Vereinbarung zur Auftragsverarbeitung

zwischen

<Name Organisation/Unternehmen>, <Name Verantworlicher/Vertretungsberechtigter>, <Straße Hausnnummer>, <Postleitzahl Ort>

- im Folgenden "Auftraggeber/AG" -

und

LE Commsulting GmbH, Nuthestraße 25, 14959 Trebbin

- im Folgenden "Auftragnehmer/AN" -

Hauptvertrag zwischen den Parteien (Gegenstand des Auftrags): Lizenz- und Kooperationsvertrag
Zweck dieser Datenverarbeitungen durch den Auftragnehmer für den Auftraggeber ist es, dem Auftraggeber die Konzeption, Verwaltung, Durchführung und Auswertung von Quizfragen, Karteikarten, Live-Quiz, E-Prüfung zu ermöglichen, wobei die konkrete inhaltliche Ausgestaltung, die Verbreitung und die Durchführung der genannten Funktionen allein von dem Auftraggeber verantwortet und durch entsprechende Konfiguration und Planung vorgegeben werden.

Sitz des AN:
☒ Sitz1: innerhalb des EWR oder einem sicheren Drittland (Art. 45 DSGVO)
☐ Sitz2: sonstiges Drittland

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien von betroffenen Personen:

Art und Zweck der Verarbeitung	Kategorien von betroffenen Personen	Art der personenbezogenen Daten
Erstellung und Verwaltung eines Nutzeraccounts, Technischer Support, Wartung, Fehlersuche	Nutzer (Lehrende)	Logdaten, IP-Adresse, ggf. Daten in Datenbanken, Titel, Anrede, Name, Vorname, Telefonnummer, E-Mail Adresse, Informationen über Accountaktivität, Informationen über Lernendengruppen, Inhalte aus Mitteilungsfeld, Name der Lehreinrichtung/Organisation/Unternehmen, Adresse der Organisation/Lehreinrichtung/Unternehmen, Registrierungsdatum, zugeordnete Edition, Anmeldestatus, Kontaktinformation Lehreinrichtung/Organisation/Unternehmen (u.a. E-Mail, Telefonnmmer, Faxnummer), Bezahlplan, Kommunikationsverläufe (E-Mail & Notizen)
Analyse der Antwortqualität von Usergruppen	Nutzer (Lernende)	Leistungsdaten: Die Analyse erfolgt grundsätzlich anonym. Bei kleinen Usergruppen bzw. Usergruppe n=1 (Einzelperson) ist die Leistung dieser Person zuordenbar.
Analyse der Ergebnisse des Life-Quiz und der E-Prüfung	Nutzer (Lernende)	Nutzername (Anonym oder Klarname) des Teilnehmers, Ergebnisse (richtig/falsch) sind eine Nutzername zuordenbar
Bereitstellung von Statistiken	Nutzer (Lehrende)	Anzahl von Kursen, Quizzen, Fragen, Karteikartenstapeln, Karteikarten, gespielte Fragen, Live Quiz

Verarbeitung von Risikodaten ☐ nein ☒ ja

- große Mengen personenbezogener Daten (> 1000 Datensätze)
- große Anzahl betroffener Personen (> 1000)
- Daten schutzbedürftiger Personen

Für den AN gelten Binding Corporate Rules - Processor (BCR-P) gem. Art. 47 DSGVO
☒ nein ☐ ja

Der AN ist zertifiziert
☒ nein ☐ ja

wenn ja, nach: ☐ ISO 27001: ☐ SOC 2 Typ 2 ☐ Sonstiges:

Subunternehmer des AN:
☐ Es werden keine Subunternehmer eingesetzt
☒ SUB1: innerhalb des EWR oder einem sicheren Drittland (Art. 45 DSGVO)
☐ SUB2: sonstiges Drittland

Subunternehmer des AN (soweit eingesetzt):

