

**Vertrag
über die Verarbeitung personenbezogener
Daten im Auftrag („AVV“)**

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

- (a) Mit diesem Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (im Folgenden „AVV“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO) sichergestellt werden.
- (b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.
- (c) Diese AVV gilt für die Verarbeitung personenbezogener Daten gemäß Anhang II.
- (d) Die Anhänge I bis IV sind Bestandteil der Klauseln.
- (e) Diese AVV gilt unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.
- (f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

- a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
- b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

- (a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- (b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.
- (c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5

Kopplungsklausel

- a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
- b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
- c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II

PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1. Weisungen

- (a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

- (b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

- (a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
- (b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogener Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

- (a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- (b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- (c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden

Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

- (d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- (e) Die Parteien stellen der/ den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

- (a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind (Anhang IV). Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens sieben Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.
- (b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.
- (c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- (d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten, gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

7.8. Internationale Datenübermittlungen

- (a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.
- (b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen

können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

- (a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
- (b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- (c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:
 - (1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
 - (2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
 - (3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
 - (4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
- (d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

- (a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
- (b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
 - (1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - (2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - (3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und sofern nicht alle diese Informationen zur selben Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

- (c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- (a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- (b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- (c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und sofern nicht alle diese Informationen zur selben Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III
SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

- (a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- (b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 - (1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 - (2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;
 - (3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.
- (c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.
- (d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Klausel 11

Haftung

- (a) Der Auftragsverarbeiter haftet für die ordnungsgemäße Ausführung dieses AVV dem Grunde nach den gesetzlichen Bestimmungen, insbesondere nach Art. 82 Abs. 2 DS-GVO. Machen betroffene Personen Ansprüche gegenüber dem Verantwortlichen wegen unzulässiger oder unrichtiger Datenverarbeitung geltend, so wird der Auftragsverarbeiter den Verantwortlichen unterstützen und darlegen, dass der Auftragsverarbeiter seinen speziell als Auftragsverarbeiter auferlegten Pflichten gemäß der DS-GVO bei der Datenverarbeitung nachgekommen ist oder unter Beachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder nicht gegen diese Anweisungen gehandelt hat.
- (b) Etwaige Haftungsbeschränkungen aus einem ggf. geschlossenen Hauptvertrag, den Allgemeinen Geschäftsbedingungen (AGB) für die Nutzung der Online-Lernplattform oder den übrigen Anhängen zu dem Hauptvertrag finden auf diesen Vertrag Anwendung.

ANHANG I

Liste der Parteien

Verantwortlicher

	Name und Anschrift	Gemäß Kundenangaben innerhalb des Vertrages über Nutzung der Service Online-Lernplattform KI-Kompetenz Akademie zu den Allgemeinen Geschäftsbedingungen der PRICOM („Hauptvertrag“)
	Name, Funktion und Kontaktdaten der Kontaktperson	Gemäß Kundenangaben innerhalb des Hauptvertrags

Auftragsverarbeiter

	Name und Anschrift	MAMS Consulting GmbH Landsberger Str. 155 80687 München
	Name, Funktion und Kontaktdaten der Kontaktperson	Mail: dsb@pri-com.de

Verantwortlicher und Auftragsverarbeiter gemeinsam im Rahmen dieses AVV „die Vertragspartner“ oder „die Parteien“ genannt.

