

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) · Musterfassung, Stand 08.10.2026

Vertragsparteien

Auftraggeber / Verantwortlicher	der Kunde, der ProfiCampus mit Leistungen beauftragt, bei denen ProfiCampus personenbezogene Daten in seinem Auftrag verarbeitet (Firma und Anschrift gemäß Angebot bzw. Vertrag)
Auftragnehmer / Auftragsverarbeiter	Timo Eppler, handelnd unter ProfiCampus Hudtwalckerstr. 26, 22299 Hamburg Datenschutzkontakt: timo@proficampus.de

Der Auftraggeber und der Auftragnehmer werden nachfolgend einzeln auch „Partei“ und gemeinsam „Parteien“ genannt.

1. Gegenstand, Dauer, Abschluss und Verhältnis zum Hauptvertrag

Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Zusammenhang mit der Bereitstellung, dem Betrieb und der Betreuung der ProfiCampus-Lernplattform sowie ergänzender Leistungen (z. B. Präsenz- und Online-Schulungen, individuelle E-Learning-Produktion).

Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich als Auftragsverarbeiter und nur nach Maßgabe dieser Vereinbarung, des Hauptvertrags, der Leistungsbeschreibung und dokumentierter Weisungen des Auftraggebers.

Diese Vereinbarung gilt als Rahmenvereinbarung für alle Leistungen des Auftragnehmers, bei denen personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden. Sie wird Bestandteil jedes Vertrags, in dem auf sie Bezug genommen wird, und kommt mit der Annahme des Angebots bzw. dem Vertragsschluss zustande; eine gesonderte Unterzeichnung ist nicht erforderlich. Der Abschluss im elektronischen Format ist zulässig (Art. 28 Abs. 9 DSGVO). Auf Wunsch stellt der Auftragnehmer ein unterzeichnetes Exemplar bereit.

Die Vereinbarung beginnt spätestens mit der erstmaligen Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer und gilt so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet.

Bei Widersprüchen gehen die Regelungen dieser Vereinbarung in Datenschutzfragen den sonstigen vertraglichen Regelungen vor. Preise, Leistungsumfang, Kündigung, Gewährleistung, Vergütung, Verfügbarkeit und Haftung bleiben, soweit sie nicht datenschutzrechtlich zwingend in dieser Vereinbarung geregelt sind, dem Hauptvertrag, den Angeboten oder den AGB vorbehalten.

2. Art, Zweck und Umfang der Verarbeitung

Art und Zweck der Verarbeitung bestehen in der Bereitstellung, dem Betrieb und der Pflege der vom Auftragnehmer selbst entwickelten ProfiCampus-Lernplattform einschließlich Nutzerverwaltung, Datenimport und Verzeichnisabgleich, Schulungszuweisung, Erinnerungen an fällige Schulungen, Lernfortschritts- und Testergebnisverarbeitung, Zertifikatserstellung und -prüfung, Teamübersichten und Berichten für berechnete Leitungen, Verwaltung von Präsenz- und Online-Terminen

einschließlich Anwesenheitserfassung, freiwilligem Kursfeedback, Hilfe-Chat und technischem Support, automatisierten System-E-Mails, Hosting, Wartung, Updates, Sicherungen, technischer Absicherung sowie der Erstellung und Bereitstellung individueller E-Learning-Inhalte.

Der genaue Umfang der Verarbeitung ergibt sich ergänzend aus Anlage 1 „Leistungs- und Verarbeitungsbeschreibung“.

Der Auftragnehmer verarbeitet die personenbezogenen Daten nicht für eigene Zwecke, insbesondere nicht für Werbung gegenüber Lernenden, nicht zum Verkauf personenbezogener Daten und nicht zum Training von KI-Systemen. Anonymisierte und nicht mehr personenbezogene statistische Auswertungen, insbesondere zur technischen Fehleranalyse und Verbesserung der Plattform und der Kurse, bleiben zulässig.

