlage 2 BaySchO
- Passwort gemäß 3.1.3 in Nr. 7 Anlage 2 BaySchO
- Inhaltsdaten gemäß 3.1.4 in Nr. 7 Anlage 2 BaySchO
- Sonstige Nutzungsdaten (Protokolldaten) gem. 3.1.5 in Nr. 7 Anlage 2 BaySchO
- Video- und Bilddaten für die Videonutzung gem. 3.2 in Nr. 7 Anlage 2 BaySchO
- Audiodaten für die Nutzung von Ton bei Videonutzung oder Telefonie (bei Video- oder Telefonkommunikation) gem. 3.2 in Nr. 7 Anlage 2 BaySchO

- Gruppenbezogene Nutzungsdaten gemäß 3.3 in Nr. 7 Anlage 2 BaySchO

Kategorien der betroffenen Personen

- Pädagogisches Personal: Lehrkräfte, Betreuungspersonal förderbedürftiger Schülerinnen und Schüler, Studienreferendare, Lehramtsstudierende im Schulpraktikum, weiteres pädagogisches Personal (z. B. Ganztagsbetreuung)
- Schülerinnen und Schüler
- Gastnutzer
- Weitere Personen, die von der Video- oder Tonübertragung erfasst werden (z. B. Schulbegleitungen)

1.2 Die in diesem Vertrag vereinbarten Leistungen und damit verbundene Datenverarbeitungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Dies gilt unabhängig davon, ob diese von dem Auftragsverarbeiter selbst oder weiteren Auftragsverarbeitern erbracht werden (s. Ziffer 6).

2. Rechte und Pflichten des Auftragsverarbeiters

2.1 Der Auftragsverarbeiter verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Verantwortlichen sowie entsprechend den datenschutzrechtlichen Regelungen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, verpflichtet ist. In letzterem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 Buchst. a DSGVO). Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen Daten für keine anderen Zwecke und insbesondere nicht für eigene Zwecke. Kopien der Daten werden, ohne dass sie im Auftrag oder in diesem Vertrag geregelt sind, nicht erstellt.

Sofern Weisungen des Verantwortlichen zunächst mündlich erfolgen, sind sie unverzüglich schriftlich oder elektronisch zu bestätigen.

2.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Ist die Rechtmäßigkeit einer Weisung zweifelhaft, ist der Auftragsverarbeiter berechtigt, die Durchführung der Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird. Stehen schwere Persönlichkeitsrechtsverletzungen im Raum oder nimmt der Auftragsverarbeiter bei weisungsgemäßem Handeln das Risiko einer strafbaren Handlung auf sich, darf er die Umsetzung der Weisung darüber hinaus aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

2.3 Der Auftragsverarbeiter gestaltet seine innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft insbesondere geeignete technische und organisatorische Maßnahmen, um einen dem Risiko angemessenen Schutz der Daten des Verantwortlichen zu gewährleisten (Art. 32 Abs. 1 DSGVO). Er trifft diese technischen und organisatorischen Maßnahmen so, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Die entsprechenden technischen und organisatorischen Maßnahmen ergeben sich aus der Anlage 1. Änderungen der getroffenen Maßnahmen durch den Auftragsverarbeiter sind nur zulässig, wenn sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Verantwortlichen mitzuteilen und mit diesem abzustimmen.

2.4 Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte (Art. 28 Abs. 3 Buchst. e DSGVO) und unterstützt den Verantwortlichen unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa bei erforderlichen Datenschutz-Folgenabschätzungen (Art. 28 Abs. 3 Satz 2 Buchst. f DSGVO).

2.5 Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung der Daten des Verantwortlichen befassten Beschäftigten und anderen für den Auftragsverarbeiter tätigen Personen nach Maßgabe des Art. 29 DSGVO untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragsverarbeiter, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Die Vertraulichkeits- /Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

2.6 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn ihm im Rahmen des Auftragsverhältnisses Verletzungen des Schutzes personenbezogener Daten des Verantwortlichen bekannt werden. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

2.7 Der Auftragsverarbeiter nennt dem Verantwortlichen Ansprechpartner für im Rahmen des Vertrages anfallende Weisungen sowie einen etwaigen Datenschutzbeauftragten. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Verantwortlichen die Kontaktdaten eines neuen, zuständigen Ansprechpartners bzw. etwaigen Datenschutzbeauftragten unverzüglich anzuzeigen
.

