Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

zwischen dem/der

Name und Anschrift einfügen
- Verantwortlicher - nachstehend Auftraggeber genannt und der

Axel Schäfer & Partner GmbH, Am Oberen Luisenpark 22, 68165 Mannheim
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Diese Vereinbarung zur Auftragsverarbeitung ist Bestandteil der Verträge zwischen den Parteien über die Bereitstellung und Nutzung von E-Learning-Lösungen (Leistungsvereinbarungen). Diese Vereinbarung konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus der in den Leistungsvereinbarungen in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Leistungsvereinbarung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Bereitstellung und Nutzung von E-Learning-Lösungen.

In der zwischen dem Auftraggeber und dem Auftragnehmer abgeschlossenen Leistungsvereinbarung sind die beauftragten Leistungen näher spezifiziert.

(2) Die Dauer dieses Auftrags entspricht der Laufzeit der am längsten laufenden Leistungsvereinbarung zwischen den Parteien.

2. Konkretisierung des Auftragsinhalts

(1) Der Auftragnehmer stellt dem Auftraggeber Software zur Bereitstellung von Lerninhalten und der Verarbeitung von Lernaktivitäten sowie Lernständen zur Verfügung (Lernplattform). Der Zweck ist in der Anlage definiert. Soweit in der Leistungsvereinbarung von dem Auftraggeber beauftragt, umfassen die Leistungen des Auftragnehmers u.a. das Hosting der Lernplattform in einem sicheren Rechenzentrum sowie Wartung und Support.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen

Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Im Rahmen der Leistungsvereinbarung erfolgt die Verarbeitung personenbezogener Daten. Die Kategorien personenbezogener Daten sind in der Anlage festgelegt.

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Anlage 4 definiert.

3. Technische und organisatorische Sicherheitsmaßnahmen

(1) Der Auftragnehmer hat die Umsetzung der organisatorischen Sicherheitsmaßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Die im Einzelnen getroffenen Maßnahmen sind in Anlage 6 beschrieben. Bei Akzeptanz durch den Auftraggeber werden die in der Anlage dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Soweit die Anpassung für den Auftragnehmer einen erhöhten Aufwand in technischer oder personeller Hinsicht bedeutet, vergütet der Auftraggeber den mit der Anpassung verbundenen Mehraufwand zu den in der Leistungsvereinbarung benannten Verrechnungssätzen.

(2) Der Auftragnehmer hat die Sicherheit der Verarbeitung gemäß Art. 28 Abs. 3 lit. c, 32 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. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(3) Die technischen und organisatorischen Sicherheitsmaßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung der Verarbeitung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Rechte auf Löschung, Berichtigung, Datenübertragbarkeit und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer im Rahmen der Funktionen der von dem Auftragnehmer zur Verfügung gestellten Lernplattform sicherzustellen.

5. Sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der beauftragten Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO. Die im Einzelnen getroffenen Maßnahmen sind in Anlage 6 beschrieben. Anlage 6 ist Bestandteil dieser Vereinbarung.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Sicherheitsmaßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Sicherheitsmaßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieser Vereinbarung.

6. Unterauftragsverhältnisse

1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Postleistungen, oder Transportdienstleistungen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Auftraggebers auch bei solchen ausgelagerten Nebenleistungen angemessene vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Zurzeit sind für den Auftragnehmer die in der Anlage 5 mit Name, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer mit der Verarbeitung von personenbezogenen Daten in dem genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

(3) Der Auftragnehmer darf weitere Auftragsverarbeiter zur Verarbeitung von Daten des Auftraggebers ohne vorherige gesonderte Zustimmung des Auftraggebers beauftragen. Der