3. Arten personenbezogener Daten

Gegenstand der Verarbeitung können insbesondere folgende Datenarten sein:

- Vorname, Nachname, E-Mail-Adresse, Sprache;
- Personalnummer, interne ID oder Kennung aus dem Verzeichnisdienst des Auftraggebers (z. B. Microsoft Entra ID), soweit vom Auftraggeber geliefert;
- Einrichtung, Standort, Organisationseinheit, Abteilung, Team, Gruppe, Vorgesetzte bzw. Leitung;
- Rolle oder Funktion, z. B. Lernende, Leitung, Administration;
- Schulungszuweisungen, Fälligkeiten, Erinnerungen, Kursaufrufe, Bearbeitungszeiten und Lernfortschritte;
- Testergebnisse, Bestehensstatus und Abschlussdaten;
- Zertifikatsdaten, z. B. Kursname, Lernziele, Abschlussdatum, Prüfnummer;
- Termin- und Anwesenheitsdaten bei Präsenz- und Online-Schulungen;
- freiwilliges Kursfeedback (Sternebewertung, Kommentar);
- Anmelde- und Nutzungsdaten, technische Protokolldaten wie IP-Adresse, Zeitstempel, Browser/User-Agent;
- Supportdaten, z. B. Chatnachrichten, E-Mail-Anfragen, Fehlerbeschreibungen und Screenshots;
- Kommunikationsdaten von Ansprechpartnern des Auftraggebers, z. B. Name, E-Mail-Adresse, Telefonnummer.

Im Rahmen individueller E-Learning-Produktion können zusätzlich Namen, Funktionen, Kontaktdaten, Fotos, Videos, Sprachaufnahmen, Screenshots aus Kundensystemen, echte oder kundenspezifische Fallbeispiele, Organigramme, Dienstpläne oder interne Dokumente verarbeitet werden, soweit der Auftraggeber diese Daten bereitstellt oder deren Nutzung ausdrücklich freigibt. Soweit möglich, werden dafür anonymisierte, pseudonymisierte oder fiktive Daten verwendet.

KI-Dienste: Für Antwortvorschläge im Hilfe-Chat und im Support kann der Auftragnehmer ein KI-Sprachmodell einsetzen. Dabei wird der Inhalt der jeweiligen Anfrage verarbeitet; jede Antwort prüft und versendet der Auftragnehmer selbst. Lern-, Test-, Anwesenheits- und Zertifikatsdaten werden nicht an KI-Dienste übermittelt.

4. Kategorien betroffener Personen

- Beschäftigte / Mitarbeitende des Auftraggebers;
- Leitungs- und Führungskräfte des Auftraggebers;

- externe Nutzer des Auftraggebers, z. B. Honorarkräfte, freie Mitarbeitende, Praktikanten oder Auszubildende;
- Dozentinnen und Dozenten von Präsenz- und Online-Schulungen;
- Ansprechpartner und administrative Kontaktpersonen des Auftraggebers.

Besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO werden im Regelbetrieb nicht verarbeitet. Personenbezogene Daten betreuter Kinder werden nicht verarbeitet. Der Auftraggeber übermittelt solche Daten nicht an den Auftragnehmer, sofern dies nicht vorher ausdrücklich gesondert vereinbart wurde.

5. Pflichten des Auftragnehmers

- Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit keine gesetzliche Verarbeitungspflicht besteht.
- Der Auftragnehmer wahrt Vertraulichkeit und verpflichtet Personen mit Zugriff auf personenbezogene Daten vor Aufnahme der Tätigkeit auf Vertraulichkeit, soweit nicht bereits eine gesetzliche Verschwiegenheitspflicht besteht.
- Der Auftragnehmer setzt angemessene technische und organisatorische Maßnahmen gemäß Anlage 2 um und überprüft diese regelmäßig.
- Der Auftragnehmer unterstützt den Auftraggeber nach Maßgabe dieser Vereinbarung bei Betroffenenrechten, Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und Behördenanfragen.
- Der Auftragnehmer stellt sicher, dass Kundendaten nur berechtigten Personen zugänglich sind und Zugriffsrechte nach dem Need-to-know- und Least-Privilege-Prinzip vergeben werden.
- Der Auftragnehmer informiert den Auftraggeber, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt oder technisch/organisatorisch problematisch ist. Die Umsetzung kann bis zur Klärung ausgesetzt werden.