Ansprechpartner des Auftragsverarbeiters:

Böhm, Maximilian, techn. Projektleiter Softwareentwicklung, 09181/5198-0, info@auctores.de

Datenschutzbeauftragter des Auftragsverarbeiters

Wanjura, Thomas, ext. Datenschutzbeauftragter Projekt 29 GmbH & Co. KG 0941/2986930 info@ projekt29.de

2.8 Der Auftragsverarbeiter berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Verantwortliche dies anweist und dies vom Weisungsrahmen umfasst ist, es sei denn, die Weisung widerspricht etwaigen gesetzlichen Aufbewahrungspflichten.

2.9 Nach Auftragsende sind Daten, Datenträger sowie sonstige Materialien auf Verlangen und nach Wahl des Verantwortlichen entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht.

2.10 Im Falle einer Inanspruchnahme des Verantwortlichen durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragsverarbeiter, den Verantwortlichen bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3. Rechte und Pflichten des Verantwortlichen

3.1 Der Verantwortliche ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO, die Datenweitergabe an den Auftragsverarbeiter sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO verantwortlich (" Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO).

3.2 Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, falls er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.3 Im Falle einer Inanspruchnahme des Auftragsverarbeiters durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Verantwortliche, den Auftragsverarbeiter bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3.4 Der Verantwortliche nennt bei der Registrierung im Schulportal weisungsberechtigte Personen für im Rahmen des Vertrages anfallende Weisungen sowie den Datenschutzbeauftragten. Der Auftragsverarbeiter bekommt diese Informationen in einer CSV-Datei vom StMUK. Bei einem Wechsel

oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Auftragsverarbeiter über dessen Ansprechpartner unverzüglich die Kontaktdaten eines neuen, zuständigen Ansprechpartners bzw. Datenschutzbeauftragten anzuzeigen.

Weisungsberechtigte Personen des Verantwortlichen

Leitung des Auftraggebers
Zinner, Jörg
Joerg.Zinner@schule.bayern.de

Administratoren des Auftraggebers
Fichtel, Kim
Kim.Fichtel@schule.bayern.de

Starz, Thomas
Thomas.Starz-Rampp@schule.bayern.de

Freissle, Bianca
Bianca.Freissle@schule.bayern.de

Datenschutzbeauftragte(r) des Verantwortlichen

Datenschutzbeauftragter des Auftraggebers
Failner, Gerald
dsb-schulamt-lkr@lra-bt.bayern.de

3.5 Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen. Die Befugnisse der Aufsichtsbehörden
- insbesondere nach Art. 58 Abs. 1 DSGVO - bleiben hiervon unberührt.

4. Anfragen betroffener Personen

Macht eine betroffene Person ihre Rechte gemäß Art. 15 ff. DSGVO gegenüber dem Auftragsverarbeiter geltend, wird dieser die betroffene Person an den Verantwortlichen verweisen, sofern eine Zuordnung an den Verantwortlichen auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Nr. 2.4 dieser Vereinbarung unterstützt der Auftragsverarbeiter den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.

5. Kontrollrechte des Verantwortlichen

5.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO).

5.2 Sofern einschlägig, verpflichtet sich der Auftragsverarbeiter, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zuinformieren.

5.3 Der Verantwortliche ist berechtigt, sich vor Beginn und während der Verarbeitung von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen. Dies und Maßnahmen nach Nr. 5.4 werden nicht durch die Vorlage von Nachweisen nach Nr. 5.1 ausgeschlossen.

