Vertrag über die Auftragsverarbeitung

Fassung AVV-UKKI 0.9.1 (vorläufig) · Stand 22.10.2026
Prüfwert (SHA-256 über alle Teile): 6486f4e12089fafe41e4d58023540df0618c9d75e743f165e4c34c9fab0a0913
Teile: Vertrag · Anlage 1: Verarbeitung · Anlage 2: Technische und organisatorische Maßnahmen · Anlage 3: Unterauftragsverarbeiter · Wer ist wofür verantwortlich?

Frühere, vorläufige Fassung – ersetzt durch AVV-UKKI 1.0.

Vertrag über die Auftragsverarbeitung (Art. 28 DSGVO)

Plattform „Unternehmen Kompetenz KI“ – Firmenkonto Fassung **AVV-UKKI 0.9.1 (Entwurf)** · Stand 22.10.2026

> *ENTWURF. Erstellt von Claude, geprüft von Volker (Jurist-Agent, Prüfaufträge 07–09 und 14). Vor dem Einsatz prüft ein Fachanwalt für IT-Recht/Datenschutz. Stellen mit* `[FACHANWALT]` *sind offen. Diese Vorbemerkung und alle Marken entfallen in der freigegebenen Fassung.*

Vertragsparteien

Verantwortlicher (im Folgenden „Kunde“): das Unternehmen, für das der Firmen-Admin diesen Vertrag in der Plattform abschließt. Name und Anschrift stehen im Firmenkonto und im Abschlussnachweis (§ 14 Abs. 1).

Auftragsverarbeiter (im Folgenden „Anbieter“): Content Butler GmbH, Tannenweg 22, 55129 Mainz, vertreten durch die Geschäftsführer Hans J. Friedrich und Stephan Heinrich, Amtsgericht Mainz HRB 52834. Kontakt in Datenschutzfragen: info@unternehmen-kompetenz-ki.de, Telefon +49 6131 624694-01. `[FACHANWALT]` Ist ein Datenschutzbeauftragter bestellt oder zu bestellen? Falls ja: Kontaktdaten hier eintragen.

§ 1 Gegenstand und Abgrenzung der Rollen

(1) Der Anbieter betreibt die Lern- und Community-Plattform „Unternehmen Kompetenz KI“ unter app.unternehmen-kompetenz-ki.de. Mit einer Mitgliedschaft für ein Unternehmen (Firmenkonto) kann der Kunde Mitarbeitende einladen, ihnen Zugang zu den Inhalten der Plattform geben und ihre Teilnahme einsehen. Grundlage ist der Vertrag über die Mitgliedschaft (Hauptvertrag) samt den Allgemeinen Geschäftsbedingungen des Anbieters.

(2) **Auftragsverarbeitung.** Soweit der Anbieter dabei personenbezogene Daten der Personen, die der Kunde über das Firmenkonto einlädt (Beschäftigte und weitere Personen nach § 5 Abs. 2 und 3, Anlage 1 Ziffer 5), für den Kunden verarbeitet, handelt er als Auftragsverarbeiter. Das betrifft:

1. die Verwaltung der Zugänge im Firmenkonto: Einladen, Zuordnen, Entfernen und Rollen der Mitarbeitenden;
2. die Teilnahmeübersicht für den Firmen-Admin: Stand der Einladung und Zahl der vollständig abgeschlossenen Kurse je Person;
3. Teilnahmebescheinigungen je Person und Kurs, sobald die Plattform sie anbietet;
4. die Mails, die die Plattform dafür im Auftrag des Kunden verschickt, z. B. Einladungen.

Art, Zweck, Datenarten, betroffene Personen und Dauer stehen in **Anlage 1**.

(3) **Eigene Verantwortung des Anbieters.** Für die folgenden Verarbeitungen entscheidet der Anbieter selbst über Zweck und Mittel. Er ist dafür Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, und dieser Vertrag gilt dafür nicht:

1. Abschluss, Durchführung und Abrechnung des Hauptvertrags mit dem Kunden, einschließlich Zahlungsabwicklung, Rechnungen und Kundenkommunikation mit dem Firmen-Admin als Ansprechpartner des Kunden;

2. das Lernen der einzelnen Person auf der Plattform. Dazu gehört der Lernfortschritt je Lektion mit Zeitpunkt, den die Person selbst sieht („Weiter, wo Sie waren“). Der Anbieter zeigt dem Kunden daraus nur die Zahl der abgeschlossenen Kurse nach Absatz 2 Nr. 2, keine Lektionen und keine Zeitpunkte;
3. der Community-Betrieb über Unternehmensgrenzen hinweg: Forum, Profil und Mitgliederverzeichnis, Live-Termine (Einladung, Erinnerung, Durchführung über Zoom, Aufzeichnung), Mitteilungen an die Mitglieder;
4. Support-Anfragen, die eine Person selbst über die Plattform stellt;
5. die Sicherheit der Plattform und die Abwehr von Missbrauch: Anmeldung, Sitzungen, Begrenzung wiederholter Anfragen, Fehler- und Betriebsprotokolle;
6. Veranstaltungen ohne Konto auf der Plattform, z. B. das KI-Frühstück für Unternehmer.

Für diese Verarbeitungen schließt der Anbieter mit jeder Person bei ihrer ersten Anmeldung eigene Nutzungsbedingungen. Er informiert sie in seiner Datenschutzerklärung nach Art. 13 DSGVO.

(4) Der Anbieter gibt dem Kunden **keine** Daten aus den Bereichen nach Absatz 3 weiter. Das gilt besonders für Forumsbeiträge, Support-Anfragen und die Teilnahme an Live-Terminen. Ausgenommen ist eine Weitergabe mit Einwilligung der betroffenen Person oder aufgrund einer gesetzlichen Pflicht.

(5) Richtet der Anbieter künftig Bereiche ein, die nur den Mitarbeitenden eines Kunden offenstehen (z. B. ein firmeneigenes Forum), oder erfasst er die Teilnahme an Live-Terminen für den Kunden, fällt das unter die Auftragsverarbeitung. Der Anbieter passt dann Anlage 1 nach § 14 Abs. 3 an.

[FACHANWALT] Volker (Prüfauftrag 7) hält die Mischrollen für tragfähig. Die eigenen Nutzungsbedingungen je Person hält er für nötig (MUSS), den Lernfortschritt ordnet er der eigenen Verantwortung zu (SOLLTE). Zu prüfen bleibt: Ist die Weitergabe der Zahl abgeschlossener Kurse aus dem eigenen Lernfortschritt an den Kunden sauber begründet (Abs. 2 Nr. 2 in Verbindung mit Abs. 3 Nr. 2)?

§ 2 Dauer

(1) Dieser Vertrag beginnt mit dem Abschluss in der Plattform (§ 14 Abs. 1). Er läuft so lange wie der Hauptvertrag und darüber hinaus, solange der Anbieter noch personenbezogene Daten für den Kunden verarbeitet, etwa bis zur Löschung nach § 12.

(2) Das Recht zur außerordentlichen Kündigung bleibt unberührt, insbesondere bei schweren Verstößen gegen diesen Vertrag oder gegen Datenschutzvorschriften.

§ 3 Weisungen

(1) Der Anbieter verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, auch bei Übermittlungen in Drittländer. Ausgenommen ist eine Verarbeitung, zu der ihn das Recht der Union oder eines Mitgliedstaats verpflichtet. In diesem Fall teilt er dem Kunden die rechtliche Anforderung vor der Verarbeitung mit, sofern das Recht eine solche Mitteilung nicht verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(2) Der Kunde erteilt seine Weisungen

1. abschließend durch diesen Vertrag und den Hauptvertrag;
2. im Einzelfall über die Funktionen der Plattform, die der Firmen-Admin bedient (Einladen, Entfernen, Rolle setzen). Jede Bedienung gilt als dokumentierte Weisung;
3. darüber hinaus in Textform (E-Mail an info@unternehmen-kompetenz-ki.de).

(3) Weisungsberechtigt sind die Firmen-Admins des Kunden, auch soweit der Kunde nach § 5 Abs. 3 für verbundene Unternehmen handelt. Der Kunde sorgt dafür, dass nur Personen Firmen-Admin sind, die für ihn handeln dürfen.