Auftragnehmer informiert den Auftraggeber spätestens 30 Tage vor jeder geplanten Beauftragung weiterer Auftragsverarbeiter. Erfolgt eine Information nicht rechtzeitig, gilt sie als nicht erteilt. Der Auftragnehmer informiert den Auftraggeber über Name und Anschrift des Unterauftragnehmers sowie über den Inhalt des geplanten Unterauftrags. Der Auftragnehmer dokumentiert diese Information in geeigneter Weise. Der Auftraggeber kann bis zur Beauftragung des Weiteren Auftragsverarbeiters schriftlich oder in Textform Einspruch erheben. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösung zwischen den Parteien nicht möglich, kann der Auftraggeber die Leistungsvereinbarung außerordentlich kündigen. Die Kündigung hat unverzüglich, spätestens jedoch innerhalb von 90 Tagen ab Zugang der Information über den Einsatz eines weiteren Auftragsverarbeiters zu erfolgen.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an Unterauftragnehmer und deren erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Dazu sind die vertraglichen Vereinbarungen zwischen dem Auftragnehmer und dem Unterauftragnehmer so zu gestalten, dass sie den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entsprechen.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/ des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

7. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen nachzuweisen.

(2) Auftraggeber und Auftragnehmer verständigen sich darauf, dass der Nachweis der Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen nach Wahl des Auftragnehmers durch Unterlagen erbracht werden kann, die ein nachvollziehen von Sicherheitsmaßnahmen möglich machen.

(3) 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 darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Sicherheitsmaßnahmen abhängig machen.

Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(4) Für die Unterstützung bei der Durchführung einer Inspektion kann der Auftragnehmer eine angemessene Vergütung gemäß den in der Leistungsvereinbarung benannten Verrechnungssätzen verlangen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen.

Hierzu gehören unter anderem:

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Sicherheitsmaßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber der betroffenen Person zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
- die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgenabschätzung und die Unterstützung des Auftraggebers im Rahmen
- vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsvereinbarung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung gemäß den in der Leistungsvereinbarung benannten Verrechnungssätzen beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und gemäß den Weisungen des Auftraggebers. Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens in Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Weisungsberechtigte Personen des Auftraggebers sind der Verantwortliche, der Datenschutzbeauftragte des Auftraggebers, der in der Leistungsvereinbarung benannte Projektverantwortliche sowie deren Vertreter. Sofern ein Supportvertrag vereinbart wurde, gelten auch die Personen, die der Verantwortliche als supportberechtigt benannt hat, als weisungsbefugt. Änderungen bei den benannten Personen nach Satz 1 und Satz 2 werden dem Auftragnehmer in Textform übermittelt.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung

(1) Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung.

Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadenersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit dies ihrem Anteil an der Verantwortung entspricht.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Weisungsberechtige Personen des Auftraggebers sind der Verantwortliche, der Datenschutzbeauftragte des Auftraggebers, der in der Leistungsvereinbarung benannte Projektverantwortliche sowie deren Vertreter. Sofern ein Supportvertrag vereinbart wurde, gelten auch die Personen, die der Verantwortliche als supportberechtigt benannt hat, als weisungsbefugt. Änderungen bei den benannten Personen nach Satz 1 und Satz 2 werden dem Auftragnehmer in Textform übermittelt.

12. Schlussbestimmungen

(1) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand bei allen Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist Mannheim.

(2) Sollten die EU-Kommission oder die zuständige Aufsichtsbehörde Standardklauseln für Auftragsverarbeitungsverträge festlegen, werden sich die Parteien im erforderlichen Umfang auf eine mögliche Anpassung dieser Vereinbarung an die Standardklauseln verständigen.

(3) Änderungen und Ergänzungen dieser Vereinbarungen und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(4) Im Falle eines Widerspruchs zwischen Leistungsvereinbarung und dieser Vereinbarung geht diese Vereinbarung vor, soweit die Regelung dieser Vereinbarung die Verarbeitung personenbezogener Daten betrifft. Sollten einzelne Teil dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen dieser Vereinbarung oder der Leistungsvereinbarung nicht.

(5) Sollte das Eigentum des Auftragnehmers durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so wird der Auftragnehmer den Auftraggeber unverzüglich verständigen. Er wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Verfügungsbefugnisse an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ liegen.