5.4 Inspektionen durch den Verantwortlichen oder durch einen von diesem beauftragten Prüfer werden grundsätzlich nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlauffrist zu den üblichen Geschäftszeiten durchgeführt. Der Auftragsverarbeiter hat die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung abhängig zu machen, wenn die Möglichkeit besteht, dass der Verantwortliche oder ein von diesem beauftragter Prüfer im Rahmen seiner Inspektion auch Kenntnis von Daten erlangt, die der Auftragsverarbeiter im Auftrag eines anderen Verantwortlichen verarbeitet. Der Verantwortliche stellt sicher, dass ein von ihm beauftragter Prüfer in keinem Wettbewerbsverhältnis zu dem Auftragsverarbeiter steht.

6. Subunternehmer (weitere Auftragsverarbeiter)

6.1 Ein Subunternehmerverhältnis liegt vor, wenn der Auftragsverarbeiter weitere Auftragsverarbeiter mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt.

Der Auftragsverarbeiter trägt bei der Auswahl eines Subunternehmers insbesondere Sorge dafür, dass dieser hinreichende Garantien dafür bietet, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der Datenschutz-Grundverordnung erfolgt.

Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn ein Zugriff auf personenbezogene Daten des Verantwortlichen ausgeschlossen ist), Reinigungskräfte und Prüfer. Der Auftragsverarbeiter trifft mit diesen Dritten im erforderlichen Umfang

schriftliche Vereinbarungen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten und behält sich Kontrollmaßnahmen vor, um den Schutz und die Sicherheit der Daten des Verantwortlichen zu gewährleisten.

6.2 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). In dem Vertrag mit dem Subunternehmer sind dieselben datenschutzrechtlichen Pflichten aus der vorliegenden Vereinbarung dem Subunternehmer wirksam aufzuerlegen. Insbesondere muss der Verantwortliche berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

6.3 Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Abschnitt vertraglich auferlegt wurden.

6.4 Der Auftragsverarbeiter nimmt keinen Subunternehmer ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung in Anspruch. Der Auftragsverarbeiter teilt dem Verantwortlichen die bereits bei Abschluss dieses Vertrags bestehenden Subunternehmer vorab mit. Die bei Vertragsbeginn bestehenden Subunternehmer wurden vom Auftragsverarbeiter im Rahmen seines Angebots in der Anlage 2 benannt. Diese gelten als von Beginn des Auftrages an genehmigt.

6.5 Gemäß den vorgenannten Regelungen erteilt der Verantwortliche dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 Abs. 2 DSGVO in Anspruch zu nehmen (Art. 28 Abs. 2 Satz 1 Alt. 2, Satz 2 DSGVO). Der Auftragsverarbeiter informiert den Verantwortlichen frühzeitig, wenn er Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben. Der Einspruch ist innerhalb von einem Monat nach Zugang der Information über die Änderungen schriftlich gegenüber dem Auftragsverarbeiter einzulegen. Kann keine einvernehmliche Lösung erzielt werden, erfolgt eine Einschränkung oder Beendigung der Auftragsverarbeitung.

6.6 Eine Beauftragung von Subunternehmern mit Sitz in Drittstaaten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums darf nicht erfolgen.

7. Haftung und Schadensersatz

Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

8. Schlussbestimmungen

8.1 Die Laufzeit der vorliegenden Vereinbarung entspricht der Laufzeit des Auftrags.

8.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn die Daten des Verantwortlichen durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter beim Auftragsverarbeiter gefährdet werden. Der Auftragsverarbeiter informiert in diesem Fall alle Beteiligten unverzüglich darüber, dass das Eigentum an den Daten ausschließlich beim Verantwortlichen liegt.

8.3 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen oder in einem elektronischen Format abgefassten Vereinbarung, die den ausdrücklichen Hinweises darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

8.4 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieser Anlage beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

Weidenberg, den 24.04.2021	Neumarkt, den 24.04.2021
Ort, Datum	Ort, Datum
Jörg Zinner	Karl Weigl
- Verantwortlicher -	- Auftragsverarbeiter -

Dieses Dokument ist ohne Unterschrift gültig.