ANHANG II

Beschreibung der Verarbeitung

Gegenstand, Art und Umfang der Verarbeitung	<p>Der Auftragsverarbeiter ist ein u.a. auf Künstliche Intelligenz („KI“) spezialisiertes Beratungsunternehmen, das für den Verantwortlichen eine Software-as-a-Service („SaaS“) Schulungsplattform bereitstellt. Diese Schulungsplattform richtet sich an die Beschäftigten und sonstigen autorisierten Nutzer des Verantwortlichen und dient der Vermittlung essenzieller Kompetenzen im Bereich der Künstlichen Intelligenz.</p> <p>Die Lernumgebung der Plattform bietet den Nutzern die Möglichkeit, fundiertes Wissen über KI-Technologien zu erwerben, mit dem Ziel, ein vertieftes Verständnis der Funktionsweise von KI, ihrer potenziellen Risiken, ethischen Implikationen sowie der einschlägigen regulatorischen Rahmenbedingungen zu entwickeln. Gleichzeitig wird praktisches Wissen über die Entwicklung, Implementierung und den rechtskonformen Einsatz von KI-Systemen vermittelt.</p> <p>Hierfür führt der Auftragsverarbeiter im Auftrag des Verantwortlichen und unter dessen Weisung die folgenden Verarbeitungstätigkeiten durch:</p> <ol style="list-style-type: none"> 1. Hosting, Zurverfügungstellung, Betrieb und Wartung der Schulungsplattform, 2. Benutzerverwaltung einschließlich Benutzerregistrierung und Login, sowie 3. Bereitstellung von technischem Support und Wartungsleistungen. <p>Hierbei werden personenbezogene Daten des Verantwortlichen verarbeitet, insbesondere erhoben, erfasst, geordnet, gespeichert, abgefragt, verwendet, abgeglichen und gelöscht. Der Zugriff des Auftragsverarbeiters auf personenbezogene Daten des Verantwortlichen erfolgt nur in dem Umfang, der zur Erfüllung der oben genannten Zwecke erforderlich ist. Die genannten Verarbeitungstätigkeiten erfolgen ausschließlich in IT-Systemen, die vom Auftragsverarbeiter oder von ihm sorgfältig ausgewählten Unterauftragsverarbeitern bereitgestellt und betrieben werden.</p> <p>Weitere Informationen zum Gegenstand, der Art und dem Zweck der Verarbeitung sind im zugrunde liegenden Hauptvertrages zwischen den Parteien geregelt.</p>
--	---

	Dauer des Auftrags	<p>Dieser Vertrag kommt mit Abschluss des Hauptvertrages durch beide Parteien zustande und läuft auf unbestimmte Zeit. Vorliegender Vertrag ist rechtlich unselbständig und teilt das rechtliche Schicksal des Hauptvertrags.</p> <p>Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Es ist den Parteien bewusst, dass ohne Vorliegen eines gültigen Auftragsverarbeitungsvertrags keine (weitere) Auftragsverarbeitung durchgeführt werden darf.</p> <p>Eine isolierte ordentliche Kündigung dieses Vertrags ist ausgeschlossen.</p>
	Zweck(e) der Verarbeitung	<p>Mit der Datenverarbeitung werden folgende Zwecke verfolgt:</p> <ol style="list-style-type: none"> 1. Primärzweck: Schulung der Nutzer, damit diese über ein ausreichendes Maß an KI-Kompetenz verfügen. Dies umfasst auch <ul style="list-style-type: none"> ○ Förderung der digitalen Kompetenz und Innovationsfähigkeit ○ Verbesserung der Effizienz und Optimierung von Geschäftsprozessen 2. Sekundärzweck: Gewährleistung der Integrität und Sicherheit der Schulungsplattform. Dies umfasst auch: <ul style="list-style-type: none"> ○ Verwaltung von Zugangs-/ Zugriffsrechten auf Informations- und Kommunikationstechnik und Unternehmensnetzwerk ○ Wartung/ Support (Maintenance)
	Datenkategorien, die durch den Auftragsverarbeiter verarbeitet werden	<p>Der Verantwortliche kann die Datenkategorien auswählen, die von den betroffenen Personen angefordert werden, wie z. B.: Daten bezüglich Teilnehmenden der Schulungsinhalte:</p> <ul style="list-style-type: none"> • Beschäftigtenstammdaten (z. B. Name, Vorname, berufliche E-Mailadresse, berufliche Telefonnummer, Berufsbezeichnung, Firmenadresse) • IP-Adresse • Nutzungsdaten (z. B. Beginn, Ende, Umfang der jeweiligen Nutzung) • Endgeräte-Informationen • Nutzerkennungen (z.B. Login-Daten, Benutzername und Passwort) • Antworten der betroffenen Person auf Freitextfragen • Antworten der betroffenen Person auf Dropdown-Fragen • Weitere Daten: Informationen, die im Checkout-Prozess abgefragt werden.

