wb CONSULTING + DEVELOPMENT

Anlage 1
Auftragsverarbeitungsvertrag

Stand: August 2018

wb CONSULTING + DEVELOPMENT
Birgit Winter & Oliver Winter
Rhöndorfer Str. 23A · 53604 Bad Honnef

Telefon +49 (0) 2224 - 98199 - 01
Telefax +49 (0) 2224 - 98199 - 02
E-Mail info@wb-consulting.eu
Internet www.wb-consulting.eu

1 Präambel

Bei der Nutzung der Lernplattform werden vom Kunden unter anderem personenbezogene Daten in der ihm zur Verfügung gestellten Software verarbeitet und gespeichert. Die Verarbeitung der personenbezogenen Daten erfolgt in diesem Fall durch die wb für den Kunden im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

Die Verarbeitung und Speicherung personenbezogener Daten im Rahmen der Nutzung der Lernplattform erfolgt ausschließlich im Auftrag und nach den Weisungen des Kunden. Der Inhalt und der Umfang der Weisungsbefugnis sind in dieser Anlage definiert.

Um die Anforderungen einer Auftragsverarbeitung bei der Verarbeitung und Speicherung personenbezogener Daten zu gewährleisten, halten die Parteien das Nachfolgende fest:

2 Gegenstand und Dauer der Vereinbarung

Gegenstand des Auftrages ist Hosting, Wartung, Betrieb und Zurverfügungstellen einer Lernplattform-Software zum Online-Abruf für den Kunden. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Die Dauer der Datenspeicherung ist gleichbedeutend mit der Laufzeit des Nutzungsvertrages zur Nutzung der Lernplattform.

Unabhängig von der Laufzeit des Vertrages kann der Kunde die Auftragsverarbeitung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der wb gegen Datenschutzvorschriften oder die Bestimmungen dieser Anlage oder des Nutzungsvertrages vorliegt, wb eine Weisung des Kunden nicht ausführen kann oder will oder wb Kontrollrechte des Kunden vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in dieser Anlage vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen solchen schweren Verstoß dar.

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

3.1 Die Verarbeitung personenbezogener Daten erfolgt durch Eingabe solcher Daten durch den Kunden oder die wb im Auftrag des Kunden in der Software zur Lernplattform. Die Datenverarbeitung ist hierbei zur Nutzung der Lernplattform erforderlich bzw. hilfreich. Die eingegebenen Daten werden von wb mit Ausnahme von entsprechenden Anweisungen des Kunden weder bearbeitet, noch verändert oder an Dritte weitergegeben. wb wird die vom Kunden eingegebenen Daten ausschließlich unter Beachtung der Bestimmungen dieses Vertrages und etwaigen weiteren Weisungen des Kunden speichern. Der Kunde allein ist berechtigt, die Daten zu berichtigen, zu löschen und zu sperren (Art der Verarbeitung, Art. 4 Nr. 2 DSGVO). Zudem ist jeder Teilnehmer der Lernplattform berechtigt und in der Lage, die ihn betreffenden personenbezogenen Daten selbst zu bearbeiten, zu löschen oder zu entfernen.

3.2 Der Teilnehmer kann in der Software zur Lernplattform folgende personenbezogene Daten eingeben (Art der personenbezogenen Daten, Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

- Personenstammdaten der Teilnehmer

- Kommunikationsdaten der Teilnehmer (z.B. Telefon, E-Mail)

3.3 Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Daten der Mitarbeiter des Kunden
- Daten des Kunden

4 Rechte und Pflichten sowie Weisungsbefugnisse des Kunden

4.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Kunde verantwortlich. Gleichwohl ist wb verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Kunden gerichtet sind, unverzüglich an diesen weiterzuleiten.

4.2 Der Kunde erteilt etwaige Aufträge, Teilaufträge und Weisungen in Bezug auf die Auftragsverarbeitung ausschließlich schriftlich oder in einem dokumentierten elektronischen Format. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen dem Kunden und der wb abzustimmen und schriftlich festzulegen.

4.3 Der Kunde ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der bei der wb getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Anlage festgelegten Verpflichtungen zu überzeugen.

Der Kunde informiert die wb unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt. Der Kunde ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der wb vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

5 Pflichten der wb

5.1 wb verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Kunden, sofern sie nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem sie unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt wb dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

wb verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen und ausdrücklicher Zustimmung des Kunden nicht erstellt.

wb sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Sie sichert zu, dass die für den Kunden verarbeiteten Daten von sonstigen Datenbeständen der wb strikt getrennt werden.

5.2 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Kunden, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Kunden hat wb im notwendigen Umfang mitzuwirken und den Kunden soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). wb ist berechtigt, dem Kunden den hierbei

angefallenen Aufwand nach den allgemein gültigen Honorarsätzen der wb gesondert in Rechnung zu stellen.

5.3 wb wird den Kunden unverzüglich darauf aufmerksam machen, wenn eine vom Kunden erteilte Weisung ihrer Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). wb ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen des Kunden nach Überprüfung bestätigt oder geändert wird. wb hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Kunde dies mittels einer Weisung verlangt und berechtigte Interessen der wb dem nicht entgegenstehen. wb ist berechtigt, dem Kunden den hierbei angefallenen Aufwand nach den allgemein gültigen Honorarsätzen der wb gesondert in Rechnung zu stellen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf wb nur nach vorheriger Weisung oder schriftlicher Zustimmung durch den Kunden erteilen.

wb erklärt sich damit einverstanden, dass der Kunde - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Kunden beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). wb sichert zu, dass sie, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. wb ist berechtigt, dem Kunden den hierbei angefallenen Aufwand nach den allgemein gültigen Honorarsätzen der wb gesondert in Rechnung zu stellen.