(4) Hält der Anbieter eine Weisung für rechtswidrig, teilt er das dem Kunden unverzüglich mit (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung aussetzen, bis der Kunde die Weisung bestätigt oder ändert.

(5) Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, behandeln die Parteien als Antrag auf eine Leistungsänderung.

§ 4 Pflichten des Anbieters

(1) **Vertraulichkeit.** Der Anbieter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b DSGVO). Zugriff haben nur Personen, die ihn für ihre Aufgabe brauchen.

(2) **Sicherheit.** Der Anbieter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in **Anlage 2** beschrieben sind. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt. Wesentliche Änderungen dokumentiert er und nimmt sie in Anlage 2 auf.

(3) **Zweckbindung.** Der Anbieter nutzt die Daten nach § 1 Abs. 2 nur für die Leistung an den Kunden. Insbesondere nutzt er sie nicht für Werbung, gibt sie nicht an Dritte weiter und verwendet sie nicht zum Training von KI-Modellen. Erlaubt bleiben Kopien für die Datensicherung nach Anlage 2 und anonymisierte Gesamtzahlen. Solche Zahlen dürfen keinen Rückschluss auf einzelne Personen oder auf den Kunden zulassen. Deshalb fasst der Anbieter dafür jeweils mindestens zehn Personen und mehrere Kunden zusammen.

(4) **Unterstützung.** Der Anbieter unterstützt den Kunden nach §§ 9 und 10 bei Betroffenenrechten, bei Pflichten nach Art. 32 bis 36 DSGVO und bei Anfragen der Aufsichtsbehörde, soweit sie diesen Auftrag betreffen.

(5) **Verzeichnis.** Der Anbieter führt ein Verzeichnis der Verarbeitungstätigkeiten, die er für Verantwortliche durchführt (Art. 30 Abs. 2 DSGVO).

(6) **Ort der Verarbeitung.** Der Anbieter verarbeitet die Daten auf Servern in Deutschland. Eine Verarbeitung außerhalb der EU oder des EWR findet nur nach § 8 statt.

§ 5 Pflichten des Kunden

(1) Der Kunde ist dafür verantwortlich, dass die Verarbeitung, die er in Auftrag gibt, zulässig ist. Insbesondere

1. hat er für die Verarbeitung der Beschäftigtendaten eine Rechtsgrundlage;
2. informiert er seine Mitarbeitenden nach Art. 13 DSGVO über die Nutzung der Plattform und über die Teilnahmeübersicht;
3. beteiligt er einen Betriebsrat, soweit das Gesetz das vorsieht. Die Teilnahmeübersicht kann eine technische Einrichtung im Sinne von § 87 Abs. 1 Nr. 6 BetrVG sein.

(2) Der Kunde lädt nur Personen ein, die er für die Plattform einladen darf, und nur mit Adressen, die er dafür verwenden darf. Einladen kann der Firmen-Admin Personen mit einer E-Mail-Adresse unter einer Domain des Kunden (Firmendomain), auch freie Mitarbeitende und Beschäftigte verbundener Unternehmen; nutzt der Kunde keine eigene Domain, einzelne Adressen von Personen, die für ihn tätig sind (AGB § 4 Abs. 3). Der Anbieter prüft die Auswahl nicht. Verlässt eine Person das Unternehmen oder endet ihre Tätigkeit für den Kunden, entfernt der Firmen-Admin sie aus dem Firmenkonto, auch wenn ihre Adresse weiterbesteht.

(3) **Verbundene Unternehmen und freie Mitarbeitende.** Lädt der Kunde Personen ein, die bei einem verbundenen Unternehmen oder als freie Mitarbeitende tätig sind, gilt:

1. Für Beschäftigte eines verbundenen Unternehmens schließt der Kunde diesen Vertrag zugleich im Namen dieses Unternehmens ab und versichert, dazu berechtigt zu sein; andernfalls stellt er sicher, dass die erforderlichen datenschutzrechtlichen Vereinbarungen mit dem verbundenen Unternehmen bestehen, bevor er dessen Beschäftigte einlädt. Weisungen erteilt in beiden Fällen allein der Kunde über seine Firmen-Admins (§ 3 Abs. 3); das verbundene Unternehmen übt seine Rechte aus diesem Vertrag über den Kunden aus.
2. Der Kunde versichert, für die Verarbeitung der Daten aller eingeladenen Personen eine Rechtsgrundlage zu haben und sie nach Art. 13 DSGVO zu informieren (Absatz 1).
3. Der Kunde stellt den Anbieter von Ansprüchen Dritter frei, die darauf beruhen, dass die Voraussetzungen nach Nr. 1 oder 2 nicht vorlagen.

[FACHANWALT] Volker (Prüfauftrag 14.1, MUSS): Jedes Konzernunternehmen ist eigener Verantwortlicher; der Kunde kann für dessen Beschäftigte nicht ohne Weiteres allein handeln. Absatz 3 folgt seinem Vorschlag (Abschluss auch im Namen des verbundenen Unternehmens oder eigene Vereinbarung, Zusicherung, Freistellung). Seine Formulierung „weisungsbefugt oder Einwilligung eingeholt“ für freie Mitarbeitende ist durch die allgemeine Zusicherung einer Rechtsgrundlage ersetzt, weil eine Einwilligung hier nicht die einzige und oft nicht

die passende Grundlage ist. Zu prüfen: Trägt der Abschluss im Namen verbundener Unternehmen per Klick, und genügt die Freistellung?

(4) Der Kunde hält die Zugangsdaten seiner Firmen-Admins geheim. Er informiert den Anbieter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(5) Die Teilnahmeübersicht zeigt, wer eingeladen und angemeldet ist und wie viele Kurse eine Person vollständig abgeschlossen hat. Sie zeigt keine Bewertung, keine Zeiten und keine einzelnen Lektionen. Für die Verwendung der Übersicht ist allein der Kunde verantwortlich. Der Anbieter weist den Firmen-Admin in der Plattform darauf hin, dass eine Auswertung je Person eine eigene Rechtsgrundlage braucht und bei einem Betriebsrat dessen Beteiligung (Betriebsvereinbarung).

§ 6 Kontaktdaten und Kommunikation

(1) Der Anbieter schickt Mitteilungen nach diesem Vertrag an die Firmen-Admins des Kunden, die im Firmenkonto eingetragen sind. Benennt der Kunde in Textform eine andere Adresse für Datenschutzfragen, schickt der Anbieter sie dorthin.

(2) Der Kunde erreicht den Anbieter unter info@unternehmen-kompetenz-ki.de.

§ 7 Unterauftragsverarbeiter

(1) Der Kunde erteilt dem Anbieter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten stehen in **Anlage 3** und gelten als genehmigt.

(2) Der Anbieter informiert den Kunden mindestens **vier Wochen** vorher in Textform, wenn er einen Unterauftragsverarbeiter hinzunehmen oder ersetzen will. Der Kunde kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Die Parteien suchen dann eine Lösung. Kann der Anbieter auf den Unterauftragsverarbeiter nicht verzichten, ohne die vertragsgemäße Leistung zu ändern, und finden die Parteien keine Lösung, kann der Kunde den Hauptvertrag zum Zeitpunkt der Änderung kündigen. Bereits gezahlte Entgelte für die Zeit danach erstattet der Anbieter anteilig. Einen Anspruch darauf, den bisherigen Zustand beizubehalten, hat der Kunde nicht.

(3) Der Anbieter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten wie in diesem Vertrag, insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Bei großen Anbietern geschieht das über deren Standardbedingungen zur Auftragsverarbeitung. Der Anbieter prüft vorher, ob diese Bedingungen gleichwertig sind.

(4) Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Anbieter dem Kunden dafür wie für eigenes Handeln (Art. 28 Abs. 4 Satz 2 DSGVO).

(5) Keine Unterauftragsverarbeitung sind Nebenleistungen, bei denen der Dienstleister keinen Zugriff auf personenbezogene Daten hat, z. B. Telekommunikation oder Wartung von Rechenzentrumsgebäuden. Auch dann sorgt der Anbieter für angemessene Vereinbarungen.

§ 8 Übermittlung in Drittländer

(1) Daten dürfen nur unter den Voraussetzungen der Art. 44 bis 49 DSGVO außerhalb der EU oder des EWR verarbeitet werden. Grundlagen sind ein Angemessenheitsbeschluss, etwa das EU-US Data Privacy Framework für zertifizierte Empfänger, oder die Standardvertragsklauseln der EU-Kommission.