6. Pflichten des Auftraggebers

- Der Auftraggeber bleibt für die Rechtmäßigkeit der Verarbeitung, insbesondere für die Rechtmäßigkeit der Datenübermittlung an den Auftragnehmer, verantwortlich.
- Der Auftraggeber informiert seine Mitarbeitenden, Nutzer und sonstigen betroffenen Personen über die Nutzung der ProfiCampus-Leistungen und die damit verbundene Datenverarbeitung.
- Der Auftraggeber stellt sicher, dass nur erforderliche, richtige und aktuelle Daten übermittelt werden.
- Der Auftraggeber benennt weisungsberechtigte Ansprechpartner.
- Der Auftraggeber entscheidet, welche Personen als Lernende, Leitungen, Administratoren oder sonstige Nutzer Zugriff erhalten, und verantwortet intern, wer Lernfortschritte, Testergebnisse, Zertifikate, Teamübersichten und Berichte einsehen darf.
- Bittet der Auftragnehmer im Auftrag des Auftraggebers Teilnehmende um eine öffentliche Bewertung (z. B. bei Google), geschieht dies nur mit Einverständnis des Auftraggebers.
- Bei Fotos, Videos, Sprachaufnahmen, echten Fallbeispielen oder internen Dokumenten für individuelle E-Learnings stellt der Auftraggeber sicher, dass die Nutzung rechtlich zulässig ist.
- Der Auftraggeber übermittelt keine besonderen Kategorien personenbezogener Daten und keine Daten betreuter Kinder, soweit dies nicht ausdrücklich gesondert vereinbart wurde.

7. Weisungen

Die anfänglichen Weisungen ergeben sich aus dieser Vereinbarung, dem Hauptvertrag, der Leistungsbeschreibung und den vereinbarten Plattformfunktionen sowie aus den Einstellungen, die der Auftraggeber in der Plattform selbst vornimmt (z. B. Erinnerungsrhythmus, Anmeldeverfahren, Teamansichten). Einzelweisungen erfolgen grundsätzlich in Textform, z. B. per E-Mail, durch benannte Ansprechpartner des Auftraggebers.

Mündliche Weisungen sind nur in Ausnahmefällen zulässig und unverzüglich in Textform zu bestätigen. Einzelweisungen dürfen den vereinbarten Leistungsumfang nicht ohne gesonderte Vereinbarung erweitern. Entstehen durch besondere Weisungen Zusatzaufwände, können diese nach vorheriger Abstimmung gesondert berechnet werden.

8. Vertraulichkeit, Personal und externe Mitwirkende

Zugriff auf Kundendaten erhält grundsätzlich nur der Auftragnehmer persönlich bzw. klar autorisierte Personen. Der Auftragnehmer beschäftigt derzeit keine festangestellten Mitarbeitenden mit Zugriff auf Kundendaten der Lernplattform. Externe Dienstleister oder Freelancer erhalten nur Zugriff auf personenbezogene Kundendaten, soweit dies für Support, Technik oder Content-Erstellung erforderlich ist und die datenschutzrechtlichen Voraussetzungen erfüllt sind. Dozentinnen und Dozenten erhalten für die Anwesenheitserfassung nur Zugriff auf die Teilnehmerliste des jeweiligen Termins.

Bei individueller E-Learning-Erstellung erhalten externe Content-Ersteller grundsätzlich nur anonymisierte oder fiktive Inhalte, soweit keine ausdrückliche Freigabe des Auftraggebers für Echtdaten vorliegt. Zugriffe werden entzogen, sobald sie nicht mehr erforderlich sind.

9. Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen. Diese Maßnahmen dürfen im Rahmen technischer Weiterentwicklung angepasst werden, sofern das Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

Der Auftragnehmer schuldet keine absolute Sicherheit, sondern angemessene Maßnahmen unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere möglicher Risiken.

10. Unterauftragnehmer

Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter, soweit dies zur Erbringung der vereinbarten Leistungen erforderlich ist. Die aktuell eingesetzten Unterauftragnehmer sind in Anlage 3 aufgeführt.

Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen durch Hinzunahme oder Austausch von Unterauftragnehmern mindestens 14 Kalendertage vor deren Einsatz per E-Mail an den benannten Ansprechpartner oder durch Veröffentlichung einer aktualisierten Unterauftragnehmerliste auf proficampus.de. Eine kürzere Frist ist zulässig, wenn dringende technische, sicherheitsrelevante oder betriebliche Gründe dies erfordern.

Der Auftraggeber kann der Änderung aus wichtigem datenschutzrechtlichem Grund widersprechen. Pauschale oder rein kaufmännische Widersprüche genügen nicht. Können die Parteien den

Widerspruch nicht angemessen lösen, können sie eine zumutbare Alternative vereinbaren oder die betroffene Leistung kündigen.