Es wurde digital unterzeichnet: 24.04.2021 04:48

Anlage 1 – Technische und organisatorische Maßnahmen

1. Vertraulichkeit gem. Art. 32 Abs 1 lit. b DSGVO
1.1. Zutrittskontrolle

Maßnahmen, die dazu dienen, Unberechtigte den Zutritt zu Systemen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Schließanlage	Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.
Die Räumlichkeiten bei den Rechenzentrumsbetreibern sind mit entsprechend Schließanlagen ausgestattet.	Besucheranmeldung, Besucherbücher
Das Gebäude ist mit einer Sicherheits-Schließanlage ausgerüstet.	Geschultes Personal zum Empfang von Gästen
Automatische Bildschirmsperre nach Inaktivität	
Alarm-Anlage mit Bewegungsmelder in den Fluren	

1.2. Zugangskontrolle

Maßnahmen, die verhindern sollen, dass Systeme von Unberechtigte genutzt werden können

Technische Maßnahmen	**Organisatorische Maßnahmen**
Zugriff ist selektiv geregelt. Es wird lediglich von firmeneigenen Geräten über verschlüsselte Zugangswege auf die Daten zugegriffen.	Mitarbeiter haben Zugang zum Gebäude. Benutzerzugänge werden selektiv für Mitarbeiter ausgegeben. Sensible Daten sind nur für ausgewählte Mitarbeiter zugänglich.
Es gibt Heimarbeitsplätze, welche nach Best-Practice-Maßnahmen des LDA Bayern umgesetzt wurden.	Benutzerzugänge werden entsprechend bei Zugängen und Abgängen von Mitarbeitern aktualisiert
Sichere VPN-Verbindung zwischen Betriebsstätten und Rechenzentren. Einsatz von verschlüsselten State-of-the-Art-Verbindungen (SSH, HTTPS)	Es findet keine Dokumentation von Benutzerzugängen statt. Gültige Benutzer sind alle Mitarbeiter.
State-of-the-Art Firewall. Durch einen Prozess wird sichergestellt, dass jederzeit die aktuellen Updates eingespielt sind	Die Entscheidungen zur Rechtevergabe halten sich streng an die entsprechenden Vorgaben, Datenvermeidung und Datensparsamkeit, weniger ist hier oft mehr.
Aktuellste Sicherheitsupdates und Virenscanner. Es wird wöchentlich geprüft, dass entsprechende Updates eingespielt sind. Zusätzlich bekommen Systemadministratoren Warn-Hinweise, wenn Updates ausstehend sind.	Klare Schlüsselregelung, in der beschrieben wird, wer wozu Zugang hat.
	Langjährige vertrauenswürdige Partner im Bereich Sicherheit und Hygiene, mit welchen geprüfte AV-Verträge bestehen

1.3. Zugriffskontrolle

Maßnahmen, die sicherstellen sollen, dass die Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Die Vorgaben der Passwort-Richtlinien folgen den Empfehlungen des BSI, Einstellungen nach Privacy-by-Default	Die Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Die strengen Systemvoreinstellungen zwingen zu einer hohen Passwortkomplexität. Passwörter werden nicht gespeichert. Mitarbeiter müssen beim erstmaligen Anmelden ihr Passwort ändern.
Die Richtlinien der Domäne stellen sicher, dass Passwörter regelmäßig geändert werden.	Schulung und Sensibilisierung der Mitarbeiter. Einweisungen und regelmäßige Schulungen zu den verwendeten Geräten
Datenschutzkonforme & sicheres Disk-Wiping von deprovisionierten Servern	Die IT-Abteilung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur
Verschlüsselung von mobilen Datenträgern und Endgeräten (Bitlocker, Kaspersky Enterprise Endpoint Security Encryption)	Mitarbeiter haben nur Zugriff auf die für sie relevanten Systeme
API-Endpoints sind zugriffsgeschützt und exponieren keine vertraulichen Informationen	Protokoll-Zugriff ist nur ausgewählten Mitarbeitern möglich.
	Zugriffs-Minimierung: Anzahl der Administratoren ist möglich gering
	Vernichtung von Datenträgern (Entsorgung von Akten & Laufwerken) durch zertifizierte Dienstleister gegen Vernichtungszertifikat

