Auftragsverarbeitungsvertrag
Gemäß Art. 28 Abs. 3 S. 1 DSGVO – nachstehend bezeichnet als AV-Vertrag

Zwischen

Musterschule Musterstraße 1200 Musterstadt

nachstehend bezeichnet als **Auftraggeber** und

Cucua Einzelunternehmen Große Kapellenstraße 43 67105 Schifferstadt Deutschland

nachstehend bezeichnet als **Auftragnehmer.** Auftragnehmer und Auftraggeber werden nachstehend auch als **Vertragsparteien** bezeichnet.

Erstellt und unterzeichnet vom Auftragnehmer: _____

Weisungsberechtigte Person des Auftragnehmers: Annette Pitters

Schifferstadt am: _____

Unterzeichnet vom Auftraggeber: _____

Weisungsberechtigte Person des Auftraggebers: _____

Ort und Datum: _____

Hiermit bestätige ich als Vertreter des Auftraggebers, dass ich die Seiten 1 bis xxx der Auftragsdatenvereinbarung gelesen und verstanden habe und damit einverstanden bin.

Vertreten durch: _____, _____

Name Auftraggeber Stempel und Unterschrift Auftraggeber

Bitte unterschreiben Sie dieses Dokument und senden Sie es uns per Email zu. Alle Weisungen sollten schriftlich an annette.pitters@cucua.co erfolgen.

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

In diesem Vertrag verwendete Begriffe, die in Art. 4, 9 und 10 DS-GVO definiert werden, sind im Sinne dieser gesetzlichen Definition zu verstehen.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber folgende Leistungen: Bereitstellung einer cloudbasierten Testplattform.

Grundlage dieser Leistungserbringung ist der Hauptvertrag vom („Dienstleistungsvertrag“). Dieser Vertrag beginnt am Unterzeichnungsdatum. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag und der nachfolgenden Leistungsbeschreibung:

Leistungsbeschreibung zu Art, Umfang und Zweck der Datenverarbeitung

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

a) Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

Die Art der Verarbeitung umfasst alle Formen der Verarbeitung i.S.v. Art. 4 Nr. 2 DSGVO, die zur Bereitstellung der Cucua Platform und damit zur Erreichung der vereinbarten Vertragszwecke erforderlich sind. Dies beinhaltet die Speicherung (bzw. Löschung) persönlicher Identifikationsmerkmale (Vor- und Nachname, E-Mail-Adresse, Name der Einrichtung, Land, Stadt) im Rahmen der Erstellung (bzw. Löschung) von Benutzeraccounts. Die Anmeldung erfolgt durch personenbezogene Benutzeraccounts (Benutzername und Passwort).

b) Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS- GVO):

Profildaten:

- Vor- / Nachname
- Email-Adresse
- Standort (Stadt / Land)
- Interessen und Expertise
- Berufliche und akademische Erfahrung
- Profilbild
- Profilbeschreibung

Inhaltsdaten:

- z.B. Texteingaben, Fotografien, Videos

Benutzerdaten:

- Nutzername
- Passwort

Zugriffsdaten:

- IP-Adresse
- Datum und Uhrzeit der Anfrage
- Meldung über erfolgreichen Abruf

Optionale / funktionsabhängige Daten

- Telefonnummer
- Standort- oder Adressangaben
- Profilbild und Profilbeschreibung
- Interessen, Expertise sowie berufliche oder akademische Angaben
- Eltern- bzw. Erziehungsberechtigtendaten, soweit für Schülerkonten oder Einwilligungsprozesse erforderlich
- Inhaltsdaten, z.B. Texteingaben, hochgeladene Dateien, Fotografien, Videos, Audio- oder Dokumenteninhalte
- KI-bezogene Eingaben und Ausgaben, soweit KI-Funktionen genutzt werden
- Zahlungs- und Abonnementdaten, soweit kostenpflichtige Funktionen genutzt werden
- Benachrichtigungs- und Gerätedaten, soweit entsprechende Funktionen genutzt werden

Besondere Kategorien:

Personenbezogene Daten gemäß Art. 9 Abs. 1 DS-GVO werden nur mit der ausdrücklichen Einwilligung der betroffenen Person gemäß Art. 9 Abs. 2 DS-GVO verarbeitet.

c) Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

Mitarbeiter*innen des Auftragnehmers, Schüler des Auftragnehmers.

d) Zweck der Datenverarbeitung:

Zweck der Verarbeitung ist die Bereitstellung einer cloudbasierten Testerstellungs und Testkorrekturplattform mit dem Ziel, Leistungsüberprüfungen zu erstellen und durchzuführen.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.