Der Auftragnehmer stellt sicher, dass Unterauftragnehmer vertraglich auf Datenschutzpflichten verpflichtet werden, die ein angemessenes Schutzniveau gewährleisten. Kundendaten werden nur weitergegeben, soweit dies für die Leistungserbringung erforderlich ist.

11. Internationale Datenübermittlungen

Die Lernplattform und ihre Datenbank werden auf Servern in Frankfurt am Main, Deutschland, betrieben. Soweit bei eingesetzten Unterauftragnehmern, insbesondere Microsoft-Diensten, Drittlandbezüge nicht ausgeschlossen werden können, erfolgt eine Verarbeitung nur bei Vorliegen geeigneter Garantien nach Kapitel V DSGVO, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (EU-U.S. Data Privacy Framework) oder von Standardvertragsklauseln.

Der Auftragnehmer wird keine eigenständigen Drittlandübermittlungen außerhalb des vereinbarten Leistungsumfangs vornehmen.

12. Rechte betroffener Personen

Der Auftragnehmer beantwortet Anfragen betroffener Personen, insbesondere von Lernenden, nicht eigenständig inhaltlich, sondern leitet sie unverzüglich an den Auftraggeber weiter, sofern sich die Anfrage auf die Auftragsverarbeitung bezieht.

Der Auftragnehmer unterstützt den Auftraggeber nach dokumentierter Weisung bei Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und sonstigen Betroffenenrechten, soweit dies technisch möglich und vom Leistungsumfang umfasst ist. Die Umsetzung erfolgt grundsätzlich innerhalb von 10 Werktagen, soweit keine besonderen Umstände entgegenstehen. Personen werden auf Weisung anonymisiert: Name und Kontaktdaten werden entfernt, Abschluss- und Zertifikatsnachweise bleiben ohne Personenbezug erhalten, soweit der Auftraggeber nichts anderes anweist.

13. Datenschutzverletzungen und Sicherheitsvorfälle

Der Auftragnehmer informiert den Auftraggeber unverzüglich, möglichst innerhalb von 24 Stunden nach Bekanntwerden, über Verletzungen des Schutzes personenbezogener Daten, soweit diese die Auftragsverarbeitung betreffen.

Die Meldung enthält, soweit zum Zeitpunkt der Meldung verfügbar, Art des Vorfalls, betroffene Datenkategorien, betroffene Personengruppen, geschätzten Umfang, wahrscheinliche Folgen, bereits ergriffene oder vorgeschlagene Maßnahmen sowie einen Ansprechpartner. Der Auftragnehmer dokumentiert den Vorgang intern und unterstützt den Auftraggeber angemessen bei Meldungen an Aufsichtsbehörden oder Betroffene.

Technische Sicherheitsvorfälle ohne unmittelbaren Personenbezug werden bewertet und dokumentiert, soweit sie Auswirkungen auf Vertraulichkeit, Integrität oder Verfügbarkeit personenbezogener Daten haben können.

14. Import, Verzeichnisabgleich, Reporting und Zertifikate

Nutzerdaten können durch Upload einer Datei in der Plattformverwaltung, durch einen automatisierten Abgleich mit dem Verzeichnisdienst des Auftraggebers (z. B. Microsoft Entra ID),

über die Programmierschnittstelle (REST-API) der Plattform, durch manuelle Nutzeranlage durch den Auftragnehmer oder durch berechtigte Leitungen/Administratoren des Auftraggebers übermittelt werden. Die Übermittlung von Nutzerlisten per E-Mail ist zulässig, jedoch nicht der bevorzugte Weg.

Importdaten werden nur zur Nutzeranlage oder Nutzeraktualisierung verwendet. Der Auftraggeber ist verantwortlich dafür, keine unnötigen Datenfelder zu liefern. Per E-Mail übermittelte Dateien löscht der Auftragnehmer nach erfolgreichem Import.

Berichte und Teamübersichten können direkt in der Plattform eingesehen oder exportiert werden. Sie enthalten insbesondere Name, Team, Kurs, Fälligkeit, Status, Abschlussdatum und Zertifikatsstatus. Die Einsicht erhalten nur die vom Auftraggeber berechtigten Leitungen bzw. Administratoren. Der Auftraggeber entscheidet und verantwortet intern, wer solche Berichte erhalten darf.