(2) Welche Unterauftragsverarbeiter Daten in einem Drittland verarbeiten und auf welcher Grundlage, steht in Anlage 3.

§ 9 Rechte der betroffenen Personen

(1) Wendet sich eine betroffene Person mit einem Anliegen zur Auftragsverarbeitung an den Anbieter, leitet er es unverzüglich an den Kunden weiter. Er beantwortet es nicht selbst, außer der Kunde weist ihn dazu an. Anliegen zu den Bereichen in eigener Verantwortung (§ 1 Abs. 3) bearbeitet der Anbieter selbst.

(2) Der Anbieter unterstützt den Kunden mit geeigneten Maßnahmen dabei, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch zu ermöglichen (Art. 28 Abs. 3 Satz 2 lit. e DSGVO). Einiges kann der Firmen-Admin selbst erledigen, etwa eine Person aus dem Firmenkonto entfernen. Was dafür nicht ausreicht, erledigt der Anbieter auf Weisung in Textform, in der Regel innerhalb von **zehn Werktagen**.

(3) Der Anbieter kann für Unterstützung, die über die Funktionen der Plattform hinausgeht und deutlichen Aufwand verursacht, eine angemessene Vergütung verlangen. Das gilt nicht, wenn der Aufwand auf einem Verstoß des Anbieters beruht.

§ 10 Meldung von Verletzungen und weitere Unterstützung

(1) Wird dem Anbieter eine Verletzung des Schutzes personenbezogener Daten bekannt, die Daten des Kunden betrifft, meldet er sie dem Kunden **unverzüglich**, möglichst innerhalb von **24 Stunden**, in Textform an die Firmen-Admins (Art. 33 Abs. 2 DSGVO). Die Frist beginnt, sobald der Anbieter von der Verletzung Kenntnis hat. Die Meldung enthält, soweit bekannt,

1. die Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze;
2. eine Ansprechperson;
3. die wahrscheinlichen Folgen;
4. die ergriffenen oder vorgeschlagenen Maßnahmen.

Was noch nicht bekannt ist, reicht er nach, sobald er es weiß.

(2) Der Anbieter ergreift unverzüglich Maßnahmen, um die Daten zu sichern und mögliche Folgen für die betroffenen Personen zu mindern. Er stimmt sie mit dem Kunden ab, soweit das ohne Verzögerung möglich ist.

(3) Der Anbieter unterstützt den Kunden bei dessen Meldung an die Aufsichtsbehörde und bei der Benachrichtigung der betroffenen Personen (Art. 33, 34 DSGVO). Er unterstützt ihn auch bei einer Datenschutz-Folgenabschätzung und einer vorherigen Konsultation (Art. 35, 36 DSGVO), soweit sie die Plattform betreffen. Dafür stellt er die vorhandenen Unterlagen bereit, insbesondere Anlage 2.

(4) Eine Meldung oder Unterstützung nach diesem Paragraphen ist kein Anerkenntnis eines Verschuldens.

§ 11 Nachweise und Kontrollen

(1) Der Anbieter stellt dem Kunden auf Anfrage alle Informationen zur Verfügung, die zum Nachweis seiner Pflichten nach Art. 28 DSGVO nötig sind (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Dazu gehören diese Anlagen, eine aktuelle Liste der Unterauftragsverarbeiter und deren Nachweise, soweit sie vorliegen, z. B. Zertifizierungen der Rechenzentren.

(2) Der Kunde kann die Einhaltung dieses Vertrags überprüfen oder durch einen zur Verschwiegenheit verpflichteten Prüfer überprüfen lassen. Das Recht auf Überprüfungen einschließlich Inspektionen vor Ort bleibt bestehen. Die Parteien gehen dabei so vor:

1. Zuerst beantwortet der Anbieter einen schriftlichen Fragenkatalog des Kunden und legt Nachweise vor.
2. Reicht das für einen begründeten Prüfbedarf nicht aus, ist eine Inspektion möglich. Sie findet nach Anmeldung mit einer Frist von mindestens **vier Wochen** statt, zu den üblichen Geschäftszeiten und ohne Störung des Betriebs. Ausgenommen sind Inspektionen aus konkretem Anlass, etwa nach einer Datenpanne.
3. Ein Prüfer darf kein Wettbewerber des Anbieters sein.

Rechenzentren der Unterauftragsverarbeiter prüft der Kunde anhand ihrer Nachweise und Zertifikate.

(3) Den eigenen Aufwand einer Prüfung trägt jede Partei selbst. Eine Prüfung im Kalenderjahr ist für den Kunden ohne zusätzliche Kosten. Für weitere Inspektionen vor Ort kann der Anbieter eine angemessene Vergütung seines Aufwands verlangen, außer sie haben einen konkreten Anlass in einem Verstoß des Anbieters.

§ 12 Löschung und Rückgabe nach Vertragsende

(1) Mit dem Ende des Hauptvertrags endet der Zugang der Mitarbeitenden über das Firmenkonto. Vor dem Ende kann der Kunde die Teilnahmeübersicht abrufen. Auf Wunsch in Textform, gestellt vor dem Vertragsende oder innerhalb von **30 Tagen** danach, stellt der Anbieter sie ihm als Datei bereit (Rückgabe).

(2) Spätestens **60 Tage** nach dem Vertragsende löscht oder anonymisiert der Anbieter die Daten, die er nach diesem Vertrag für den Kunden verarbeitet hat (Anlage 1). Davon ausgenommen sind Daten, die er nach dem Recht der Union oder eines Mitgliedstaats aufbewahren muss (Art. 28 Abs. 3 Satz 2 lit. g DSGVO). Auf Anfrage bestätigt er die Löschung in Textform.

(3) **Ausnahme Datensicherungen.** Abweichend von Absatz 2 löscht der Anbieter Datensicherungen nicht einzeln. Sie werden nach dem Plan in Anlage 2 unwiederbringlich gelöscht, spätestens **90 Tage** nach ihrer Erstellung. Bis dahin sind sie verschlüsselt und werden ausschließlich für eine Wiederherstellung verwendet, für keinen anderen Zweck. Wird eine Sicherung zurückgespielt, löscht der Anbieter die betroffenen Daten unverzüglich erneut.

(4) **Ausnahme eigener Zugang der Person.** Abweichend von Absatz 2 bleibt das Konto einer Person bestehen, wenn sie unabhängig vom Kunden weiter Zugang zur Plattform hat, etwa durch einen selbst gekauften Einzelkurs oder über das Firmenkonto eines anderen Kunden. Das Konto wird dann nicht mehr im Auftrag des Kunden geführt. Auch in diesem Fall löscht der Anbieter nach Absatz 2 die Zuordnung zum Kunden und alles, was er nach Anlage 1 für den Kunden verarbeitet hat. Konten ohne einen solchen eigenen Zugang löscht der Anbieter mit Ablauf der Frist nach Absatz 2. Für Forumsbeiträge und Lernfortschritt der Person gelten die Nutzungsbedingungen (§ 1 Abs. 3).

(5) Entfernt der Firmen-Admin während der Laufzeit eine Person, endet ihr Zugang sofort. Ihre Zuordnung bleibt als Verlauf bis zum Vertragsende gespeichert, damit Einladungen und Plätze nachvollziehbar sind. Danach gilt Absatz 2. Auf Weisung löscht der Anbieter früher.

§ 13 Haftung

(1) Für Schäden betroffener Personen haften die Parteien nach Art. 82 DSGVO.

(2) Im Verhältnis zwischen den Parteien gelten die Haftungsregeln des Hauptvertrags, soweit dieser Vertrag nichts anderes bestimmt. Eine Haftungsbeschränkung im Hauptvertrag gilt nicht für Ansprüche betroffener Personen nach Art. 82 DSGVO. Sie gilt auch nicht für die Haftung wegen Vorsatz, grober Fahrlässigkeit oder der Verletzung von Leben, Körper oder Gesundheit.

(3) Wird eine Partei von einer betroffenen Person in Anspruch genommen, obwohl die andere Partei den Schaden zu vertreten hat, stellt die andere Partei sie im Umfang ihrer Verantwortung frei (Art. 82 Abs. 5 DSGVO).