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Systeme sind anhand Ihrer Nutzungsprofile voneinander getrennt und autark. Insb. bei Visavid findet eine physikalische Trennung statt. Der Server, über den ein Videoraum abgewickelt wird, ist strikt von der Nutzer- und Raum-Datenbank getrennt.	Selektive Rechtevergabe verhindert übergreifenden Zugriff
Metriken zur Nutzung von Visavid werden in separaten Systemen erhoben, dabei jedoch bereits komplett anonymisiert oder ohne Personenbezug.	

2. Pseudonymisierung und Verschlüsselung nach Art. 32 Abs. 1 lit. a DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**
Videokonferenz: Daten-Streams sind mittels Datagram Transport Layer Security (DTLS) und Media-Streams (Audio- und Video-Übertragung) sind mittels Secure Real-time Transport Protocol (SRTP) verschlüsselt. DTLS ist über die Browser implementiert und orientiert sich an TLS. Web-Applikation: Jeglicher Traffic wird über HTTPS geleitet. Dort wird insbesondere darauf geachtet, dass aktuelle und sichere Cipher-Suites genutzt werden.	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt gemacht. Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogene Webschulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten. Auf die Besonderheiten im Umgang mit pseudonymisierten Daten wurde hingewiesen.
Das Passwort der berechtigten Personen wird mittels BCrypt als Hash abgelegt.	
E-Mails werden verschlüsselt, soweit dies die Gegenstelle unterstützt (S/MIME)	
Metriken zur Nutzung von Visavid werden entweder komplett anonymisiert, pseudonymisiert oder ohne Personenbezug erhoben.	

3. Datenminimierung
Die Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO wird durch ein Löschkonzept gewährleistet.
4. Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

4.1. Weitergabekontrolle

Maßnahmen, die garantieren, dass personenbezogene Daten nicht unberechtigt verarbeitet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Personenbezogene Daten werden mit einer Transportverschlüsselung übertragen	Es werden keine personenbezogenen Daten der Auftragnehmer weitergegeben.
	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.
	Unberechtigter Abfluss kann mangels Zugriffsmöglichkeiten Dritter ausgeschlossen werden, siehe Rechtevergabe.

4.2. Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich geprüft werden kann, ob und vom wem Daten verarbeitet wurden

Technische Maßnahmen	**Organisatorische Maßnahmen**
Bei Datenverarbeitung wird anhand des Rollen- & Rechtekonzepts geprüft, ob die Verarbeitung legitim ist.	Das Rollen- & Rechtekonzept (mit unterschiedlichen Berechtigungsstufen) verhindert, dass unberechtigt Daten verarbeitet werden.
Sichergestellte Löschung und Sperrung personenbezogener Daten nach Ende der jeweiligen Aufbewahrungsfrist.	Sämtliche Unterauftragnehmer unterliegen den gleichen Vorgaben wie der Auftragnehmer. Entsprechende Verträge sind geschlossen. Die Pflichten zur Überprüfung der Unterauftragnehmer übernimmt der Datenschutzbeauftrage des Unternehmens. Er ist auch bei der Auswahl der beauftragten Firmen maßgeblich beteiligt.
Das Protokoll-System protokolliert alle Änderungen (CRUD) der berechtigten Nutzer	Die Eingabekontrolle orientiert sich an dem vorgegebenen Rechtekonzept. Berechtigte Nutzer erhalten aufgrund individueller Benutzerzugänge Zugang zum System und können dort entsprechend Ihrer Zugriffsberechtigung Eingaben tätigen.

5. Verfügbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**
Gesicherte Daten sind räumlich getrennt von Produktivdaten	Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor der Entsorgung
Ständig aktuelle Virenscanner und Spamfilter finden Einsatz. Die Systeme werden regelmäßig aktualisiert.	
Die personenbezogenen Daten eines Betroffenen (Auskunftspflicht) können auf Anfrage in einem gängigen Format exportiert werden.	