Zertifikate werden während der Vertragslaufzeit gespeichert und können durch Lernende und berechtigte Leitungen heruntergeladen werden. Jedes Zertifikat trägt eine Prüfnummer; über die öffentliche Prüfseite kann jeder, der die Nummer kennt, die Echtheit prüfen. Ob dabei der Name angezeigt wird, legt der Auftraggeber fest. Nach Vertragsende können Zertifikats- und Abschlussdaten exportiert werden. ProfiCampus übernimmt keine eigenständige gesetzliche Archivierungspflicht für Schulungsnachweise des Auftraggebers; diese verbleibt beim Auftraggeber, soweit nicht ausdrücklich etwas anderes vereinbart wurde.

15. Support, Hilfe-Chat und E-Mails

Supportanfragen erreichen den Auftragnehmer per E-Mail (z. B. an support@proficampus.de, verarbeitet über Microsoft 365) oder über den Hilfe-Chat in der Lernplattform. Chatnachrichten werden in der eigenen Kundenverwaltung des Auftragnehmers auf einem Server in Frankfurt am Main gespeichert. Supportanfragen können personenbezogene Daten wie Name, E-Mail-Adresse, Nutzerkonto, Kurs, Fehlerbeschreibung oder Screenshots enthalten.

Supportdaten werden nur zur Bearbeitung des jeweiligen Falls und zur Verbesserung künftiger Antworten genutzt. Support-Kommunikation mit Bezug zur Auftragsverarbeitung wird während der Vertragslaufzeit aufbewahrt und danach gelöscht oder anonymisiert, soweit sie nicht für eigene Nachweis-, Vertrags- oder Rechtsverteidigungszwecke des Auftragnehmers erforderlich ist. Vertrags-, Rechnungs- und allgemeine Geschäftskommunikation sind eigene Verarbeitung des Auftragnehmers und keine Auftragsverarbeitung.

System-E-Mails der Lernplattform (z. B. AnmeldeLinks, Einladungen, Erinnerungen, Zertifikatsbenachrichtigungen) werden über einen E-Mail-Versanddienst innerhalb der EU versendet (siehe Anlage 3). Der Auftraggeber kann den Versand für seinen Bereich pausieren.

16. Löschung, Rückgabe und Export

Nach Beendigung der Leistung oder auf dokumentierte Weisung des Auftraggebers löscht der Auftragnehmer personenbezogene Daten oder gibt sie in einem gängigen Format heraus, soweit dies technisch möglich und vom Leistungsumfang umfasst ist. Der Auftraggeber kann vor Löschung einen Export, z. B. als CSV oder PDF, erhalten.

Produktive personenbezogene Daten werden spätestens 30 Tage nach Vertragsende gelöscht, sofern keine abweichende Weisung oder Vereinbarung besteht. Sicherungen werden nicht einzeln bereinigt; sie laufen nach der Aufbewahrungsfrist der Sicherung (Anlage 2 Nr. 6) automatisch aus. Ein Löschnachweis wird auf Anfrage bereitgestellt. Daten, die der Auftragnehmer für eigene

gesetzliche Pflichten, insbesondere Vertrags-, Rechnungs-, Steuer- oder Nachweiszwecke, benötigt, bleiben hiervon unberührt und werden nicht als Auftragsverarbeitung behandelt.

17. Kontrollrechte und Audits

Der Auftraggeber ist berechtigt, die Einhaltung dieser Vereinbarung zu kontrollieren. Die Kontrolle erfolgt vorrangig durch Auskünfte, Dokumentation, technische und organisatorische Maßnahmen, Unterauftragnehmerliste, Sicherheitskonzept, Lösch-/Sicherungskonzept oder sonstige geeignete Nachweise.

Vor-Ort-Audits oder Inspektionen sind nachrangig und nur zulässig, wenn die dokumentenbasierte Prüfung nicht ausreicht oder ein berechtigter, nachvollziehbarer Anlass besteht. Anlasslose Prüfungen sind auf maximal eine Prüfung pro Kalenderjahr beschränkt und mindestens 30 Kalendertage vorher anzukündigen. Audits dürfen Betriebsabläufe, Sicherheit, Geheimhaltungsinteressen und Rechte anderer Kunden nicht unangemessen beeinträchtigen. Direkter Zugriff auf Server, Datenbanken, Administrationsbereiche, Quellcode, Infrastruktur oder Daten anderer Kunden ist ausgeschlossen. Prüfungen erfolgen während üblicher Geschäftszeiten und nur durch geeignete, zur Vertraulichkeit verpflichtete Prüfer.