`[FACHANWALT]` Die Haftungsklausel ist der wichtigste Punkt für die Prüfung. Volker (Prüfauftrag 9) hält die Grundstruktur für tragfähig. Eine Grenze in Höhe der Jahrespauschale (599 €) hält er für zu niedrig: Sie wirke faktisch wie ein vollständiger Haftungsausschluss und sei nach § 307 BGB riskant. Er schlägt einen Mindestbetrag vor (z. B. 5.000 €) oder das Jahresentgelt je Kunde mit einer Untergrenze. Zu entscheiden sind Höhe und Ort der Regel (AGB oder AVV).

§ 14 Schlussbestimmungen

(1) **Abschluss.** Ein Firmen-Admin schließt diesen Vertrag in elektronischem Format in der Plattform ab, indem er ihn ausdrücklich bestätigt (Art. 28 Abs. 9 DSGVO). Dabei versichert er, dass er den Kunden vertreten darf oder von einer vertretungsberechtigten Person des Kunden dazu ermächtigt ist. Der Anbieter speichert als Nachweis:

- die Fassung und den Prüfwert (Hash) des Vertragstexts;
- den Zeitpunkt;
- die bestätigende Person und das Unternehmen.

Der Kunde kann den Vertrag jederzeit in der Plattform als Datei abrufen und erhält eine Bestätigung per E-Mail. Wünscht er eine unterschriebene Ausfertigung, stellt der Anbieter sie zusätzlich bereit.

(2) **Vorrang.** Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes dem Hauptvertrag und den AGB vor. Allgemeine Geschäftsbedingungen des Kunden gelten nicht.

(3) **Änderungen.** Änderungen und Ergänzungen bedürfen der Textform. Das gilt auch für einen Verzicht auf diese Form. Die Anlagen 2 und 3 kann der Anbieter nach § 4 Abs. 2 und § 7 fortschreiben. Andere Änderungen dieses Vertrags werden erst wirksam, wenn ein Firmen-Admin die neue Fassung in der Plattform bestätigt. Bis dahin gilt die bisherige Fassung weiter. Stimmt der Kunde einer Änderung nicht zu, die das Gesetz oder eine Entscheidung einer Aufsichtsbehörde erzwingt, kann jede Partei den Hauptvertrag zum Zeitpunkt der Änderung kündigen.

(4) **Salvatorische Klausel.** Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam. An ihre Stelle tritt eine Regelung, die den Anforderungen von Art. 28 DSGVO entspricht und dem Zweck am nächsten kommt.

(5) **Recht und Gerichtsstand.** Es gilt deutsches Recht. Gerichtsstand ist Mainz, soweit der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

Anlagen

- Anlage 1 – Gegenstand, Art und Zweck der Verarbeitung, Datenarten, betroffene Personen, Dauer (`Anlage-1_Verarbeitung.md`)
- Anlage 2 – Technische und organisatorische Maßnahmen (`Anlage-2_TOM.md`)
- Anlage 3 – Unterauftragsverarbeiter (`Anlage-3_Unterauftragsverarbeiter.md`)

Anlage 1 zum AVV – Gegenstand, Art und Zweck der Verarbeitung

Zum Vertrag über die Auftragsverarbeitung, Fassung **AVV-UKKI 0.9.1 (Entwurf)** · Stand 22.10.2026 Grundlage: Programmstand 0.9.0 der Plattform (app.unternehmen-kompetenz-ki.de)

1. Gegenstand

Der Anbieter stellt dem Kunden ein **Firmenkonto** auf der Plattform „Unternehmen Kompetenz KI“ bereit. Damit kann der Kunde

- Personen mit einer E-Mail-Adresse unter seinen Firmendomains einladen (ohne eigene Domain: einzelne Adressen), im Rahmen der gebuchten Plätze (Grundlizenz 20 Plätze, dazu Blöcke zu je 10 Plätzen), und ihnen Zugang zu den Kursen der Mitgliedschaft geben,
- Firmen-Admins bestimmen,
- Mitarbeitende wieder entfernen,
- die Teilnahme seiner Mitarbeitenden einsehen.

2. Art der Verarbeitung

Erheben (Eingabe durch den Firmen-Admin, Anmeldung der eingeladenen Person), Speichern, Ordnen, Abfragen, Verwenden (Anzeigen, Versand von Mails), Einschränken, Löschen und Datensicherung.

3. Zwecke

Nr.	Zweck	Was die Plattform dafür tut
Z1	Zugänge des Kunden verwalten	Einladung per Mail, Zuordnung zum Firmenkonto, Rollen „Firmen-Admin“ und „Mitarbeiter/in“, Entfernen mit sofortigem Ende des Zugangs, Prüfung der erlaubten E-Mail-Domains und der Platzgrenze
Z2	Zugang über das Firmenkonto	Freischaltung der Kurse der Mitgliedschaft für alle aktiv zugeordneten Personen; Ende des Zugangs beim Entfernen oder Vertragsende
Z3	Teilnahmeübersicht für den Kunden	Für den Firmen-Admin eine Liste der Mitarbeitenden mit Stand der Einladung bzw. Anmeldung und der Zahl vollständig abgeschlossener Kurse. Die Zahl ermittelt die Plattform aus dem Lernfortschritt der Person, den der Anbieter in eigener Verantwortung führt (§ 1 Abs. 3 Nr. 2 AVV)
Z4	Teilnahmebescheinigung (geplant, noch nicht gebaut)	Bescheinigung je Person und abgeschlossenem Kurs als PDF für das Schulungsverzeichnis des Kunden. Sie bescheinigt die Maßnahme, keine Kompetenz

4. Was der Firmen-Admin sieht – und was nicht

Sieht der Firmen-Admin	Sieht der Firmen-Admin nicht
Vorname, Nachname, E-Mail-Adresse der Mitarbeitenden seines Unternehmens	einzelne Lektionen, Reihenfolge, Zeitpunkte, Dauer
Rolle (Firmen-Admin oder Mitarbeiter/in), dabei seit	Ergebnisse, Bewertungen, Ranglisten (gibt es nicht)
eingeladen oder angemeldet, Konto aktiv	Forumsbeiträge, Profilangaben über das hinaus, was alle Mitglieder sehen
Zahl vollständig abgeschlossener Kurse	Support-Anfragen, Teilnahme an Live-Terminen
Plätze „x von y“ (belegt von gebucht)	Anmeldezeiten, Geräte, IP-Adressen

Auf der Seite steht sichtbar der Hinweis, dass die Übersicht nur die Teilnahme zeigt und keine Leistung.

5. Kategorien betroffener Personen

- Beschäftigte des Kunden, die der Kunde einlädt (Mitarbeitende), auch Auszubildende
- Firmen-Admins des Kunden
- freie Mitarbeitende des Kunden mit einer Adresse unter einer Firmendomain oder, wenn der Kunde keine eigene Domain nutzt, mit einzeln eingeladener Adresse
- Beschäftigte verbundener Unternehmen des Kunden mit einer Adresse unter einer Firmendomain (§ 5 Abs. 3 AVV)

6. Datenarten

Datenart	Einzelheiten	Zweck
Stammdaten	Vorname, Nachname, dienstliche E-Mail-Adresse	Z1–Z4
Zuordnung zum Kunden	Firmenkonto, Rolle, eingeladen von (Person), seit, beendet am und von wem	Z1, Z3
Kontostand	Einladung offen/angenommen, Konto aktiv, Zeitpunkt der letzten Anmeldung (nur intern, nicht für den Kunden sichtbar)	Z1, Z3
Zugangsdaten	Passwort nur als Hash (scrypt), zweiter Faktor (falls eingerichtet), Einmal-Links nur als Hash	Z1
Teilnahmedaten	Zahl vollständig abgeschlossener Kurse je Person; künftig Bescheinigung je Kurs mit Datum	Z3, Z4
Versandprotokoll	je Mail: Empfängeradresse, Betreff, Art, Status, Zeitpunkt, ggf. Fehlertext; **kein Mailinhalt**	Z1

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) verarbeitet der Anbieter nicht. Der Kunde gibt keine solchen Daten ein.