6. Belastbarkeit gem. Art 32 Abs. 1 lit. b DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**
Monitoring des Gesamtzustands des Systems, insb. hinsichtlich Auslastung, Sicherheitsvorfälle, Fehlerfälle	Weiterbildung und Ausbildung der Mitarbeiter hinsichtlich Resilienz von großen, komplexen Systemen
Puffersystem, um Lastspitzen ausgleichen zu können	Alle 12 Monate wird ein PenTest von einem spezialisierten und zertifizierten Unternehmen durchgeführt.
Regelmäßige automatisierte Sicherheitstests (Prüfung der Cipher-Suites, Web-Crawler, die die öffentlichen API-Endpoints und Webserver auf Sicherheitslücken prüfen)	
„Self-Healing“, abgestürzte Prozesse/Server werden automatisch ersetzt und geprüft, um eine Wiederholung zu vermeiden	

7. Wiederherstellung gem. Art. 32 Abs. 1 lit. c DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**
Automatisierte Durchführung relevanter Daten und manuelle Prüfung und Sichtung der Backups	Reaktionszeit und Verfügbarkeit des Supports gemäß EVB-IT-Vertrag

8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO

Technische Maßnahmen	**Organisatorische Maßnahmen**
Anfragen und Probleme werden mittels einer Telefonhotline oder eines Ticketsystems (Erreichbar per E-Mail) angenommen.	Der externe Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.
Ein separates Incident-System delegiert Vorfälle automatisch an die passenden Mitarbeiter, die entsprechend der Eskalationskette ausgewählt werden.	Das System nutzt datenschutzfreundliche Voreinstellungen und verzichtet auf Vorbelegungen von Haken.

Anlage 2 - Liste der Subunternehmer (weitere Auftragsverarbeiter)

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer (weitere Auftragsverarbeiter) im Sinne der Nr. 6.4 der Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 DSGVO.

Firma/Adresse	**Kontaktdaten/Ansprechpartner**	**Leistung**
Proact Deutschland GmbH Südwestpark 43 90449 Nürnberg Germany https://proact.de	Andreas Schmitt Telefon: 0911 30999-0 info@proact.de	Linux-Administration, Betreuung und Beratung auf fachlicher Ebene, Bereitstellung Rechenzentrum-Services
OVH GmbH St. Johanner-Str. 41-43 66111 Saarbrücken https://ovh.de	Jonas Metz Telefon: 0681 906730 kundendienst@ovh.de	Bereitstellung Rechenzentrum-Services (z.B. Bereitstellung Server)
Hetzner Online GmbH Sigmundstrasse 135 90431 Nürnberg https://hetzner.de	Michael Hertlein Telefon: 09831 505-0 info@hetzner.com	Bereitstellung Rechenzentrum-Services (z.B. Bereitstellung Server)
bkd GmbH Hubertusstr. 44 45657 Recklinghausen https://bkd.de	Ulrich Braukmann Telefon: 02361 9175-0 dialog@bkd.de	Call-Center für First-Level-Support
dtms GmbH Taunusstrasse 57 55118 Mainz https://www.dtms.de	Philipp Duile Telefon: 06131/4646000 info@dtms.de	Bereitstellung VOIP-Interconnect für Telefon-Einwahl
LEIBOLD Sicherheits- & Informationstechnik GmbH Nordring 98 90409 Nürnberg https://www.leibold-it.de	Ramona Karner Telefon: 0911/975592-0 info@leibold-it.de	Bereitstellung Rechenzentrum-Services, Linux-Administration, Betreuung und Beratung auf fachlicher Ebene
SpaceNet AG Joseph-Dollinger-Bogen 14 80807 München https://www.space.net	Stefan Hagen Telefon: 089/32356-0 info@space.net	Bereitstellung Rechenzentrum-Services (z.B. Bereitstellung Server)
Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg https://www.projekt29.de	Thomas Wanjura Telefon: 0941/298693-0 info@projekt29.de	Externer Datenschutz-beauftragter