(6) Die Einrede des Zurückbehaltungsrechts i.S.d. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(7) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, berührt dies die Wirksamkeit der Gesamtvereinbarung nicht.

Ort/Datum	Mannheim,
(Firma)	Axel Schäfer & Partner GmbH
Name, Position	Axel Schäfer, Geschäftsführer

Anlage 1: Kontaktdaten

Verantwortliche/r des Aufraggebers
Stellvertretung der Verantwortlichen Stelle des Auftraggebers
Datenschutzbeauftragte/r des Auftraggebers (falls bestellt)
Stellvertretung des Datenschutzbeaufragten (falls bestellt)

Bei Änderung der Daten ist der Auftragnehmer in Textform zu informieren.

Verantwortlicher des Auftragnehmers:

Axel Schäfer

Axel Schäfer & Partner GmbH
Am Oberen Luisenpark 22
68165 Mannheim

Telefon 0621-32491213

a.schaefer@sp-lernwelt.de

Datenschutzbeauftragter des Auftragnehmers:

Aufgrund der Unternehmensgröße ist die Bestellung eines Datenschutzbeauftragten nicht erforderlich.

Anlage 2: Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber

Der Auftragnehmer stellt für den Auftraggeber Software zur Bereitstellung von Lerninhalten und der Verarbeitung von Lernaktivitäten und Lernständen zur Verfügung. Die Software dient zur Ausbildung, Fort- und Weiterbildung sowie zur Kommunikation zwischen Anwendern.

Bei Änderung der Daten ist der Auftragnehmer in Textform zu informieren.

Anlage 3: Kategorien der verwendeten personenbezogenen Daten

- Vorname, Nachname, E-Mail des Nutzers
- Anmeldename, wird i.d.R. durch den Benutzer selbst vergeben
- persönliches Kennwort (kann geändert werden)
- Stadt, Land
- weitere Daten, die der Nutzer in seinem Profil einstellt
- belegte Kursveranstaltungen
- Aktivitäten in Kursen
- Forenbeiträge
- bearbeitete Lernaktivitäten
- Lernergebnisse
- Protokolldaten über die Aktivität des Nutzers unter Angabe seiner IP-Adresse, durchgeführter
- Aktivitäten, Inhalt der Nutzereingabe und Zeitpunkt der Aktivität.

Anlage 4: Kategorien betroffener Personen

Die folgenden Kategorien betroffene Personen werden verarbeitet:

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers
- Teilnehmende

Sonstige (ggf. ergänzen)

Bei Änderung der Daten ist der Auftragnehmer in Textform zu informieren.

Anlage 5: Unterauftragnehmer

Es werden folgende Unterauftragnehmer eingesetzt:

Unterauftragnehmer	Anschrift/Land	Leistung
eLedia GmbH	Wilhelmsaue 37 10713 Berlin	Hosting der Lernplattform; Softwarepflege, Update; Support bei Technischen Problemen

Anlage 6: Technisch-organisatorische Maßnahmen

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen, die der Auftragnehmer zum Schutz der verarbeiteten Daten getroffen hat. Für die von dem Auftragnehmer eingesetzten Unterauftragnehmer gelten gesonderte technische und organisatorische Maßnahmen, die auf Anfrage zur Verfügung gestellt werden.

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

Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Räumlichkeiten zu verwehren, in denen personenbezogene Daten verarbeitet werden:

Die Räume verfügen über ein Schließsystem mit Sicherheitsschlössern.
Ein Zutritt ohne Befugnis ist nicht möglich.
Die Ausgabe von Schlüsseln wird dokumentiert.
Der Zutritt von Besuchern ist nur in Begleitung durch Mitarbeiter zulässig.
Die Gebäudereinigung erfolgt in Anwesenheit von Mitarbeitern während der Bürozeiten.

Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten verarbeitet werden können:

Es erfolgt eine Begrenzung der Zugangsberechtigten.
Den Benutzern werden Benutzerrechte in Abhängigkeit von den von ihnen ausgeübten Funktionen zugewiesen.
Eine Authentifizierung erfolgt mit Benutzernamen und Passwort.
Es existieren Vorgaben zur Passwortgestaltung, -handhabung und -verwaltung.
Es wird auf allen PCs Antivirensoftware mit automatisierter Aktualisierung eingesetzt.

Zugriffskontrolle

Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Die Zugriffsberechtigungen werden in Abhängigkeit von der Funktion eines Mitarbeiters vergeben.
Die Anzahl der Administratoren ist begrenzt.
Der Zugriff auf Anwendungen wird protokolliert.
Für die Vernichtung papiergebundener personenbezogener Daten stehen Aktenvernichter zur Verfügung.

Trennungskontrolle

Die Verarbeitung von Daten verschiedener Auftraggeber erfolgt getrennt.

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

Weitergabekontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt verarbeitet werden können:

- Der Zugriff auf personenbezogene Datensätze des Auftraggebers erfolgt nach Möglichkeit und nach Maßgabe der vertraglichen Vereinbarung über verschlüsselte Zugänge (https bzw. SSH).
- Die Weitergabe von Daten ist nur nach Maßgabe der vertraglichen Vereinbarungen und auf Weisung des Auftraggebers zulässig.
- Es werden Logprotokolle erzeugt.
- Die Abfrage und Übertragung personenbezogener Daten durch Anwender erfolgt verschlüsselt mittels Webbrowser (https). Passwörter der Nutzer werden in der Datenbank nach Möglichkeit verschlüsselt abgelegt.

Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme verarbeitet worden sind:

- Es gibt ein Protokoll der Eingaben.
- Es werden serverseitige Logprotokolle über Nutzerzugriffe geführt.
- Es besteht ein Berechtigungskonzept.
- Die Protokollierung erfolgt im Rahmen der Funktionen in den vom Auftraggeber beauftragten Anwendungsprogramme.
- Sofern ein automatisierter Austausch personenbezogener Daten zwischen Anwendungen des Auftraggebers und des Auftragnehmers erfolgen (z.B. Authentifizierungssysteme, Anbindung an HR-Systeme), werden diese Übertragungen über sichere Transportwege vorgenommen. Für den Austausch von Daten in manueller Weise stellt der Auftragnehmer einen geschützten Upload auf Anfrage zur Verfügung.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Datensicherung: Es erfolgt eine tägliche Sicherung der Daten. Die Daten werden nach erfolgter Sicherung auf getrennten Servern abgelegt.
- Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO): Die Wiederherstellung der Daten aus den Backups kann jederzeit beauftragt werden. Die Wiederherstellbarkeit wird exemplarisch bzw. nach gesonderter Beauftragung durch den Auftraggeber geprüft.

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

Die in dieser Anlage beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen werden mindestens einmal jährlich geprüft und bei Bedarf angepasst. Bei Feststellung eines sicherheitsrelevanten Vorfalls werden die getroffenen Maßnahmen umgehend geprüft und im erforderlichen Umfang angepasst.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO): Die Konfiguration des Anwendungsprogramms erfolgt in Abstimmung zwischen dem Auftraggeber und dem Auftragnehmer.

Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Die Auswahl von Auftragsverarbeitern erfolgt sorgfältig unter Beachtung der Bestimmung des Art. 28 DSGVO.
- Weisungen an die beauftragten Auftragsverarbeiter erfolgen in Textform.
- Der Auftragnehmer arbeitet nur mit Auftragsverarbeitern zusammen, die soweit gesetzlich vorgeschrieben einen Datenschutzbeauftragten benannt haben.
- Die Mitarbeiter des Auftragnehmers werden schriftlich auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet.
- Die Mitarbeiter des Auftragnehmers werden regelmäßig über die Verpflichtungen unterrichtet, welche sich aus der Auftragsverarbeitung ergeben.
- Sämtliche personenbezogenen Daten werden nach Beendigung des Auftrags bzw. nach Ablauf gesetzlicher Aufbewahrungsfristen gelöscht.