		<p>Daneben können die betroffenen Personen selbst personenbezogene Daten verarbeiten, indem sie auf die erstellten Inhalte zugreifen und diese nutzen, wie z. B.:</p> <ul style="list-style-type: none"> • Testergebnisse • Prüfungsergebnisse • dem System hinzugefügte Kommentare • Zertifizierungsdokumente
	Betroffene Personen	Durch den Verantwortlichen ausgewählte Beschäftigte und sonstige Nutzer der Online-Schulung
	Datenempfänger	<p>Im Rahmen der Auftragsverarbeitung können die personenbezogenen Daten durch folgende Kategorien von Empfängern verarbeitet werden:</p> <ul style="list-style-type: none"> • Unterauftragsverarbeiter des (vgl. Anhang IV)
	Speicherort	Deutschland
	Standorte, von denen aus auf die Daten des Verantwortlichen zugegriffen werden kann	Deutschland und EU/EWR
	Datenlöschung	<p>Die Daten des Verantwortlichen werden gelöscht, wenn sie für die Durchführung des Auftrags nicht mehr erforderlich sind, es sei denn es liegt eine abweichende Weisung des Verantwortlichen vor. Das bedeutet, dass Daten in unseren Systemen vernichtet oder gelöscht werden, sobald sie nicht länger benötigt werden. Es werden angemessene Maßnahmen ergriffen, um sicherzustellen, dass Ihre personenbezogenen Daten nur unter den folgenden Voraussetzungen verarbeitet werden:</p> <ol style="list-style-type: none"> 1. Für die Dauer, die die Daten verwendet werden, um den Dienst bereitzustellen 2. Wie laut geltendem Recht, Vertrag oder im Hinblick auf unsere gesetzlichen Verpflichtungen erforderlich 3. Nur so lange, wie es für den Zweck notwendig ist, zu dem die Daten erfasst wurden, oder länger, wenn dies aus Vertrag, geltendem Recht erforderlich ist, unter Anwendung angemessener Schutzmaßnahmen. <p>Ein Erfordernis kann insbesondere dann bestehen, wenn die Daten noch benötigt werden, um vertragliche Leistungen zu erfüllen, Gewährleistungs- und ggf. Garantiesprüche prüfen und gewähren oder abwehren zu können. Sind die Daten für die Erfüllung vertraglicher oder gesetzlicher Pflichten nicht mehr erforderlich, werden sie regelmäßig gelöscht, soweit nicht ihre - befristete -</p>

		<p>Aufbewahrung weiterhin notwendig ist, insbesondere zur Erfüllung gesetzlicher Aufbewahrungsfristen von bis zu zehn Jahren (u.a. aus dem Handelsgesetzbuch, der Abgabenordnung und dem Geldwäschegesetz). Im Falle von gesetzlichen Aufbewahrungspflichten kommt eine Löschung erst nach Ablauf der jeweiligen Aufbewahrungspflicht in Betracht</p> <p>Nach Beendigung dieses Vertrags sind die Daten des Verantwortlichen unverzüglich zu löschen.</p>
--	--	---

ANHANG III

Technische und organisatorische Maßnahmen des Auftragsverarbeiters

1. Zutrittskontrolle		
	<p>Zur Gewährleistung der physischen Sicherheit der Datenverarbeitung sind folgende Maßnahmen zur Zutrittskontrolle implementiert worden, welche sicherstellen, dass unbefugten Personen der Zugang zu Systemen, Datenverarbeitungsanlagen und Verfahren, in denen personenbezogene Daten verarbeitet werden, verwehrt bleibt.</p>	<ul style="list-style-type: none"> - Schlüsselverwaltung / Dokumentation der Schlüsselvergabe - Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/Chipkarten) - Empfangskraft - Sicherheitstüren - Türsicherungen - Alarmanlage - sicherheitstechnische Maßnahmen zur Absicherung des Serverraums - Sonstiges:
2. Zugangskontrolle		
	<p>Zur Sicherstellung der Vertraulichkeit personenbezogener Daten sind unternehmensseitig Maßnahmen der Zugangskontrolle implementiert worden, die gewährleisten, dass ein unbefugter Zugriff auf Datenverarbeitungssysteme wirksam verhindert wird.</p>	<ul style="list-style-type: none"> - Jede berechnigte Nutzerperson verfügt über einen eindeutigen, personenbezogenen Identifikator - Verwendung individueller, voneinander getrennter Benutzerkennungen für privilegierte Zugriffsrechte - Benutzerkennungen werden nach dem Ausscheiden der jeweiligen Nutzer aus dem Unternehmen unverzüglich deaktiviert oder gelöscht, um einen unbefugten Zugriff auf die Systeme auszuschließen - Passwörter werden grundsätzlich weder im Klartext gespeichert noch unverschlüsselt übertragen; vielmehr erfolgt deren Verarbeitung ausschließlich in verschlüsselter bzw. pseudonymisierter Form - Sichere Passwortverfahren - Einsatz einer Zwei-Faktor-Authentifizierung zur Absicherung des Zugriffs auf sicherheitskritische Anwendungen - Automatisierte Sperrmechanismen der Client-Systeme nach Ablauf einer definierten Inaktivitätszeitspanne ohne Benutzeraktivität - Regelmäßige Durchführung von Softwareaktualisierungen - Nutzung von Firewalls zur Überwachung und Sicherung der Netzwerkinfrastruktur
3. Zugriffskontrolle		
	<p>Im Rahmen der Zugriffskontrolle werden Maßnahmen ergriffen, die sicherstellen, dass ausschließlich berechnigte Personen Zugang zu den Datenverarbeitungssystemen erhalten und lediglich auf die Daten zugreifen können, für die sie eine entsprechende Zugriffsberechtigung besitzen, sodass eine unbefugte Einsichtnahme, Kopierung, Veränderung oder Entfernung personenbezogener</p>	<ul style="list-style-type: none"> - Erfassung und Dokumentation der für den Auftrag relevanten Werte - Angemessene Berechnigungskonzepte, einschließlich der Dokumentation von Verantwortlichkeiten, aufgabenbezogenen Profilen sowie Rollen und Rollenkonzepten - Vorhandensein und Einhaltung eines Benutzermanagementprozesses einschließlich eines formellen Genehmigungsverfahrens - Regelmäßige Überprüfung der Aktualität und Angemessenheit von Zugriffsrechten