Firmenname	Sitz (Land)	Einsatz-/Tätigkeitsbereich	vertreten durch AN für Abschluss der AVV/ SCC zwischen Subunternehmer und AG (ja/nein)
Amazon Web Services (AWS) EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg "z. Hd.: AWS EMEA Legal"	USA, Ort der Verarbeitung: EU (Deutschland)	Der Service des Anbieters wird zur Speicherung der Ergebnisse genutzt, zur Verwaltung der Nutzerkonten der Lehrenden, zur Dateiablage, zur Bereitstellung des Webservers und zum Hosting von Medien.	☒ ja ☐ nein
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland. Kontakt Datenschutz: https://support.google.com/policies/contact/general_privacy_form	USA, Ort der Verarbeitung: EU (Irland)	Der Service des Anbieters wird genutzt, um Statistiken über das Nutzungverhalten zu erhalten sowie für die Bereitstellung von Schulungsvideos auf der Lernplattform.	☒ ja ☐ nein
Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland Kontakt Datenschutz: dpo@stripe.com	EU (Irland)	Abwicklung von Zahlungsdienstleistungen	☒ ja ☐ nein
1&1 IONOS SE, Elgendorfer Str. 57, 56410 Montabaur Kontakt Datenschutz: datenschutz@ionos.de	EU (Deutschland)	Ionos Webmail: E-Mail versenden und empfangen Ionos Domain & Webhosting: Domainregistrierung (.de/.io), Hosting und Veröffentlichung der Homepage auf quizacademy.de	☒ ja ☐ nein

☐ Alternativ:

Die Liste der eingesetzten Subunternehmer sowie deren Einsatz-/Tätigkeitsbereiche

☐ ist abrufbar unter: [Webadresse]

☒ ist beigefügt und bildet einen Teil dieses Formblatts

Die Parteien schließen hiermit die vorliegende Vereinbarung zur Auftragsverarbeitung, bestehend aus:
- dem vorliegenden Formblatt;
- Vereinbarung zur Auftragsverarbeitung (Anlage 1) nebst Anlagen
  (falls S1 angekreuzt wurde oder falls S2 angekreuzt wurde und für den AN BCR-P gelten)
- SCC (Anlage 3) nebst Anlagen
  (falls S2 angekreuzt wurde und für den AN keine BCR-P gelten)

Für den Auftraggeber:

Datum:	_____	_____
Unterschrift:	_____	_____
Name:	_____	_____
Titel:	_____	_____

Für den Auftragnehmer:

Datum:	_____	_____
Unterschrift:	_____	_____
Name:	_____	_____
Titel:	_____	_____

Vereinbarung zur Auftragsverarbeitung

1. Begriffsbestimmungen und Abkürzungen

Zum Zwecke dieser Vereinbarung gelten die Begriffsbestimmungen des Art. 4 DSGVO.
Unsichere Drittländer sind solche, für die ein Angemessenheitsbeschluss im Sinne des Art. 45 DSGVO der EU-Kommission nicht vorliegt.
Die Affiliates des Auftraggebers im Sinne dieser Regelung entsprechen denjenigen des Hauptvertrags.
Die Abkürzung „SCC“ meint die Standardvertragsklauseln Auftragsverarbeiter) gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist.

2. Gegenstand und Dauer der Vereinbarung

Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des im Formblatt genannten Hauptvertrags. Dabei verarbeitet der Auftragnehmer personenbezogene Daten des Auftraggebers und ggf. seiner Gruppengesellschaften („Kundendaten“) im Auftrag und nach dokumentierter Weisung.

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

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

Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und den dazugehörigen Leistungsbeschreibungen) sowie aus dem Formblatt.

4. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Die Weisungen des Auftraggebers werden anfänglich durch den Hauptvertrag und diese Vereinbarung festgelegt und können vom Auftraggeber grundsätzlich in Textform durch Einzelweisungen geändert, ergänzt oder ersetzt werden. Mündlich erteilte Weisungen sind vom Auftraggeber in Textform zu bestätigen.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

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.

6. Anforderungen an Personal

Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der Kundendaten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7. Technische und organisatorische Maßnahmen

Der Auftragnehmer ergreift geeignete technische und organisatorische Maßnahmen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Kundendaten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Kundendaten zu gewährleisten.

Soweit der Auftragnehmer nach den Angaben im Formblatt zertifiziert ist, wird der Auftragnehmer diese, eine vergleichbare oder im Hinblick auf die Anforderungen an technische und organisatorische Maßnahmen bessere Zertifizierung während der Vertragslaufzeit aufrechterhalten. Entsprechendes gilt, soweit für den Auftragnehmer gemäß Formblatt Binding Corporate Rules-Processor (BCR-P) gelten.

Anderenfalls wird der Auftragnehmer für die Verarbeitung von Kundendaten die in der Anlage 2 aufgeführten technischen und organisatorischen Maßnahmen als Mindeststandards während der Vertragslaufzeit einhalten. Sofern im Formblatt die Verarbeitung von „Risikodaten“ bejaht wurde, sind zusätzlich die in diesen Mindeststandards ausdrücklich genannten Mindestanforderungen für „confidential/strictly confidential personal data“ während der Vertragslaufzeit zu erfüllen. Dem Auftragnehmer steht es frei, die in Anlage 2 genannten Maßnahmen durch andere zu ersetzen, solange die Mindeststandards weiter eingehalten oder übertroffen werden. Im Ausnahmefall können einzelne Maßnahmen entfallen, solange (i) das für die konkrete Datenverarbeitung erforderliche Datenschutzniveau hierdurch nicht unterschritten wird, (ii) dies für die Durchführung der konkreten Datenverarbeitung erforderlich ist und (iii) der Auftraggeber einer solchen Abweichung zuvor in Textform zugestimmt hat.
Auf Verlangen des Auftraggebers legt der Auftragnehmer ihm seine konkret getroffenen technischen und organisatorischen Maßnahmen dar.