Nicht Gegenstand dieses Vertrags (eigene Verantwortung des Anbieters, § 1 Abs. 3 AVV): Lernfortschritt je Lektion mit Zeitpunkt (dient der Person selbst, „Weiter, wo Sie waren“), Profil (Foto, Firma, Funktion, Vorstellung, LinkedIn, Eintrag im Mitgliederverzeichnis), Forumsbeiträge und Anhänge, Benachrichtigungen, Support-Anfragen, Einladungen und Erinnerungen zu Live-Terminen und die Teilnahme daran, Mitteilungen an Mitglieder, Einstellungen zu Mails, Kalender-Abo, Sitzungen und Sicherheitsprotokolle, Zahlungs- und Vertragsdaten.

[FACHANWALT] Volker (Prüfauftrag 7) ordnet den Lernfortschritt je Lektion der eigenen Verantwortung des Anbieters zu, weil der Kunde ihn weder anweist noch einsieht. Zu bestätigen: Darf der Anbieter daraus die Zahl abgeschlossener Kurse für den Kunden ableiten?

7. Dauer und Löschung

Was	Wie lange
Zuordnung zum Firmenkonto, Teilnahmedaten, Bescheinigungen	Laufzeit des Hauptvertrags; danach Löschung oder Anonymisierung spätestens nach 60 Tagen (§ 12 AVV)
Zuordnung einer entfernten Person	als Verlauf bis zum Vertragsende, auf Weisung früher
Versandprotokoll	12 Monate (automatische Löschung im Bau, Anlage 2 L5; bis dahin auf Weisung von Hand)
Datensicherungen	auf dem Server 7 Tagesstände; verschlüsselte Kopie beim Anbieter bis 90 Tage (Anlage 2)

8. Ort der Verarbeitung

Server in einem Rechenzentrum in Deutschland (Anlage 3). Für Übermittlungen in Drittländer gilt § 8 AVV in Verbindung mit Anlage 3.

Anlage 2 zum AVV – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Zum Vertrag über die Auftragsverarbeitung, Fassung **AVV-UKKI 0.9.1 (Entwurf)** · Stand 22.10.2026 Grundlage: Programmstand 0.9.0, Betriebsdokumentation `app/README.md`

> *Diese Anlage beschreibt, was tatsächlich gebaut ist und gemessen wurde. Wo etwas fehlt, steht es im Abschnitt 11 „Bekannte Lücken und Maßnahmenplan“. Marken für die interne Prüfung:* `[PRÜFEN]` *(Tatsache vor Freigabe nachmessen),* `[FACHANWALT]`*. Beide entfallen in der freigegebenen Fassung.*

---

0. Rahmen und Schutzbedarf

- **System:** Webanwendung (Next.js, PostgreSQL) in Docker-Containern auf einem virtuellen Server, den der Anbieter bei der IONOS SE betreibt (Rechenzentrum Deutschland). Auf demselben Server laufen weitere Anwendungen des Anbieters, jede in einem eigenen, abgeschotteten Compose-Projekt.
- **Daten:** geschäftliche Kontaktdaten und Lernteilnahme von Beschäftigten, keine besonderen Kategorien (Art. 9 DSGVO), keine Zahlungsdaten (die liegen nur beim Zahlungsdienstleister).
- **Schutzbedarf:** normal. Besonderes Augenmerk liegt auf der Vertraulichkeit der Teilnahmedaten gegenüber Dritten und der Trennung zwischen den Firmenkonten.

1. Vertraulichkeit – Zutrittskontrolle (Räume, in denen Daten verarbeitet werden)

- Server im Rechenzentrum der IONOS SE in Deutschland. Den physischen Schutz leistet IONOS nach ihren eigenen Maßnahmen (Zertifizierung nach ISO/IEC 27001). `[PRÜFEN]` Zertifikat und IONOS-AVV für den Vertrag von cb-vps abrufen und ablegen.
- Beim Anbieter selbst liegen keine Server. Die Verwaltung erfolgt über verschlüsselte Verbindungen von den Arbeitsgeräten der Geschäftsführung.

2. Vertraulichkeit – Zugangskontrolle (Zugang zu den Systemen)

Server

- Anmeldung per SSH nur mit Schlüssel, Passwort-Anmeldung abgeschaltet, direkte root-Anmeldung abgeschaltet. Fehlversuche sperrt fail2ban.
- Einen Server-Zugang hat nur ein persönlicher Verwaltungsbenutzer der Geschäftsführung. `[PRÜFEN]` Bestätigen, dass außer Stephan Heinrich niemand einen Schlüssel hat.
- Von außen erreichbar sind nur HTTPS (443) und die Weiterleitung von HTTP (80) über einen Reverse-Proxy (Traefik). Die Datenbank hat keinen öffentlichen Port.

Anwendung

- Konten entstehen nur durch Einladung oder Kauf, nicht durch freie Registrierung.
- Passwörter werden nur als Hash gespeichert (scrypt, speicherhart, mit Salz).
- Einladungs- und Passwort-Links gelten einmal und höchstens 7 Tage. In der Datenbank steht nur ihr Hash. Eingelöst wird ein Link erst per Knopfdruck, nicht schon beim Aufruf. So können Link-Scanner in Firmenpostfächern ihn nicht verbrauchen.
- Sitzungen: signiertes Cookie (HttpOnly) und Eintrag in der Datenbank, dort nur als Hash. Laufzeit 30 Tage. Abmelden beendet die Sitzung.
- Zweiter Faktor (TOTP mit Notfallcodes) für Administratoren des Anbieters ist eingebaut. Zur Pflicht wird er erst noch (Abschnitt 11).
- Formulare prüfen die Herkunft der Anfrage (Schutz gegen Cross-Site-Request-Forgery).
- Wiederholte Versuche werden gebremst (Anmeldung über Einladung, Forum, Formulare).

3. Vertraulichkeit – Zugriffskontrolle (Berechtigungen)

- **Eine Stelle für Zugriffsrechte:** Ob jemand einen Kurs, einen Termin oder einen Bereich sehen darf, entscheidet die Plattform an genau einer Stelle im Code, und zwar auf dem Server, nicht nur in der Anzeige. Wer keinen Zugang hat, erhält „nicht gefunden“.
- **Rollen:** Administratoren des Anbieters (derzeit die zwei Geschäftsführer); Firmen-Admins (nur das eigene Firmenkonto); Mitglieder (nur eigene Daten und freigegebene Inhalte).
- **Trennung der Firmenkonten:** Ein Firmen-Admin sieht nur die Personen, die seinem Firmenkonto aktiv zugeordnet sind. Jede Person gehört höchstens einem Firmenkonto aktiv an. Das sichert die Datenbank selbst ab.
- **Datensparsame Teilnahmeübersicht:** nur Einladungsstand und Zahl abgeschlossener Kurse, keine Lektionen und keine Zeiten (Anlage 1, Ziffer 4).
- **Eingeladen werden darf nur mit Adressen der Firmendomain.** Bei Freemail-Adressen gibt die Plattform keine Domain frei, dann sind nur einzelne Adressen möglich. Die Platzgrenze prüft der Server mit einer Sperre gegen gleichzeitige Einladungen.
- **Testansicht** („Ansehen als“) nur für Administratoren des Anbieters, für Support und Fehlersuche. Ein roter Balken kennzeichnet sie. In der Testansicht sind keine schreibenden Aktionen im Namen der Person möglich.
- **Dateien** (Material, Anhänge, Profilfotos) gibt die Plattform nur nach Prüfung des Zugriffsrechts heraus, unter zufälligen Schlüsseln. Hochgeladene Dateien prüft sie am Dateiinhalt, nicht an der Endung.

4. Vertraulichkeit – Trennungskontrolle

- Eigenes Docker-Compose-Projekt nur für diese Plattform, mit eigener Datenbank in eigenem Container.
- Eigenes Netz zum Reverse-Proxy. Die Datenbank liegt in einem internen Netz, das nur die Plattform erreicht, nicht die anderen Anwendungen auf dem Server.
- Die Plattform meldet sich an der Datenbank mit einem eigenen Benutzer ohne Superuser-Rechte an.
- Container laufen nicht als root, sondern als eigener Benutzer (uid 1001). Der Programmcode ist für diesen Benutzer nicht veränderbar, schreiben darf er nur in Zwischenspeicher und Dateiablage. Geprüft beim ersten Livegang am 18.10.2026.
- Zugangsdaten (Datenbank, Mail, Zahlungsdienst) liegen nur in einer Konfigurationsdatei auf dem Server (Rechte 600), nie im Abbild und nie im Code-Archiv. Jeder Container erhält nur die Zugangsdaten, die er braucht.
- Tests laufen mit Wegwerfkonten (Adressen `@example.com`), die direkt danach gelöscht werden. Echte Personendaten werden nicht zum Testen verwendet.