(5) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

(6) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Vertragsraum (Beschluss 94/1/EG) statt. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Schriftform oder dokumentiertem elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 3 Weisungsrecht

(1) Der Auftraggeber ist als Verantwortlicher gem. Art. 4 Nr. 7 DS-GVO für die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere für die Auswahl des Auftragnehmers, die an diesen übermittelten Daten sowie erteilte Weisungen verantwortlich (Art. 28 Abs. 3 lit. a, 29 u. 32 Abs. 4 DS-GVO).

(2) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren

Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(3) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus dem Hauptvertrag. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(4) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer entstehen, bleiben unberührt.

(5) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an 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 und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in **Anlage 1** aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden

Beschäftigte genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Der Auftragnehmer unterstützt den Auftraggeber erforderlichenfalls bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DS-GVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DS-GVO). Meldungen für den Auftraggeber nach Art. 33 oder 34 DS-GVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gem. § 5 dieses Vertrags durchführen.

(5) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren,

dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.

(6) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 6 Abs. 2 dieses Vertrags hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(8) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(9) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DS-GVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

(6) Geht die Duldung und Mitwirkung bei den Kontrollen, bzw. adäquaten Alternativmaßnahmen des Auftraggebers über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem

Fehlverhalten des Auftragnehmers, dann hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.

§ 9 Einsatz von Subunternehmern

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 2** genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich oder in dokumentiertem elektronischen Format zugestimmt hat. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) [falls einschlägig: direkt gegenüber den Subunternehmern] wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln und zusätzlichen Schutzmaßnahmen). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS- GVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

(2) Der Auftragnehmer stellt den Auftraggeber auf erstes Anfordern von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die

DSGVO auferlegten Pflicht oder der Nichtbeachtung oder Verletzung einer vom Auftraggeber in dieser AV- Vereinbarung oder einer gesondert erteilten Anweisung geltend machen.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn/ soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DS-GVO.

(4) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 12 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer sich den Kontrollrechten des Auftraggebers auf vertragswidrige Weise widersetzt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. Im Übrigen bleiben die Verpflichtungen aus diesem AV-Vertrag im Hinblick auf die im Auftrag verarbeiteten Daten auch nach Beendigung des AV-Vertrages bestehen.

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Für alle Streitigkeiten aus diesem Vertrag gilt der gesetzliche Gerichtsstand.

Anlagen:

Anlage 1 – TOM's (Technische und organisatorische Maßnahmen des Auftragnehmers)

Anlage 2 – Genehmigte Subunternehmer inklusive AVV

Anlage 3 – Beschreibung der betroffenen

Personen/Betroffenengruppen/ besonders

schutzbedürftiger Daten/Datenkategorien

Anlage 1 – Technische und organisatorische Maßnahmen des Auftragnehmers

Stand: Mai 2026

Das vorliegende Dokument ergänzt Kapitel 11 der Datenverarbeitungsvereinbarung (DPA) zwischen Auftraggeber und Auftragnehmer gemäß Art. 28 GDPR (EU-Datenschutzgrundverordnung). Die technischen und organisatorischen Maßnahmen werden von Cucua gemäß Art 32 DSGVO umgesetzt. Sie werden von Cucua entsprechend der Machbarkeit und dem Stand der Technik kontinuierlich verbessert.