8. Inanspruchnahme von Subunternehmen

Der Auftraggeber genehmigt hiermit den Einsatz der im Formblatt genannten Subunternehmer des Auftragnehmers sowie in allgemeiner Weise die Inanspruchnahme weiterer Subunternehmen durch den Auftragnehmer für die Verarbeitung von Kundendaten. Die Genehmigung steht unter dem Vorbehalt, dass die Bedingungen dieser Vereinbarung zur Inanspruchnahme von Subunternehmen eingehalten und die Voraussetzungen der anwendbaren Datenschutzgesetze für die Inanspruchnahme weiterer Auftragsverarbeiter durch den Auftragnehmer und die Subunternehmer während der gesamten Vertragslaufzeit erfüllt sind.

Der Auftragnehmer informiert den Auftraggeber mit angemessener Frist vorab über jede beabsichtigte oder notwendige Änderung hinsichtlich der Einbeziehung oder der Ersetzung eines Subunternehmers und gibt ihm damit die Möglichkeit, diesen Änderungen mit angemessener Frist aus wichtigem datenschutzrechtlichem Grund zu widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

Der Auftragnehmer wird jedem weiteren Subunternehmen vertraglich dieselben Datenschutzpflichten auferlegen, die in dieser Vereinbarung zur Auftragsverarbeitung in Bezug auf den Auftragnehmer festgelegt sind.

Der Auftragnehmer wählt sämtliche Subunternehmer sorgfältig aus, insbesondere unter Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Sicherheitsmaßnahmen, und überprüft vor der Beauftragung und regelmäßig während der Vertragslaufzeit die Einhaltung der gesetzlichen und vertraglichen Datenschutzbestimmungen durch den Subunternehmer, um den Schutz der Kundendaten zu gewährleisten. Der Auftragnehmer dokumentiert die Prüfergebnisse und stellt sie dem Auftraggeber auf Verlangen zur Verfügung.

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, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

9. Internationaler Datentransfer

Sofern im Formblatt „SUB2“ angekreuzt wurde oder falls der Auftragnehmer künftig ein weiteres Subunternehmen in einem Unsicheren Drittland einschalten gilt folgendes:

(a) Beitrittsmodell. Soweit zwischen dem Auftragnehmer und dem weiteren Subunternehmen bereits SCC in Kraft sind, welche die Anforderungen gem. Anlage 3 erfüllen oder übertreffen, tritt der Auftraggeber diesen SCC hiermit bei, sofern das weitere Subunternehmen dem Beitritt zustimmt. Soweit im Formblatt angekreuzt wurde, dass auch personenbezogene Daten von Affiliates des Auftraggebers verarbeitet werden, treten auch die Affiliates des Auftraggebers (vertreten durch den Auftraggeber) diesen SCC hiermit bei, sofern das weitere Subunternehmen dem Beitritt zustimmt.

b) Vertretungsmodell („SCC-Case“). Sofern das Beitrittsmodell nicht zur Anwendung kommt, schließt der Auftragnehmer im Namen und im Auftrag des Auftraggebers mit dem weiteren Subunternehmen die SCC gem. Anlage 3 ab. Soweit im Formblatt angekreuzt wurde, dass auch personenbezogene Daten von Affiliates des Auftraggebers verarbeitet werden, sind auch diese als „Data Exporter“ im Sinne der SCC anzugeben und der Auftragnehmer schließt die SCC auch im Namen und im Auftrag dieser Affiliates des Auftraggebers ab. Der Auftraggeber erteilt hiermit dem Auftragnehmer die für den Abschluss der SCC im Namen des Auftraggebers und im Namen der Affiliates des Auftraggebers notwendigen Vollmachten.

Auf Verlangen des Auftraggebers legt der Auftragnehmer dem Auftraggeber einen Nachweis über die im Namen und im Auftrag des Auftraggebers und sofern einschlägig der Affiliates des Auftraggebers abgeschlossenen SCC vor.