Außergewöhnliche, wiederholte oder aufwendige Prüfungen sowie Sonderauskünfte, die über angemessene Nachweise hinausgehen, können nach vorheriger Abstimmung gesondert berechnet werden, soweit dies rechtlich zulässig ist.

18. Datenschutz-Folgenabschätzung, Behördenanfragen und Zusammenarbeit

Der Auftragnehmer unterstützt den Auftraggeber angemessen, soweit dieser wegen der Nutzung der ProfiCampus-Leistungen eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation der Aufsichtsbehörde durchführen muss. Die Unterstützung erfolgt nur im Rahmen der dem Auftragnehmer vorliegenden Informationen und technischen Möglichkeiten. Eine rechtliche Bewertung oder eigene Datenschutz-Folgenabschätzung für den Auftraggeber übernimmt der Auftragnehmer nicht.

Bei Anfragen von Datenschutzaufsichtsbehörden, die die Auftragsverarbeitung betreffen, informiert der Auftragnehmer den Auftraggeber unverzüglich, soweit rechtlich zulässig, und unterstützt ihn angemessen. Zusatzaufwände, die über normale Auskünfte hinausgehen, können nach vorheriger Abstimmung gesondert berechnet werden.

19. Inhalte, externe Dienste und Testsysteme

Kursinhalte (SCORM-Pakete, eigene Lernmodule, Videos, Bilder) werden direkt aus der Lernplattform ausgeliefert. Innerhalb der Lernplattform werden keine externen Schriftarten, Content-Delivery-Netzwerke, Videoplattformen, Karten, Analyse-Tools oder Marketing-Tracking-Dienste eingesetzt. Externe Links in Kursen können vorkommen; deren Nutzung liegt außerhalb der Plattform. Online-Schulungen finden, soweit vereinbart, über Microsoft Teams statt.

Test- und Entwicklungsumgebungen werden mit fiktiven Daten betrieben. Echte personenbezogene Kundendaten werden dort nicht verwendet; ist dies zur Fehleranalyse ausnahmsweise erforderlich, geschieht es zweckgebunden und zeitlich begrenzt, und die Daten werden danach gelöscht. Demos erfolgen mit fiktiven oder anonymisierten Daten.

20. Änderungen dieser Vereinbarung und Schlussbestimmungen

Diese Vereinbarung regelt ausschließlich Datenschutz und Auftragsverarbeitung. Der Auftragnehmer kann diese Musterfassung an technische Weiterentwicklungen anpassen, soweit das Schutzniveau nicht sinkt; die jeweils aktuelle Fassung wird auf proficampus.de bereitgestellt. Änderungen der Unterauftragnehmer richten sich nach Ziffer 10. Sonstige Änderungen und Ergänzungen bedürfen mindestens der Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist. Eine elektronische Unterzeichnung ist zulässig.

Die Anlagen, insbesondere Leistungs- und Verarbeitungsbeschreibung, technische und organisatorische Maßnahmen, Unterauftragnehmerliste sowie Datenkategorien und Aufbewahrung, sind Bestandteil dieser Vereinbarung.

Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame Bestimmung durch eine wirksame Regelung ersetzen, die dem wirtschaftlichen und datenschutzrechtlichen Zweck möglichst nahekommt.

Ort, Datum, Unterschrift Auftraggeber (nur falls
unterzeichnet)

Hamburg, Datum, Timo Eppler (Auftragnehmer)