5.4 wb verpflichtet sich, bei der auftragsgemäßen Verarbeitung der vom Kunden eingegebenen Daten die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. wb sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). wb überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in ihrem Betrieb und bei ihren zur Erfüllung ihrer Aufgaben eingesetzten Subunternehmer auf eigene Verantwortung.

6 Mitteilungspflichten bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

wb teilt dem Kunden unverzüglich Störungen, Verstöße der wb oder deren Subunternehmer sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Kunden als Datenverantwortlicher nach Art. 33 und Art. 34 DSGVO. wb sichert zu, den Kunden erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). wb ist berechtigt, dem Kunden den hierbei angefallenen Aufwand nach den allgemein gültigen Honorarsätzen der wb gesondert in Rechnung zu stellen.

Meldungen nach Art. 33 oder 34 DSGVO für den Kunden darf wb nur nach vorheriger ausdrücklicher schriftlicher Weisung des Kunden durchführen.

7 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

7.1 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Kunden ist der wb generell gestattet, Art. 28 Abs. 2 DSGVO.

wb bedient sich zur Erfüllung seiner vertraglichen Pflichten derzeit der Lernsoftware von Avendoo. Betreiber von Avendoo ist die Firma Magh und Boppert GmbH, Schulze-Delitzsch-Straße 8, 33100 Paderborn.

wb informiert den Kunden über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Kunde die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

7.2 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

7.3 wb haftet gegenüber dem Kunden dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

8 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

8.1 Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

8.2 Das im Anhang 1 zu dieser Anlage beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Mindestmaßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse bei der wb bzw. ihren Subunternehmern dar.

8.3 Soweit die bei wb bzw. ihren Subunternehmern getroffenen Maßnahmen den Anforderungen des Anhang 1 nicht genügen, benachrichtigt wb den Kunden unverzüglich. Die Maßnahmen bei der wb oder ihren Subunternehmern können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards jedoch nicht unterschreiten.

Wesentliche Änderungen muss wb mit dem Kunden in dokumentierter Form schriftlich abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9 Verpflichtungen nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat wb sämtliche in ihren Besitz gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem Kunden auf

Anforderung mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10 Haftung

Auf Art. 82 DSGVO wird verwiesen.

11 Sonstiges

11.1 Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

11.2 Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

11.3 Sollte das Eigentum oder die zu verarbeitenden Kundendaten bei wb durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat wb den Kunden unverzüglich darüber zu verständigen.

11.4 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Kunden verarbeiteten Daten und der zugehörigen Datenträger hiermit ausgeschlossen.

11.5 Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

12 Anhang 1 zur Anlage 1 Einzuhaltende technisch-organisatorische Maßnahmen: Mindeststandard

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

(1) **Zutrittskontrolle**
Für die Außen- und Innensicherung sind innerhalb und außerhalb der Arbeitszeiten folgende - Maßnahmen zur Zutrittskontrolle getroffen:

- Dritten / Unbefugten wird der Zutritt zu den Systemen verwehrt
- Festlegung befugter Personen, Schlüsselregelungen
- Manuelles Schließsystem
- Einbruchmeldeanlagen
- Zugangsregelung für betriebsfremde Personen

Externe Rechenzentren: Der Zutritt zu den Systemen des Auftraggebers ist nur ausgewiesenen Mitarbeitern möglich. Die externen Rechenzentren genügen den Ansprüchen und werden regelmäßig überprüft.

(2) **Zugangskontrolle**
Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet werden, können nicht von Unbefugten genutzt werden. Es wird gewährleistet, dass nur autorisierte Mitarbeiter Zugang zu den verarbeiteten Daten haben. Hierfür werden folgende Sicherungsmaßnahmen verwendet:

- Eindeutige Identifizierung des Nutzers gegenüber dem System
- Einsatz von Anti-Viren Software
- Festgelegte Berechtigungsstrukturen
- Arbeitsanweisung zur Bildschirmsperre
- Technische Sicherstellung der Passwortqualität
- Einsatz einer Firewall

(3) **Zugriffskontrolle**
Es wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle). Maßnahmen zur Sicherstellung der Zugriffskontrolle:

- Restriktive differenzierte Rechtevergabe
- Es wird KEIN Modemzugriff eingesetzt, nur reine LAN / IP / VPN Kommunikation
- Datenterminals werden bei Nichtbenutzung gesperrt
- Sichere und verschlüsselte Speicherung von Zugangsdaten

(4) **Trennungskontrolle**
Daten sind logisch im Rahmen der Zugriffskontrolle getrennt. Durch die Trennung können jederzeit Daten auf Anforderung des Kunden vollständig gelöscht werden. Eine Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) findet nicht statt.

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

(1) **Weitergabekontrolle**
Werden Daten an Dritte weitergegeben im Sinne der Auftragsdatenverarbeitung, dann gilt:

- Es erfolgt eine Verschlüsselung der Datenträger.
- Es werden die Daten als Daten des Kunden gekennzeichnet.
- Alle Datenträger werden verschlossen aufbewahrt.
- Nur festgelegte Mitarbeiter haben Zugang zu den Datenträgern.

(2) **Eingabekontrolle**
Durch Protokollierung wird festgestellt, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

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

Verfügbarkeitskontrolle
Es wird sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

- Brandschutzmaßnahmen
- Überspannungsschutz
- Festplattenspiegelung
- Backupkonzept
- Virenschutzkonzept
- Schutz vor Diebstahl
- Durch ein Backup und Desaster Recovery Konzept wird die rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO) sichergestellt.