(c) Auffang-Lösung. Sofern ein weiteres Subunternehmen weder nach dem Beitritts- noch dem Vertretungsmodell mit dem Auftraggeber und sofern einschlägig der Affiliates des Auftraggebers die SCC abschließt, trägt der Auftragnehmer dafür Sorge, dass für die Übermittlung an das weitere Subunternehmen in einem Unsicheren Drittland andere geeignete Garantien nach Art. 44 ff. GDPR vorliegen (z.B. sofern das weitere Subunternehmen vom im Formblatt angegebenen Binding Corporate Rules-Processor (BCR-P) erfasst wird). Ein Datentransfer von Kundendaten, der nur auf das US-EU-Privacy-Shield-Framework gestützt wird, ist unzulässig.

10. Unterstützungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Dazu zählen insbesondere:

(a) Betroffenenrechte. Der Auftragnehmer wird einen Antrag einer betroffenen Person, die sich direkt an den Auftragnehmer wendet, um ihre Rechte geltend zu machen, unverzüglich an den Auftraggeber weiterleiten. Auf seine Weisung hin unterstützt der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen, um auf den Antrag der betroffenen Person adäquat zu reagieren. Der Auftraggeber ist hierbei insbesondere jederzeit berechtigt, den Auftragnehmer anzuweisen, die Verarbeitung der Kundendaten zu berichtigen, zu löschen und/oder einzuschränken.

(b) Meldepflichten. Der Auftragnehmer meldet dem Auftraggeber unverzüglich ab Kenntniserlangung jede im Verantwortungsbereich des Auftragnehmers liegende Datenschutzverletzung bei der Verarbeitung von Kundendaten. Die Meldung enthält mindestens die in Art. 33 Absatz 3 DSGVO genannten Angaben. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen im Rahmen des Zumutbaren und Erforderlichen unterstützen. Der Auftragnehmer wird insbesondere unverzüglich die erforderlichen Maßnahmen zur Sicherung der Kundendaten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Auftraggeber hierüber informieren und diesen um weitere Weisungen ersuchen.

(c) Informationspflichten. Der Auftragnehmer informiert den Auftraggeber unverzüglich über sämtliche Prüfungshandlungen und Maßnahmen, die von den Datenschutzbehörden oder einer anderen Behörde im Zusammenhang mit der Verarbeitung von Kundendaten ergriffen werden.

(d) Folgeabschätzung und Konsultation. Der Auftragnehmer unterstützt den für Auftraggeber bei der Durchführung einer Datenschutzfolgenabschätzung und bei der Konsultation der zuständigen Datenschutzbehörde, sofern dies gesetzlich vorgeschrieben ist.

Für die Unterstützungsleistungen nach dieser Ziffer darf der Auftragnehmer eine Vergütung verlangen, soweit diese den Aufwand von einem Manntag pro Vertragsjahr überschreitet.

11. Nachweismöglichkeiten

Der Auftragnehmer weist dem Auftraggeber auf Verlangen die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Dieser Nachweis kann durch Vorlage aktueller Bescheinigungen, Berichte oder Berichtsauszüge durch unabhängige Sachverständige (d.h. Prüfer, Datenschutzbeauftragte, IT-Sicherheit, Datenschutzprüfer, Qualitätsprüfer) oder durch ein entsprechendes Zertifikat nach den Grundsätzen der IT-Sicherheit und des Datenschutzes erbracht werden.

Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer unterstützt den Auftraggeber bei der Durchführung der Inspektion. Insbesondere verpflichtet sich der Auftragnehmer, soweit dies für eine umfassende Überprüfung der Datenverarbeitung erforderlich ist, Zugang zu Büros und EDV-Anlagen zu gewähren und Informationen und Unterlagen zur Verfügung zu stellen. Der Auftragnehmer darf die Inspektionen von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Der durch den Auftraggeber beauftragte Prüfer darf nicht in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen.

12. Datenlöschung und -rückgabe

Der Auftragnehmer wird auf die Weisung des Auftraggebers hin mit Beendigung des Hauptvertrages - oder zu einem früheren Zeitpunkt auf Verlangen des Auftraggebers - alle Kundendaten entweder vollständig und unwiderruflich löschen oder an den Auftraggeber zurückgeben bzw. ihm auf sonstige Weise zugänglich und speicherbar zu machen. Ein Anspruch des Auftragnehmers, die gesetzlichen Löschungs- bzw. Rückgaberechte des Auftraggebers einzuschränken, ist ausgeschlossen.

Davon unberührt bleibt das Recht des Auftragnehmers zur weiteren Speicherung der Kundendaten, solange der Auftragnehmer hierzu gesetzlich verpflichtet ist.

13. Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Die Parteien stellen sich insbesondere jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie nicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. Dies gilt auch für gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. Affiliate-DPA (Beitrittslösung)

Soweit nach dem Formblatt auch personenbezogene Daten eines oder mehrerer Affiliates des Auftraggebers verarbeitet werden und der Auftragnehmer für diese datenschutzrechtlich nicht Subunternehmer des Auftraggebers, sondern direkter Auftragsverarbeiter der für die Verarbeitung dieser personenbezogenen Daten selbst verantwortlichen Affiliates des Auftraggebers ist, tritt das Affiliate oder die Affiliates (jeweils als eigenständig Verantwortlicher im Sinne von Art. 4 Abs.7 DSGVO) diesem DPA hiermit - vertreten durch den Auftraggeber - bei („Affiliate-DPA“) nach Maßgabe dieser Ziffer bei.

(a) Affiliate Claims. Die dem Affiliate-DPA beigetretenen Affiliates werden grundsätzlich direkt gegenüber dem Auftragnehmer weder rechtliche Schritte einleiten noch Ansprüche geltend machen. Für den Fall, dass ein beigetretenes Affiliate rechtliche Schritte einleiten oder Ansprüche gegen den Auftragnehmer geltend machen möchte („Affiliate Claims“), erfolgt dies vielmehr durch den Auftraggeber im Namen der jeweiligen beigetretenen Affiliates, es sei denn, dass solche Affiliate-Claims aufgrund datenschutzrechtlicher Vorgaben ausnahmsweise selbst durch das beigetretene Affiliate erhoben werden müssen.

(b) Kommunikation. Der Auftraggeber ist für die Koordinierung der Kommunikation zwischen dem Auftragnehmer und den beigetretenen Affiliates des Auftraggebers im Zusammenhang mit den Affiliate-DPAs verantwortlich. Entsprechendes gilt für den Auftragnehmer in Bezug auf die Kommunikation zwischen ihm und seinen ggf. eingesetzten Subunternehmen.

Der Auftragnehmer stimmt diesem Beitritt hiermit zu.

14. Sonstiges

(a) Gerichtsstand und Rechtswahl. Der Gerichtsstand und die Rechtswahl des Hauptvertrags gelten auch für die vorliegende Vereinbarung.

(b) Änderungen. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(c) Salvatorische Klausel. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO am besten gerecht wird.

(d) Vorrang. Im Fall von Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag, gehen die Regelungen dieser Vereinbarung vor.

Technische und Organisatorische Maßnahmen

LE Commsulting hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme.
Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es LE Commsulting gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Da der Auftragnehmer den Betrieb der Internet-Dienstleistung QuizAcademy ausschließlich auf der Infrastruktur des auf externes Server-Hosting spezialisierten Subauftragsverarbeiters Amazon Web Services (AWS) EMEA SARL am Standort Frankfurt am Main betreibt und in den Räumlichkeiten des Auftragnehmers selbst keine personenbezogenen Daten von Teilnehmern gespeichert oder verarbeitet werden, beschränken sich die nachstehenden TOM auf die vom Auftragnehmer in seinen Räumlichkeiten gesetzten Sicherheitsmaßnahmen.

Informationen zu den TOM für das externe Server-Hosting sind abrufbar unter: https://aws.amazon.com/de/compliance/data-center/controls/

Darüber hinaus ergreift der Auftragnehmer folgende Maßnahmen:

1. Zutrittskontrolle

Maßnahmen, um zu verhindern, dass Unbefugte räumlichen Zutritt zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden:

- Zutrittsbewilligung und Schlüsselübergabe erfolgt ausschließlich durch die Geschäftsleitung an Mitarbeiter und wird schriftlich mit Übergabeprotokoll dokumentiert
- Falls Betriebsfremde Zutritt zu den Büroräumen benötigen, werden diese durch einen LE Commsulting-Mitarbeiter begleitet
- Doppeltes Sicherheitsschloss an der Bürotür
- Sorgfältige Auswahl von externen Dienstleistern wie Subauftragsverarbeitern und Subunternehmern

2. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können:

- Zugangsberechtigungen werden ausschließlich durch die Geschäftsführung gewährt und schriftlich dokumentiert
- Abgesicherter Zugang zum Entwicklungs- und Produktivsystem erfolgt mit einem Kennwortverfahren nach interner Passwortrichtlinie
- Einrichtung eines Benutzerstammsatzes pro Anwender als Nutzer-/Rollenkonzept in allen datenverarbeitenden und –datenspeichernden Systemen
- Arbeitsgeräte (PC, Tablets, Testgeräte, etc.) werden bei Verlassen des Arbeitsplatzes passwortgeschützt
- Bei Beendigung eines Dienstverhältnisses mit einem Mitarbeiter werden sämtliche Benutzerkonten übergeben und die Zugänge zu den Systemen deaktiviert