Anlage 1: Leistungs- und Verarbeitungsbeschreibung

Leistungsbereich	Beschreibung
Bereitstellung der Lernplattform	Betrieb der selbst entwickelten ProfiCampus-Lernplattform unter einer eigenen Adresse je Auftraggeber; Bereitstellung von Kursen, Startseite für Lernende mit fälligen und freiwilligen Schulungen, mobilfähige Oberfläche.
Nutzerverwaltung und Anmeldung	Anlage, Import, Verzeichnisabgleich, Aktualisierung, Deaktivierung und Anonymisierung von Nutzerkonten; Rollen Lernende, Leitung, Administration. Anmeldung über persönlichen Anmelde-link per E-Mail, wahlweise Passwort oder Single Sign-on über den Verzeichnisdienst des Auftraggebers.
Schulungszuweisung und Erinnerungen	Zuweisung von Pflicht- und freiwilligen Schulungen an Personen, Teams oder Gruppen; Fälligkeiten und Wiederholungszyklen; automatische Erinnerungen per E-Mail nach den Einstellungen des Auftraggebers.
Lernfortschritt und Tests	Erfassung von Kursaufrufen, Bearbeitungszeiten, Lernfortschritten, Testergebnissen, Bestehensstatus und Abschlussdaten; serverseitige Prüfung, ob ein Abschluss gültig ist.
Termine und Anwesenheit	Präsenz- und Online-Termine mit Anmeldung, Warteliste, Einladung und Kalendereintrag; Anwesenheitserfassung durch die Dozentin bzw. den Dozenten über einen Link zur jeweiligen Teilnehmerliste.
Zertifikate	Erstellung, Speicherung, Download und Export von Zertifikaten mit Prüfnummer; öffentliche Echtheitsprüfung.
Reporting und Teamübersicht	Einsicht in Erfüllungsstand, Fälligkeiten und Zertifikate durch berechtigte Leitungen und Administratoren; Exporte; nächtlicher Kennzahlenbericht an die Kundenverwaltung des Auftragnehmers (Anzahl Nutzer, Abschlüsse, Nutzung) zur Abrechnung und Betreuung.
Kursfeedback	Freiwillige Bewertung eines Kurses nach Abschluss (Sterne, Kommentar) zur Verbesserung der Inhalte.
Support und Hilfe-Chat	Technischer Nutzersupport per E-Mail und Hilfe-Chat in der Plattform, Fehleranalyse, Kommunikation mit Ansprechpartnern.
Systembetrieb	Hosting, Wartung, Updates, Sicherungen, Wiederherstellung, Überwachung der Erreichbarkeit, technische Absicherung und Protokollierung.
Individuelle E-Learnings	Erstellung kundenspezifischer Inhalte, soweit beauftragt; Verarbeitung personenbezogener Inhalte nur soweit vom Auftraggeber bereitgestellt oder freigegeben.

Anlage 2: Technische und organisatorische Maßnahmen

1. Mandantentrennung und Zugriffskontrolle

- Jeder Auftraggeber erhält einen eigenen Bereich (Mandant) mit eigener Adresse. Die Trennung der Mandanten wird in der Datenbank selbst durchgesetzt (Zeilensicherheit von PostgreSQL): Jede Abfrage sieht nur die Daten des Mandanten, in dessen Kontext sie läuft. Mandantenübergreifende Zugriffe sind nur über einen gesonderten, protokollierten Weg für den Plattformbetrieb möglich.

- Anmeldesitzungen gelten nur für die Adresse des jeweiligen Mandanten.
- Lernende sehen nur eigene Kurse, Fortschritte und Zertifikate; Leitungen sehen nur die ihnen zugeordneten Personen; Administrationsrechte vergibt der Auftraggeber.
- Rechtevergabe nach Need-to-know- und Least-Privilege-Prinzip; Entzug nicht mehr benötigter Zugriffe.

2. Authentifizierung

- Anmeldung von Lernenden über einen persönlichen Anmeldelink per E-Mail (gültig 14 Tage); gespeichert wird nur ein Hashwert des Links. Der Link meldet erst nach einer Bestätigung auf der Seite an, damit automatische Prüfungen von E-Mail-Programmen keine Anmeldung auslösen.
- Optional Passwort (gehasht gespeichert) oder Single Sign-on über den Verzeichnisdienst des Auftraggebers.
- Zugang zur Plattformverwaltung des Auftragnehmers nur mit Zwei-Faktor-Authentifizierung; Support-Zugänge zu einem Mandanten sind zeitlich auf 15 Minuten begrenzt und werden protokolliert.

3. Server- und Plattformssicherheit

- Betrieb auf einem eigenen virtuellen Server in Frankfurt am Main; Zugriff ausschließlich über HTTPS/TLS.
- Firewall: Aus dem Internet erreichbar sind nur die Webzugänge (HTTP/HTTPS) und der Administrationszugang des Servers; Datenbank, Zwischenspeicher und interne Dienste sind nicht aus dem Internet erreichbar.
- Administrationszugang (SSH) ausschließlich mit Schlüssel; Anmeldung mit Passwort ist abgeschaltet.
- Dateien der Mandanten liegen außerhalb des öffentlich erreichbaren Verzeichnisses und werden nur nach Berechtigungsprüfung ausgeliefert.
- Regelmäßige Updates von Betriebssystem, Laufzeitumgebung und Abhängigkeiten; Kursinhalte (SCORM-Pakete) werden beim Hochladen geprüft und von einer eigenen Adresse ohne Zugriff auf die Anmeldesitzung ausgeliefert.
- Automatisierte Tests prüfen bei jeder Änderung unter anderem die Mandantentrennung.
- Externe Überwachung der Erreichbarkeit und der Sicherung (ohne Verarbeitung personenbezogener Daten).