5. Vertraulichkeit – Pseudonymisierung und Verschlüsselung

- **Übertragung:** durchgehend TLS (HTTPS), Zertifikat von Let's Encrypt mit automatischer Erneuerung. HSTS ist für ein Jahr gesetzt.
- **Mails:** Versand über den Mailserver des Anbieters mit TLS (SMTP über SSL, Port 465).
- **Tokens und Geheimnisse** in Links (Einladung, Abbestellen, Kalender-Abo) werden als Hash oder als signierter Wert geführt, nicht im Klartext gespeichert. Seiten mit solchen Links geben keinen Referrer weiter.
- **Datensicherungen** sind verschlüsselt (AES-256, Schlüsselableitung PBKDF2), siehe Abschnitt 8.
- **Speicher auf dem Server:** keine zusätzliche Verschlüsselung des Datenträgers (Abschnitt 11).

6. Integrität – Weitergabekontrolle

- Weitergabe nur an die Unterauftragsverarbeiter in Anlage 3, jeweils verschlüsselt übertragen.
- **Betriebsmeldungen an die Administratoren** (über Slack) enthalten keine E-Mail-Adressen und keine Nachrichtentexte. Sie nennen nur Art, Nummer, Firmenname, Vorname mit Initial und einen Link in die Verwaltung. Was nach einer Adresse aussieht, schwärzt die Plattform zusätzlich automatisch.
- Das **Versandprotokoll** speichert keine Mailinhalte, nur Empfänger, Betreff, Art, Status und Zeitpunkt.

- Kein Tracking, keine Analysedienste, keine Werbe-Cookies. Die Schriften liefert die Plattform selbst aus, nicht über Google. Videos (Vimeo) laufen mit „Do Not Track“.
- Kein Verkauf und keine Weitergabe von Daten zu Werbezwecken.

7. Integrität – Eingabekontrolle (Nachvollziehbarkeit)

- **Firmenkonto:** Jede Zuordnung speichert, wer eingeladen hat, seit wann, wann und durch wen sie endete. Einträge werden beendet, nicht gelöscht.
- **Zugänge (Tags):** Jede Vergabe speichert Herkunft (Kauf, von Hand, Einladung, Übernahme), wer vergeben hat, bis wann und wer sie beendet hat.
- **Versandprotokoll** je Mail mit Status „gesendet“, „Fehler“ oder „nur protokolliert“.
- **Zahlungsereignisse** einmalig und mit Ergebnis protokolliert.
- Betriebsmeldungen mit Zustellweg und Grund (die letzten 100 in der Verwaltung).
- Es gibt kein vollständiges Protokoll darüber, welcher Administrator wann welche Daten angesehen hat (Abschnitt 11).

8. Verfügbarkeit und Belastbarkeit

- **Tägliche Sicherung** um 03:50 Uhr: Datenbank und Dateiablage, beim Erstellen verschlüsselt. Ein unverschlüsselter Abzug entsteht zu keinem Zeitpunkt, auch nicht vorübergehend. Nach jedem Lauf entschlüsselt ein Prüfschritt die Sicherung zur Probe und zählt die Tabellen.
- Auf dem Server liegen die letzten **7 Stände**. Ein Gerät des Anbieters holt die Sicherungen täglich ab (holen, nicht schieben: auf dem Server liegt kein Zugang zum Ablageort). Dort werden sie verschlüsselt **bis zu 90 Tage** aufbewahrt. `[PRÜFEN]` Aufbewahrungsdauer am Ablageort messen und technisch begrenzen.
- Der Schlüssel liegt auf dem Server nur für den Sicherungsdienst lesbar (Rechte 600) und getrennt davon in einem Passwortmanager. `[PRÜFEN]` Eintrag im Passwortmanager bestätigen.
- **Wiederherstellung geprobt** am 18.10.2026 (Datenbank vollständig zurückgelesen).
- Container starten nach Absturz oder Neustart des Servers automatisch neu. Eine Gesundheitsabfrage meldet, ob die Datenbank antwortet.
- Mails gehen über eine Warteschlange: Fällt der Versand aus, gehen sie später, ohne doppelt zu gehen.
- **Aktualisierungen:** Webframework und Bibliotheken werden in Versionen betrieben, in denen bekannte kritische Lücken geschlossen sind (u. a. CVE-2025-55182 und CVE-2025-29927). Sicherheitsupdates des Betriebssystems spielt der Server automatisch ein. `[PRÜFEN]` unattended-upgrades auf cb-vps bestätigen.

9. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- **Gegenprobe vor jedem Livegang und nach jedem Umbau**, gemessen und nicht angenommen. Geprüft wird: Container nicht als root, Programmcode nicht beschreibbar, keine Zugangsdaten im Abbild.
- **Automatische Prüfungen** im Code vor dem Ausrollen: Zugriffsregeln, Datenbankabfragen, Hilfetexte, Anrede.
- **Versionsverwaltung** (Git) für jeden Programmstand, Ausrollen nur über ein festes Skript.
- Diese Anlage wird bei wesentlichen Änderungen, mindestens jährlich, überprüft. Verantwortlich: Geschäftsführung der Content Butler GmbH. Nächste Prüfung: Oktober 2027.

10. Organisatorische Maßnahmen

- Zugriff auf Personendaten haben nur die Geschäftsführer des Anbieters. Weitere Personen erhalten Zugriff nur nach schriftlicher Verpflichtung auf die Vertraulichkeit.
- Hausregeln für den Betrieb, schriftlich festgehalten: kein Dienst als root; jede Anwendung im eigenen Netz; keine Zugangsdaten in Sicherungen; nie ein unverschlüsselter Datenbankabzug; Zugangsdaten nie über die Kommandozeile; Ausgaben von Prüfbefehlen ohne Geheimnisse und mit maskierten Adressen.
- Datenpannen meldet der Anbieter nach § 10 AVV. Für Ausfälle und Auffälligkeiten erhalten die Administratoren automatische Meldungen.

11. Bekannte Lücken und Maßnahmenplan

Nr.	Lücke	Maßnahme	Stand
L1	Zweiter Faktor für Administratoren ist eingebaut, aber noch keine Pflicht	`ZWEITFAKTOR_PFLICHT=1` setzen, sobald beide Administratoren ihn eingerichtet haben	offen, **muss vor dem ersten Abschluss geschlossen sein**
L2	Für Firmen-Admins gibt es keinen zweiten Faktor	Zweiten Faktor für Firmen-Admins anbieten (freiwillig)	offen, Entscheidung
L3	Keine Löschfunktion für Personen und Firmenkonten; Zuordnungen bleiben als Verlauf (Firmenkonten sind gegen Löschen gesperrt)	Löschen bzw. Anonymisieren einer Person (Art. 17 DSGVO), auf Weisung und nach Vertragsende (§ 12 AVV)	offen, **muss vor dem ersten Abschluss geschlossen sein**
L4	Keine Rückgabe-Datei für die Teilnahmeübersicht	Export als CSV für den Firmen-Admin	offen
L5	Versandprotokoll ohne Löschfrist (nur beim KI-Frühstück gibt es eine)	Frist 12 Monate, Löschung im Versandlauf. Bis dahin: Protokoll enthält keine Mailinhalte; Löschung von Hand auf Weisung	bis 31.12.2026 (Vorschlag)
L6	Kein Protokoll über das Ansehen von Daten durch Administratoren (Testansicht, Personenseite)	Protokoll der Testansicht und der Verwaltung von Firmenkonten. Bis dahin: nur zwei Administratoren (Geschäftsführer), Testansicht nur für Support und Fehlersuche	bis 31.12.2026 (Vorschlag)
L7	Keine Verschlüsselung des Datenträgers auf dem Server	Restrisiko: keine Art.-9-Daten; Ausgleich durch Rechenzentrum in Deutschland, Zugangskontrolle und verschlüsselte Sicherungen; nachträglich bei einem laufenden virtuellen Server nicht möglich. Bei einem Serverumzug verschlüsselten Datenträger vorsehen	Restrisiko, bei nächstem Serverwechsel
L8	Externe Erreichbarkeitsüberwachung für die Plattform nicht belegt	`[PRÜFEN]` Prüfen, ob ein Uptime-Monitor die Plattform abfragt; sonst einrichten	offen
L9	Zugriffsprotokolle des Reverse-Proxys (IP-Adressen): Speicherung und Frist nicht dokumentiert	`[PRÜFEN]` Traefik-Zugriffslog auf cb-vps prüfen, Frist festlegen	offen
L10	Aufbewahrung der abgeholten Sicherungen nicht technisch begrenzt	Abholung so einstellen, dass ältere Stände nach 90 Tagen gelöscht werden	offen
L11	Teilnahmebescheinigung noch nicht gebaut	Erst mit dem Bau in Anlage 1 aufnehmen (Zweck Z4)	geplant