1. Vertraulichkeit

1.1. Logische Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen

- ✓ Anmeldung mit komplexem Benutzernamen und Passwort
- ✓ Antiviren-Software-Server
- ✓ Antiviren-Software-Kunden
- ✓ Firewall
- ✓ Automatische Desktop-Sperre

Organisatorische Maßnahmen

- ✓ Verwaltung von Benutzerrechten
- ✓ Erstellen von Benutzerprofilen
- ✓ Zentrale Passwortvergabe
- ✓ Politik der Informationssicherheit

1.2. Berechtigungskontrolle

Maßnahmen, die sicherstellen, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten während der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen

- ✓ Aktenvernichter min. empfohlene Sicherheitsstufe P-4 (DIN 66399)
- ✓ SSH-verschlüsselter Zugang
- ✓ Zertifizierte SSL-Verschlüsselung

Organisatorische Maßnahmen

- ✓ Benutzerdaten werden mit Identifikatoren versehen, um den Zugriff nur für autorisierte Benutzer zu kontrollieren. Die Zugriffsrechte der Benutzer werden auf der Grundlage von Gruppenmitgliedschaften und Berechtigungen verfolgt.
- ✓ Das Prinzip des am wenigsten privilegierten Zugangs wird für das gesamte Personal der Studienzentrale und die Auftragnehmer umgesetzt. Die Sicherheitsgruppe des autorisierten Personals mit Zugang zu Systemen, die Benutzerdaten verarbeiten, wird auf Richtigkeit und ordnungsgemäße Umsetzung in diesen Systemen geprüft. Es gibt On-/Off-Boarding-Prozesse, die entsprechende Änderungen an der Liste der Zugriffsberechtigten vorschreiben.

1.3. Trennungskontrolle

Maßnahmen, die sicherstellen, dass Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können. Dies kann z. B. durch eine logische und physische Trennung der Daten gewährleistet werden.

Technische Maßnahmen

- ✓ Trennung von Produktiv- und Testumgebung
- ✓ Physische Trennung (Systeme / Datenbanken / Datenträger)
- ✓ Mehrmandantenfähigkeit von relevanten Anwendungen
- ✓ Staging von Entwicklungs-, Test- und Produktionsumgebung
- ✓ Führung einer Liste der Daten und des Bestandsverzeichnisses der Speicherung und Verarbeitung personenbezogener Daten für alle Systeme

Organisatorische Maßnahmen

- ✓ Steuerung über Berechtigungskonzept
- ✓ Festlegung der Datenbankrechte
- ✓ Politik der Informationssicherheit

- ✓ Datenschutzpolitik
- ✓ Datenbank- und Code-Repository-Rechte

2. Integrität

2.1. Übertragungskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten während der elektronischen Übermittlung oder während des Transports oder der Speicherung auf Datenträgern nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können und dass es möglich ist, zu überprüfen und festzustellen, an welche Stellen personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden sollen.

Technische Maßnahmen

- ✓ Verwendung von VPN
- ✓ Bereitstellung über verschlüsselte Verbindungen wie sftp, https und sicheren Cloud-Speicher
- ✓ Einsatz von Signaturverfahren (fallabhängig)

Organisatorische Maßnahmen

- ✓ Übersicht über regelmäßige Abruf- und Übermittlungsverfahren
- ✓ Übermittlung in anonymisierter oder pseudonymisierter Form

3. Verfügbarkeit und Ausfallsicherheit

3.1. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (USV, Klimatisierung, Brandschutz, Datensicherung, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid-Systeme, Plattenspiegelung usw.).

Organisatorische Maßnahmen

- ✓ Sicherungskonzept
- ✓ Vorhandensein eines Notfallplans
- ✓ Aufbewahrung von Sicherungsmedien an einem sicheren Ort an mehreren Standorten

3.2. Kontrolle der Verwertbarkeit

Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit von und des Zugangs zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls.

Technische Maßnahmen

- ✓ Backup-Überwachung und Berichterstattung
- ✓ Wiederherstellbarkeit durch Automatisierungswerkzeuge
- ✓ Backup-Konzept nach Kritikalität und Kundenvorgaben

Organisatorische Maßnahmen

- ✓ Verwertungskonzept
- ✓ Kontrolle des Sicherungsprozesses
- ✓ Regelmäßige Tests der Datenwiederherstellung und Protokollierung der Ergebnisse
- ✓ Vorhandensein eines Notfallplans

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Management

Technische Maßnahmen

- ✓ Zentrale Dokumentation aller datenschutzrechtlichen Bestimmungen mit Zugang für Mitarbeiter
- ✓ Datenschutz-Checkpoints konsequent in toolgestützter Risikobewertung umgesetzt

Organisatorische Maßnahmen

- ✓ Externer Datenschutzbeauftragter benannt
- ✓ Geschultes und zur Vertraulichkeit/zum Datengeheimnis verpflichtetes Personal
- ✓ Prozesse bezüglich der Informationspflichten gemäß Art. 13 und 14 GDPR eingerichtet
- ✓ Formalisiertes Verfahren für Auskunftsersuchen von betroffenen Personen ist vorhanden
- ✓ Datenschutzaspekte als Teil des unternehmerischen Risikomanagements etabliert

4.2. Management der Reaktion auf Vorfälle

Unterstützung bei der Reaktion auf Sicherheitsverletzungen und bei der Bearbeitung von Datenverletzungen.