	Daten während der Verarbeitung ausgeschlossen ist.	
4. Weitergabekontrolle		
	Es werden folgende Maßnahmen zur Weitergabekontrolle ergriffen, die sicherstellen, dass personenbezogene Daten während der elektronischen Übertragung, des Transports oder der Speicherung auf Datenträgern vor unbefugtem Zugriff, Kopieren, Veränderung oder Entfernung geschützt sind, und dass jederzeit überprüft und nachvollzogen werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	<ul style="list-style-type: none"> - Verschlüsselung - Verwendung gesicherter und verschlüsselter WLAN- sowie Internetnetzwerke - SSL-/TLS-Verschlüsselung - Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops - Verwaltung kryptographischer Schlüssel - Richtlinie für eine aufgeräumte Arbeitsumgebung (z.B. Clean-Desk-Policy) - Vorschriften zur Vernichtung bzw. Zerstörung von Datenträgern - Durchführung einer sicheren und vollständigen Löschung
5. Eingabekontrolle		
	Wir garantieren folgende Maßnahmen zur Eingabekontrolle, um sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	<ul style="list-style-type: none"> - Erfassung und Dokumentation der für den Auftrag relevanten Daten - Es bestehen Berechtigungskonzepte, die die Dokumentation der funktionalen Verantwortlichkeiten, die Anwendung des Need-to-know-Prinzips sowie eine angemessene Funktionstrennung umfassen
6. Auftragskontrolle		
	Im Rahmen der vertraglichen Vereinbarungen und zur Gewährleistung der Einhaltung der datenschutzrechtlichen Anforderungen wurden folgende Maßnahmen zur Auftragskontrolle implementiert, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, ausschließlich in Übereinstimmung mit den Weisungen des Verantwortlichen verarbeitet werden	<ul style="list-style-type: none"> - Es bestehen verbindliche Sicherheitsrichtlinien, die auch klare Verpflichtungen für die Beschäftigten enthalten - Schulungen für alle zugriffsberechtigten Mitarbeiter, einschließlich regelmäßig durchgeführter Auffrischungs- und Nachschulungen - Verpflichtung der Beschäftigten zur Wahrung der Vertraulichkeit personenbezogener Daten - Überwachung und Berichterstattung hinsichtlich neu identifizierter Risiken und Schwachstellen - Verbot der Installation nicht autorisierter Software oder Applikationen auf den Endgeräten - Trennung von Entwicklungs- und "Live-Umgebung" - Verbindliche Vorgaben für die sichere Entwicklung von Software und Systemen, die konsequent angewendet und regelmäßig überprüft werden - Implementierung eines „Need-to-Know“-Prinzips für den Zugriff auf die Schulungsumgebung
7. Verfügbarkeitskontrolle		
		<ul style="list-style-type: none"> - Bestehen von Service-Level-Agreements (SLAs) mit Dienstleistern - Backup Verfahren inkl. Sicherer Aufbewahrung der Backups - Viren-/Schadcodeschutz