Anlage 3 zum AVV – Unterauftragsverarbeiter

Zum Vertrag über die Auftragsverarbeitung, Fassung **AVV-UKKI 0.9.1 (Entwurf)** · Stand 22.10.2026

> *Angaben zu Vertragspartnern, Standorten und Übermittlungsgrundlagen sind vor der Freigabe beim jeweiligen Anbieter nachzuprüfen ([PRÜFEN]): AV-Vertrag bzw. DPA als PDF ablegen, Eintrag im Register des EU-US Data Privacy Framework (dataprivacyframework.gov/list) nachsehen, Liste der Sub-Dienstleister des Anbieters ablegen. Die Marken entfallen in der freigegebenen Fassung.*

1. Genehmigte Unterauftragsverarbeiter

Nr.	Unternehmen	Leistung	Betroffene Daten aus Anlage 1	Ort der Verarbeitung	Grundlage bei Drittland
U1	**IONOS SE**, Elgendorfer Str. 57, 56410 Montabaur	Betrieb des virtuellen Servers (Hosting)	alle Daten nach Anlage 1, als gespeicherte Daten auf dem Server	Rechenzentrum in Deutschland	entfällt
U2	**STRATO GmbH**, Otto-Ostrowski-Str. 7, 10249 Berlin [PRÜFEN] Firma und Anschrift laut Vertrag	Mailserver für den Versand (z. B. Einladungen) und das Postfach info@unternehmen-kompetenz-ki.de	Name und E-Mail-Adresse der Empfänger, Inhalt der Mails	Deutschland [PRÜFEN]	entfällt
U3	**Vimeo.com, Inc.**, New York, USA [PRÜFEN] Vertragspartner für EU-Kunden	Wiedergabe der Kursvideos im eingebetteten Player	technische Daten beim Abspielen (IP-Adresse, Gerät und Browser, Wiedergabe). Einstellungen: Player mit `dnt=1` („Do Not Track“: keine Cookies und keine Nutzungsauswertung durch Vimeo), Videos auf Vimeo verborgen und nur auf app.unternehmen-kompetenz-ki.de abspielbar. Darüber hinaus gibt der Anbieter keine Daten an Vimeo, insbesondere keine Namen und E-Mail-Adressen	USA	[PRÜFEN] DPF-Zertifizierung; sonst Standardvertragsklauseln im DPA von Vimeo
U4	**Slack Technologies** (Salesforce), Vertragspartner [PRÜFEN] (für EU-Kunden in der Regel Slack Technologies Limited, Dublin)	interne Betriebsmeldungen an die Administratoren des Anbieters	nur Firmenname, Vorname und Initial des Nachnamens, Art des Vorgangs (z. B. „Platzgrenze erreicht“, „Einladung gescheitert“). Keine E-Mail-Adressen, keine Teilnahmedaten	USA möglich	[PRÜFEN] DPF-Zertifizierung von Salesforce/Slack; Standardvertragsklauseln im DPA

U5	**Dropbox** – [OFFEN] Das Konto „Dropbox-CMS“ gehört **nicht** der Content Butler GmbH, sondern Stephan Heinrich / HMC (Auskunft Stephan, 21.10.2026). Vor Abschluss: entweder Vereinbarung GmbH <-> Kontoinhaber (HMC als weiterer Unterauftragsverarbeiter, Dropbox dahinter) oder eigener Ablageort der GmbH. Vertragspartner bei Dropbox für EU-Kunden in der Regel Dropbox International Unlimited Company, Dublin	Ablage der täglich abgeholten Datensicherungen	alle Daten nach Anlage 1, ausschließlich verschlüsselt übertragen und abgelegt (AES-256). Der Schlüssel verbleibt beim Anbieter, ein Zugriff auf Klartextinhalte ist für Dropbox technisch ausgeschlossen. Dropbox verarbeitet Metadaten (Dateiname mit Datum, Größe, Zeitpunkt, Konto)	EU und USA möglich	[PRÜFEN] DPF-Zertifizierung; Standardvertragsklauseln im DPA

2. Hinweise zu Drittländern

- Die Plattform und ihre Datenbank laufen in Deutschland. Daten aus Anlage 1 erreichen ein Drittland nur in drei Fällen: beim Abspielen eines Videos (U3), in knapper Form in Betriebsmeldungen (U4) und verschlüsselt in der Sicherungsablage (U5).
- Grundlage einer Übermittlung in die USA ist vorrangig der Angemessenheitsbeschluss zum EU-US Data Privacy Framework (Art. 45 DSGVO), soweit der Empfänger zertifiziert ist. Der Anbieter prüft den Status je Empfänger im offiziellen Register und hält das Ergebnis mit Datum fest. Sonst und ergänzend gelten die Standardvertragsklauseln der EU-Kommission (Modul 3, Auftragsverarbeiter an Unterauftragsverarbeiter), die die Anbieter in ihre DPA einbeziehen. Für Empfänger, bei denen die Übermittlung auf den Standardvertragsklauseln beruht, dokumentiert der Anbieter eine Bewertung der Übermittlung (Transfer Impact Assessment). Für den Fall, dass das Data Privacy Framework entfällt, hält er diese Bewertung für alle US-Empfänger vor.
- Ergänzende Maßnahmen: Datensparsamkeit (U3 ohne Namen, U4 ohne Adressen und Inhalte), Verschlüsselung bei der Übertragung, bei U5 Verschlüsselung der Daten mit einem Schlüssel, den nur der Anbieter hat.

3. Dienste in eigener Verantwortung des Anbieters (keine Unterauftragsverarbeiter)

Diese Dienste setzt der Anbieter für Verarbeitungen ein, für die er selbst verantwortlich ist (§ 1 Abs. 3 AVV). Sie erhalten keine Daten aus Anlage 1 im Auftrag des Kunden. Der Anbieter nennt sie hier nur, damit das Bild vollständig ist:

Dienst	Wofür	Hinweis
Stripe (Stripe Payments Europe Ltd., Dublin)	Zahlung, Rechnungen, Kundenportal für den Hauptvertrag	Vertragsdaten des Kunden und Kontaktdaten des Käufers bzw. Firmen-Admins
Zoom (Zoom Communications, Inc., USA)	Durchführung der Live-Termine der Community im Konto des Anbieters	Wer an einem Termin teilnimmt, nutzt Zoom selbst. Die Plattform meldet dem Kunden keine Teilnahme an Terminen

Die Plattform selbst nutzt keine KI-Dienste, um Daten aus Anlage 1 zu verarbeiten.

4. Änderungen

Neue oder geänderte Unterauftragsverarbeiter kündigt der Anbieter nach § 7 Abs. 2 AVV mindestens vier Wochen vorher an. Die jeweils aktuelle Fassung dieser Anlage steht in der Plattform unter dem Vertrag.