Technische Maßnahmen

- ✓ Einsatz einer Firewall und regelmäßige Aktualisierung
- ✓ Einsatz eines Spam-Filters und regelmäßige Aktualisierung
- ✓ Einsatz von Virenscannern und regelmäßige Aktualisierung

Organisatorische Maßnahmen

- ✓ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenverletzungen (auch im Hinblick auf die Meldepflicht an die Aufsichtsbehörde)
- ✓ Formalisiertes Verfahren für den Umgang mit Sicherheitsvorfällen
- ✓ Dokumentation von Sicherheitsvorfällen und Datenschutzverletzungen über ein Ticketsystem
- ✓ Ein formelles Verfahren zur Weiterverfolgung von Sicherheitsvorfällen und Datenschutzverletzungen

4.3. Datenschutz durch Technik und durch Voreinstellungen

Maßnahmen gemäß Artikel 25 DSGVO, die den Grundsätzen des Datenschutzes durch Technik und durch Voreinstellungen entsprechen.

Technische Maßnahmen

- ✓ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- ✓ Verwendung von datenschutzfreundlichen Voreinstellungen in Standard- und Individualsoftware

Organisatorische Maßnahmen

- ✓ Datenschutzpolitik (einschließlich der Grundsätze "Datenschutz durch Technik / durch Voreinstellungen")

4.4. Auftragskontrolle (Outsourcing, Unterauftragnehmer und Auftragsabwicklung)

Maßnahmen, die sicherstellen, dass personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, nur gemäß den Anweisungen des Kunden verarbeitet werden können.

Technische Maßnahmen

- ✓ Überwachung des Fernzugriffs durch Externe, z. B. im Rahmen des Fernsupports
- ✓ Überwachung von Unterauftragnehmern nach den Grundsätzen und mit den Technologien gemäß den vorangegangenen Kapiteln 1, 2
- ✓ Sicherstellung der Löschung von Daten nach Beendigung des Vertrags

Organisatorische Maßnahmen

- ✓ Vorherige Überprüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und ihrer Dokumentation
- ✓ Auswahl des Auftragnehmers unter Due-Diligence-Aspekten (insbesondere im Hinblick auf Datenschutz und Datensicherheit)
- ✓ Abschluss der erforderlichen Datenverarbeitungsvereinbarung zur Auftragsverarbeitung oder EU-Standardvertragsklauseln

- ✓ Rahmenvereinbarung über die Auftragsdatenverarbeitung innerhalb der Unternehmensgruppe
- ✓ Schriftliche Anweisungen an den Auftragnehmer
- ✓ Verpflichtung der Mitarbeiter des Auftragnehmers zur Wahrung des Datengeheimnisses
- ✓ Vereinbarung über wirksame Kontrollrechte gegenüber dem Auftragnehmer

Anlage 2 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 9:

Firma und Anschrift des Subunternehmers	**Art der Leistung**	**Land der erbrachten Leistung (Speicherort)**
Hostinger International Ltd., 61 Lordou Vironos Street, 6023 Larnaca, Zypern	Infrastructure as a Service; VPS Hosting	Deutschland
DigitalOcean, LLC, 101 Avenue of the Americas, 10th Floor, New York, NY 10013, USA	Software as a Service; Managed Database Hosting; Object Storage / S3-kompatibler Speicher	Deutschland
OpenRouter, LLC, 169 Madison Avenue, Suite 2404, New York, NY 10016, United States	Software as a Service; Vermittlung und Verarbeitung von KI-/LLM-Anfragen	Europäische Union

Anlage 3 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

- Schüler
- Lehrer und Lehrpersonal
- Weitere Angestellte des Lehrinstituts (Verwaltung; IT)