		- Pläne für den Ausfall, Notfallmanagement und Wiederherstellung einzelner Komponenten sowie für deren Wiederanlauf
8. Trennung von Daten		
	Im Hinblick auf die Einhaltung des Trennungsgebots wurden folgende Maßnahmen implementiert, die sicherstellen, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, strikt getrennt verarbeitet und gegebenenfalls gelöscht werden können, um einer unzulässigen Zweckübergreifenden Nutzung entgegenzuwirken.	<ul style="list-style-type: none"> - Trennung der verwendeten Systeme - Trennung der Datenbanken - Trennung der Zugriffsregelungen
9. Informationssicherheitsvorfälle		
	Mit Blick auf die Sicherstellung einer ordnungsgemäßen und rechtzeitigen Reaktion auf Informationssicherheitsvorfälle und Krisensituationen wurden folgende umfassende Maßnahmen ergriffen und klare Verantwortlichkeiten festgelegt.	<ul style="list-style-type: none"> - Managementprozess für Informationssicherheitsvorfälle bzw. Krisensituationen (Datenschutz und Informationssicherheit) - Definition der Sicherheitsanforderungen in Krisensituation / im Notfall - Übergreifender Notfallplan inkl. regelmäßiger Aktualisierung
10. Aufzeichnung, Erfassung und Dokumentation		
	Im Rahmen der unternehmensinternen Sicherheitsvorkehrungen wurden folgende Maßnahmen in den relevanten Bereichen implementiert, um eine ordnungsgemäße Nachvollziehbarkeit und Überwachung der Systemaktivitäten sicherzustellen.	<ul style="list-style-type: none"> - Nutzung von Sicherheits-/Protokollierungssoftware - Verarbeitung der Daten in Übereinstimmung mit geltenden gesetzlichen Bestimmungen für die Informationssicherheit - Logs sind gegen einen unberechtigten Zugriff geschützt (Vertraulichkeit) - Logs sind vor unberechtigter Veränderung geschützt (Integrität) - Logs sind vor Verlust geschützt (Verfügbarkeit) - Es wird ein Logging der Datenweitergabe übernommen und es findet eine Überprüfung der Logfiles statt (Weitergabekontrolle) - Systemseitiges Logging von Eingaben (Eingabekontrolle) - Regelmäßige Überwachung der Systeme und Logfiles (Verfügbarkeitskontrolle) - Logging der Zugänge (Zugangskontrolle) - Logging der Zugriffe (Zugriffskontrolle)
11. Sonstige Maßnahmen		
	Best Practice Sicherheitsmaßnahmen	<ul style="list-style-type: none"> - Beachtung und Einhaltung von "Best Practice Sicherheitsmaßnahmen" - Dokumentation der technischen und organisatorischen Maßnahmen - Vorhandene Datenschutzrichtlinien - Besondere (Arbeits-) Anweisungen bzgl. Home-Office bzw. Arbeiten außerhalb der normalen Betriebsstätte - Zwei-Faktor-Authentifizierung

ANHANG IV

Liste der Unterauftragsverarbeiter

Der Verantwortliche genehmigt hiermit dem Auftragsverarbeiter die Inanspruchnahme folgender Unterauftragsverarbeiter:

UNTERAUFTRAGS- VERARBEITER	BESCHREIBUNG DER TÄTIGKEIT	VERTRAG ZUR UNTER- AUFTRAGSVERARBEITUNG
Easy LMS B.V. Oude Delft 48 2611 CD Delft Niederlande info@Easy- Lms.Com	Plattformbereitstellung - Easy LMS bietet die Learning-Management-Plattform an. Diese Plattform ermöglicht es uns, die Schulungsinhalte zu erstellen, zu verwalten und zu verteilen. Geografischer Serverstandort: Frankfurt, Deutschland	Ja (Vereinbarung gemäß Art. 28 Abs. 4 DSGVO besteht)
Webmansion GmbH, Halbergstr. 4, 66121 Saarbrücken	Hosting und Wartung CMS & Server inkl. laufender Systempflege	Ja (Vereinbarung gemäß Art. 28 Abs. 4 DSGVO besteht)