3. Zugriffskontrolle

Es besteht eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung.
Der Zugriff auf unsere Systeme erfolgt über ein mehrstufiges Zugriffskonzept (MFA), welches Authentifizierung durch individuelle Benutzerkennung und Passwort sowie eine separate Methode (Secure-Token) abgesichert ist. Passwörter müssen unserer internen Passwortrichtlinie entsprechen. Der Zugriff auf unsere IT-Infrastruktur ist über das Identity und Access Management (IAM) von Amazon Webservices geschützt (https://aws.amazon.com/de/iam/). Mit (IAM) wird der Zugriff auf alle AWS-Services und -Ressourcen sicher verwaltet. Dabei nutzen wir das AWS-Benutzer und -Gruppen Konzept, um den Zugriff auf Ressourcen zu steuern und nur so viel Rechte wie unbedingt nötig an unsere Mitarbeiter zu vergeben.

- Sämtliche personenbezogenen Daten in Transfer (TLS) und in Ruhe werden verschlüsselt (https://docs.aws.amazon.com/de_de/cognito/latest/developerguide/security.html)
- Systeme sind vor unbefugtem Zugang durch Firewalls und Anti-Viren-Software geschützt
- Bruteforce-Schutz, Sperrung, Reporting bei Fehlversuchen
- Monitoring und Logging von Nutzerzugriffen auf Infrastrukturkomponenten.

4. Pseudonymisierung

Maßnahmen zur Pseudonymisierung haben den Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

- Die Ablage und Zusammenführung personenbezogener Daten erfolgen anhand einer pseudonymisierten Nutzeridentifikationsnummer (Nutzer ID)

5. Weitergabekontrolle

Maßnahmen, dass personenbezogene Daten bei der elektronischen Übertragung oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.

Alle Mitarbeiter werden zur Vertraulichkeit verpflichtet, unterliegen unserer Geheimhaltungs-vereinbarung und werden regelmäßig im Umgang mit vertraulichen und personenbezogenen Daten geschult (Mitarbeiterquiz und Karteikarten).

Der Austausch von personenbezogenen Daten erfolgt ausschließlich innerhalb der Systeme des Auftragnehmers sowie ggf. deren Subunternehmer (externer Auftragsverarbeiter). Zwischen den einzelnen Systemen werden die Daten über eine SSL verschlüsselte Datenverbindung übertragen.
Personenbezogene Daten werden im Zuge der Weitergabe und Verarbeitung nicht verändert und bleiben unversehrt, vollständig und aktuell. Der Auftragnehmer unternimmt alles Notwendige, um zu verhindern, dass Daten verfälscht werden oder falsche Daten verarbeitet werden. Gleichzeitig ist gewährleistet, dass Änderungen an Daten nachvollzogen werden können.

- Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Härtung der Backendsysteme
- Sichere Ablage von Daten, inkl. Backups

6. Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.
Alle Eingaben werden vom Auftraggeber und dessen Mitarbeiter oder vom Auftragnehmer und dessen Mitarbeiter selbst vorgenommen. Die Protokollierung der Nutzeraktionen ermöglicht die Überprüfung, wer, wann und wie personenbezogene Daten eingegeben, verändert oder gelöscht hat.

Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet und nur vom Auftraggeber sowie durch den Auftragnehmer erstellt und/oder bearbeitet werden. Jede Veränderung wird unter Nennung der handelnden Person sowie einem Zeitstempel dokumentiert. Darüber hinaus erfolgt die Protokollierung über Logfiles.

7. Auftragskontrolle

Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer.
Der Auftragnehmer gewährleistet durch die nachstehenden Maßnahmen, dass die im Auftrag zu verarbeitenden Daten nur entsprechend der Auftragsbestätigung verarbeitet werden:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsbestätigung)
- Überprüfung der Einhaltung der vertraglichen Regelungen
- Alle Mitarbeiter sind im Umgang mit personenbezogenen Daten geschult
- Vertraulichkeits- und Datenschutzvereinbarung mit Subunternehmen

8. Verfügbarkeitskontrolle und Belastbarkeit

Maßnahmen, um personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen, sind hier abrufbar: https://aws.amazon.com/de/security/
Kritische System (Datenbanken) werden bei AWS in einem Multi-Availability-Zone (Multi-AZ) Konzept konfiguriert (https://aws.amazon.com/de/rds/features/multi-az/). Dieses Konzept erlaubt eine hohe Datenbeständigkeit, eine hohe Verfügbarkeit, eine hohe Performance und ein automatisches Failover-Recovery im Falle von physischen Problemen an der Hardware.
Personenbezogene Daten werden bei QuizAcademy in Amazon Cognito verwaltet. Amazon Cognito unterstützt viele Sicherheits- und Compliance-Vorgaben, auch die für stark reglementierte Unternehmen wie bspw. im Gesundheitswesen. Amazon Cognito ist HIPAA-berechtigt und konform mit PCI DSS, SOC und ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 sowie ISO 9001.

9. Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:
Die Systeme des Auftragnehmers werden von mehreren Auftraggebern und einer Vielzahl von Nutzern gleichzeitig verwendet. Die Speicherung erfolgt durch eine logische Trennung von Nutzeraccounts (Nutzer ID). Vertragsdaten der Auftraggeber (Name, Anschrift, Verträge usw.) sind ebenfalls getrennt voneinander gespeichert und durch (Kunden IDs) umgesetzt. Gleichzeitig besteht eine physikalische Trennung der Systeme nach Funktion in Test- und Produktivsystem.

10. Datenschutzmanagement

Der Auftragnehmer gewährleistet einen Prozess zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen. Dies geschieht durch:

- Alle Mitarbeiter wurden schriftlich auf die Einhaltung datenschutzrechtlicher Vorschriften verpflichtet und unterwiesen
- Die mit der Datenverarbeitung betrauten Mitarbeiter wurden auf ihre Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse hingewiesen
- Wenn aus organisatorischen Gründen Funktionsüberschneidungen bestehen, wird das Vier-Augen-Prinzip angewendet und dokumentiert
- Es existiert eine definierte Vertreterregelung innerhalb von Funktionsgruppen

Standard Contractual Clauses

Insofar "S2" is selected within the Form Sheet (in the absence of Binding Corporate Rules) or if the applicability of this Annex 3 results from the rules on "International Data Transfer" set out in Annex 1 (General Terms and Conditions for Data Processing) as "SCC-Case", the "Standard Contractual Clauses (processors)" based on the EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document number C(2010) 593, as amended) in its latest version, have to be concluded by the following parties, subject to the following:

I. Basics

A. Scope

The SCC consists of:

I. The "Clauses" (the official published contractual clauses No.1-12) available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087
II. Appendix 1 to SCC (as follows)
III. Appendix 2 to SCC (as follows)

B. Parties of the SCC

The Data Exporter is (i) the entity as described "Auftraggeber/Controller" within the Form Sheet as well as (ii) any Affiliate of the "Auftraggeber/Controller" (if the processing of personal data of the Affiliates is affirmed within the Form Sheet). The Affiliates of the "Auftraggeber/Controller" correspond to those of the "Hauptvertrag/Main Contract", defined in the Form Sheet.

The Data Importer is (i) the entity as described "Auftragnehmer/Processor" (if "S2" is selected in the Form Sheet) or (ii) the listed "Subunternehmer/subprocessor" in the Form Sheet, seated within a Third Country without adequate level of data protection ("Sub(s)")

Each of them is a "party"; together data exporter and data importer are "the parties" in the sense of the SCC.

C. Conclusion

"Direct Conclusion". Insofar selected in Form Sheet "S2", the "Auftraggeber/Controller" hereby confirms having authority and being contractually entitled to enter into the SCC with the data importer in its own name and on behalf of its Affiliates, if any. Hence, the signature of a party in the Form Sheet shall be deemed as a signature of the Clauses as well as of the Appendixes. Therefore, by signing the Form Sheet, the parties hereby also conclude the SCC.

"Representation Model". Insofar a "SCC-Case" applies, the "Auftraggeber/Controller" hereby confirms having authority and being contractually entitled to authorize the "Auftragnehmer/Processor" to enter into the SCC with the data importer (the Sub(s)) in the name and on behalf of the Auftraggeber/Controller and its Affiliates, if any. Therefore, the SCC have to be concluded by the (authorized) "Auftragnehmer/Processor" and the data importer (its Sub(s)).

"Special Case Conclusion". If and insofar however within a "SCC-Case", the "Auftragnehmer/Processor" has affirmed within the table of subprocessors in the Form Sheet to represent a subprocessor ("Represented Sub"), the "Auftragnehmer/Processor" hereby confirms, having authority and being contractually entitled to enter into the SCC with the data exporter in its own name and on behalf of the represented Sub. Therefore, by signing the Form Sheet, the appropriate parties hereby conclude the SCC whereby the signing of the Form Sheet shall be deemed as a signature of the Clauses as well as of the Appendixes.