Wer ist wofür verantwortlich? – Erläuterung zum Firmenkonto

Stand 22.10.2026 · gehört zum AVV-UKKI 0.9.1 (Entwurf) · gedacht für Firmenkunden und als Begründung für den Fachanwalt

Kurz gesagt

Auf der Plattform gibt es zwei Arten von Daten, und für sie gelten unterschiedliche Rollen:

	Ihre Sache – wir arbeiten in Ihrem Auftrag	**Unsere Sache – wir sind selbst verantwortlich**
Wer ist verantwortlich?	Ihr Unternehmen (Verantwortlicher)	Content Butler GmbH (Verantwortliche)
Unsere Rolle	Auftragsverarbeiter nach Art. 28 DSGVO	eigener Verantwortlicher nach Art. 4 Nr. 7 DSGVO
Was gehört dazu?	Wen Sie einladen und entfernen, Rollen im Firmenkonto, Ihre Teilnahmeübersicht (Zahl abgeschlossener Kurse), Bescheinigungen, Einladungsmails	Vertrag und Abrechnung mit Ihnen, Lernfortschritt je Lektion (für die Person selbst), Forum, Profil und Mitgliederverzeichnis, Live-Termine, Mitteilungen, Support, Sicherheit der Plattform, KI-Frühstück
Grundlage	der AV-Vertrag	unsere Datenschutzerklärung
Wer sieht die Daten?	Ihre Firmen-Admins (nur die Teilnahmeübersicht) und unsere Administratoren	die Community nach deren Regeln und unsere Administratoren, **nicht** Ihr Unternehmen

Warum diese Aufteilung?

Die Teilnahme Ihrer Mitarbeitenden ist Ihre Sache. Sie entscheiden, wer Zugang bekommt, und Sie wollen nachweisen können, dass Ihr Team an der Weiterbildung teilnimmt, etwa für Ihr Schulungsverzeichnis zur KI-Kompetenz (Art. 4 KI-Verordnung). Wir führen diese Daten nur für Sie und nach Ihrer Weisung. Ohne Ihr Firmenkonto würden wir sie nicht erheben. Das ist der klassische Fall der Auftragsverarbeitung, und dafür brauchen wir den AV-Vertrag.

Der Lernfortschritt im Einzelnen ist Sache der Person und unsere. Welche Lektion jemand wann erledigt hat, speichern wir, damit die Person dort weitermachen kann, wo sie war. Sie sehen diese Einzelheiten nicht und weisen sie auch nicht an. Deshalb führen wir sie in eigener Verantwortung, auf Grundlage der Nutzungsbedingungen, die jede Person bei ihrer ersten Anmeldung annimmt. Für Ihre Übersicht leiten wir daraus nur ab, wie viele Kurse jemand vollständig abgeschlossen hat.

Die Community ist unsere Sache. Im Forum, in den Live-Terminen und im Mitgliederverzeichnis treffen sich Menschen aus vielen Unternehmen. Die Regeln dafür legen wir fest, nicht Sie. Ein Forumsbeitrag Ihrer Mitarbeiterin gehört zur Community und nicht in Ihre Personalakte. Deshalb geben wir Ihnen solche Daten **nicht** weiter: keine Beiträge, keine Support-Anfragen, keine Teilnahme an Live-Terminen. So bleibt die Community ein offener Raum. Ihr Betriebsrat muss nicht befürchten, dass jede Frage im Forum beim Arbeitgeber landet.

Vertrag und Abrechnung sind unsere Sache. Den Vertrag schließen wir mit Ihrem Unternehmen, und die Rechnungen stellen wir aus. Dafür verarbeiten wir die Daten des Käufers und der Firmen-Admins als Ihre Ansprechpartner in eigener Verantwortung.

Was Ihr Firmen-Admin sieht

Unter „Firmenkonto“ (`/firma`) sieht der Firmen-Admin:

- die eingeladenen Personen mit Name, E-Mail-Adresse, Rolle und „dabei seit“,
- ob jemand die Einladung schon angenommen hat,
- wie viele Kurse eine Person **vollständig abgeschlossen** hat,
- wie viele der gebuchten Plätze belegt sind (20 in der Grundlizenz, dazu gebuchte Blöcke zu je 10 Plätzen).

Er sieht **nicht**: welche Lektion jemand wann bearbeitet hat, wie lange, in welcher Reihenfolge, wann sich jemand anmeldet, was jemand im Forum schreibt, welche Fragen jemand dem Support stellt, an welchen Live-Terminen jemand teilnimmt. Ranglisten, Punkte oder Bewertungen gibt es auf der Plattform überhaupt nicht.

Was Sie als Verantwortlicher tun sollten

1. **Mitarbeitende informieren** (Art. 13 DSGVO): dass Sie die Plattform nutzen, welche Daten Sie dabei sehen und wozu. Ein Satz in Ihrer Datenschutzinformation für Beschäftigte genügt meist. Für die Community verweisen Sie auf unsere Datenschutzerklärung.
2. **Rechtsgrundlage klären:** Die Teilnahme an einer Weiterbildung, die Sie anbieten, stützt sich in der Regel auf das Arbeitsverhältnis oder auf Ihr berechtigtes Interesse. [FACHANWALT] Formulierung prüfen (Art. 6 Abs. 1 lit. b/f DSGVO, Art. 88 DSGVO, § 26 BDSG nach EuGH C-34/21).
3. **Betriebsrat beteiligen,** wenn es einen gibt: Die Teilnahmeübersicht kann eine technische Einrichtung im Sinne von § 87 Abs. 1 Nr. 6 BetrVG sein. Dann ist die Einführung mitbestimmungspflichtig. Ob eine Betriebsvereinbarung nötig ist, klären Sie mit Ihrem Betriebsrat.
4. **Austritte pflegen:** Wer Ihr Unternehmen verlässt, entfernt Ihr Firmen-Admin aus dem Firmenkonto. Der Zugang endet dann sofort.
5. **Firmen-Admins mit Bedacht wählen:** Nur wer für Ihr Unternehmen handeln darf, sollte Firmen-Admin sein. Der Firmen-Admin schließt auch den AV-Vertrag für Sie ab.

Grenzfälle

Fall	Einordnung
Sie laden freie Mitarbeitende oder Beschäftigte eines Konzernunternehmens ein, die eine Adresse unter Ihrer Firmendomain haben	Das ist erlaubt (AGB § 4 Abs. 3). Für diese Personen sind Sie ebenso verantwortlich wie für Ihre Beschäftigten: Sie brauchen eine Rechtsgrundlage und informieren sie. Für Beschäftigte eines verbundenen Unternehmens schließen Sie den AV-Vertrag zugleich in dessen Namen ab oder sorgen für eine eigene Vereinbarung mit ihm (§ 5 Abs. 3 AVV)
Für eine Mitarbeiterin wird ein Einzelkurs gekauft	Einzelkurse gehören nicht zur Mitgliedschaft und werden gesondert gekauft (AGB § 3 Abs. 2, § 8). Kauf und Abrechnung sind unsere Sache; nur was über Ihr Firmenkonto läuft, ist Auftragsverarbeitung
Ihr Unternehmen überträgt einen Einzelkurs auf eine andere Person (einmal möglich, AGB § 8 Abs. 2)	Der Zugang der ersten Person zu diesem Kurs endet; ihren Lernfortschritt in diesem Kurs löschen wir und informieren sie. Lernfortschritt ist unsere Sache, nicht Teil der Auftragsverarbeitung
Ein Mitarbeiter verlässt Ihr Unternehmen und wechselt zu einem anderen Kunden	Die Zuordnung zu Ihnen endet, und Sie sehen ihn nicht mehr in Ihrer Übersicht. Was wir für Sie verarbeitet haben, löschen wir nach § 12 AVV. Seinen eigenen Lernfortschritt behält er nach unseren Nutzungsbedingungen, weil er ihn mit seinem neuen Zugang weiter nutzt
Ihr Firmen-Admin schreibt uns im Support	Support ist unsere Sache. Geht es um eine Weisung (z. B. „bitte Person X löschen“), behandeln wir sie als Weisung nach dem AV-Vertrag
Künftig ein Forumsbereich nur für Ihr Unternehmen	wäre Auftragsverarbeitung; wir passen Anlage 1 dann an (§ 1 Abs. 5 AVV)
Aufzeichnungen von Live-Terminen	unsere Sache. Wer in einer Aufzeichnung zu sehen oder zu hören ist, informieren wir vorher. [PRÜFEN] Hinweis- bzw. Einwilligungstext für die Zoom-Aufzeichnung (Version 0.10.0)

Die Teilnahmebescheinigung (geplant)

Die Bescheinigung belegt, dass eine Person einen Kurs vollständig bearbeitet hat. Sie bescheinigt eine Schulungsmaßnahme, keine Kompetenz und kein Prüfungsergebnis. Formulierung für Werbung und Oberfläche nach Volker: „Fördert KI-Kompetenz im Sinne von Art. 4 KI-VO – mit Teilnahmenachweis für Ihr Schulungsverzeichnis.“