II. Appendix 1 to SCC

Data exporter is the entity/are the entities of the BASF-group identified within this Appendix 3 as "Data Exporter" which is/are entitled to use the software and/or services provided by the Auftragnehmer/Processor identified within the Form Sheet.

Data importer is the entity/are the entities identified within this Appendix 3 as "Data Importer" which provide(s) the software and/or services or act(s) as Sub(s) of this provider.

Data subjects and Categories of data (including Special categories of data if appropriate) are specified in the Form Sheet.

Processing operations
The personal data transferred will be subject to the basic processing activities as specified in the Form Sheet, including the nature and purpose of

the processing, to provide the software and/or services according to the "Hauptvertrag"/"Main Contract" defined in the Form Sheet (as the subject-matter of the processing).

Additional Processing Operations
If the SCC are concluded as "Direct Conclusion" or as "Special Case Conclusion" (as described within part C. Annex 3) or if the SCC are concludes as "Representation Model" and it is commercially possible for the "Auftragnehmer/Processor" to negotiate into the following Additional Processing Operations, the following Additional Processing Operations are binding part of Appendix 2 to SCC with regard to avoid any gap in comparison with the requirements of Art. 28 Sec. 3 GDPR. Nevertheless, nothing in this Annex 3 shall be construed to prevail over any conflicting Clause of the Standard Contractual Clauses.

1. Duration of the processing The personal data shall be processed for the duration of the Main Contract.

2. Sub-processors The Data Exporter declares its general authorization to engage sub-processors. The Data Importer shall inform the data exporter of any intended changes concerning the addition or replacement of other processors, thereby giving the Data Exporter the opportunity to object to such changes.

3. Instructions The Data Importer is entitled to process the personal data without or against an instruction of Data Exporter only if required to do so by Union or Member State law to which the Data Importer is subject. After the termination of the Main Contract, the Data Importer is entitled to store the personal data only if required to do so by Union or Member State law to which the Data Importer is subject.

4. Confidentiality Data Importer ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Assistance a. Taking into account the nature of the processing, the Data Importer shall assist the Data Exporter by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Exporter's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

b. The Data Importer shall notify the Data Exporter without undue delay after becoming aware of a personal data breach as defined in the GDPR. The Data Importer shall upon consultations with the Data Exporter take the appropriate measures in order to secure the concerned personal data and to mitigate any potential negative effects on data subjects. The Data Importer shall assist the Data Exporter to the extent that the Data Exporter is obliged by applying reporting and notification obligations.

c. Data Importer shall assist the Data Exporter in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Data Importer.

6. Rights and Remedies Except where applicable Data Protection Laws and Regulations requires an Affiliate of the "Auftraggeber/Controller" (if any Affiliates are concerned) to exercise a right or seek any remedy under the SCC against the Data Importer directly by itself, the parties agree that "Auftraggeber/Controller" shall exercise any such right or seek any such remedy on behalf of its Affiliate.

7. Communication
"Auftraggeber/Controller" that is the contracting party to the Main Contract shall remain responsible for coordinating all communication with the Data Importer under this Agreement and be entitled to make and receive any communication in relation to this Agreement on behalf of its Affiliates (if any Affiliates are concerned).

Schrems II
Against the background of the recent European Court of Justice's (ECJ) ruling regarding the EU-U.S. Privacy Shield and EU Model Clauses (C-311/18, "Schrems II"), the Parties shall amicably discuss and implement technical and organizational measures to comply with the additional requirements the ECJ and / or competent supervisory authorities set out with respect to Third Country data transfers.

III. Appendix 3 to SCC

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

Insofar as the Data Importer is certified according to ISO 27001, SOC 2 Typ 2 or any comparable

certification, the associated technical and organizational measures are agreed to be the implemented organizational security measures by Data Importer. The Data importer will maintain this or any comparable certification (or better one) during the term of the SCC.

Otherwise, the Data Importer shall comply for the processing of Client Data with the technical and organizational measures listed in Annex 2 as minimum technical and organizational measures during the term of the Contract. If the processing of "Riskiodaten/risk data" is affirmed in the Form Sheet, the more expressly mentioned extensive measures for the processing of “confidential/strictly confidential personal data“must also be complied in addition during the term. The data importer is free to replace the measures mentioned in Annex 2 by others as long as the minimum standards are still met or exceeded. In exceptional cases, individual measures may be waived as long as (i) the level of data protection concretely required for the specific data processing is not compromised (ii) it is necessary for the implementation of the specific data processing and (iii) the data exporter has agreed to such a deviation in advance in text form. At the request of the data exporter, the data importer shall provide a list of its concrete technical and organizational measures taken.