4. Protokollierung

- Protokollierung von Anmeldungen, Kursaktivitäten, Abschlüssen, Zertifikatserstellung und administrativen Änderungen in einem nicht nachträglich veränderbaren Prüfprotokoll; Korrekturen erfolgen als neue Einträge.
- Technische Protokolldaten können IP-Adresse, Zeitstempel, Browser/User-Agent und technische Ereignisse enthalten.

5. Verschlüsselung

- Datenübertragung per HTTPS/TLS; E-Mail-Versand mit Transportverschlüsselung.
- Sicherungen werden vor dem Verlassen des Servers verschlüsselt (AES-256); der Schlüssel liegt nicht beim Speicheranbieter.
- Zugriff auf Hosting-, Microsoft- und Administrationskonten mit starken Passwörtern und, soweit möglich, Zwei-Faktor-Authentifizierung.

6. Sicherung, Wiederherstellung und Verfügbarkeit

- Tägliche Sicherung von Datenbank und Dateien, lokal auf dem Server und verschlüsselt zusätzlich in Microsoft OneDrive (EU).
- Aufbewahrung der Sicherungsstände: 14 tägliche, 8 wöchentliche und 12 monatliche Stände; ältere Stände werden automatisch gelöscht.
- Regelmäßige Wiederherstellungsproben.
- Wiederherstellungsziel: maximal 48 Stunden an Werktagen. Kein garantiertes 24/7-SLA mit Vertragsstrafe; Ziel ist ein stabiler Regelbetrieb.
- Planbare größere Wartungsarbeiten werden möglichst vorher angekündigt; bei schwerwiegenden Störungen erfolgt angemessene Kundeninformation.

7. Endgeräte

- Zugriff über geschäftlich genutzte Endgeräte, geschützt durch Passwort/PIN/Biometrie und Bildschirmsperre; regelmäßige Updates.
- Keine dauerhafte lokale Speicherung von Kundendaten, soweit vermeidbar; heruntergeladene Listen oder Berichte werden nach Zweckerfüllung gelöscht.
- Kein Zugriff über fremde oder öffentliche Computer.

Anlage 3: Unterauftragnehmer

Unterauftragnehmer	Sitz / Standort	Leistung	Garantien
Hostinger International Ltd.	Zypern (EU); Server in Frankfurt am Main, Deutschland	Virtuelle Server für Lernplattform und Kundenverwaltung (inkl. Hilfe-Chat)	EU; Auftragsverarbeitungsbedingungen des Anbieters
Sendinblue SAS (Brevo)	Paris, Frankreich (EU)	Versand der System-E-Mails der Lernplattform	EU; Auftragsvertragsvertrag
Microsoft Ireland Operations Limited	Dublin, Irland (EU)	Microsoft 365: Support-E-Mail, Microsoft Teams für Online-Schulungen, OneDrive für verschlüsselte Sicherungen; Verzeichnisabgleich mit Entra ID, soweit vom Auftraggeber eingerichtet	EU-Datengrenze; Microsoft-Auftragsverarbeitungsbedingungen; DPF bzw. Standardvertragsklauseln bei Drittlandbezug

Anlage 4: Datenkategorien und Aufbewahrung

Kategorie	Beispiele	Aufbewahrung / Löschung
-----------	-----------	-------------------------

Nutzerstammdaten	Name, E-Mail, interne ID, Einrichtung, Team, Rolle, Leitung	Während Vertragslaufzeit; ausgeschiedene Personen werden auf Weisung anonymisiert; Löschung/Export nach Vertragsende.
Lern- und Leistungsdaten	Zuweisungen, Fälligkeiten, Kursaufrufe, Bearbeitungszeiten, Lernfortschritt, Testergebnisse	Während Vertragslaufzeit; Export möglich; Löschung spätestens 30 Tage nach Vertragsende.
Abschluss- und Zertifikatsdaten	Kurs, Lernziele, Abschlussdatum, Prüfnummer, Status	Während Vertragslaufzeit; Export möglich; keine eigenständige Archivierungspflicht durch ProfiCampus.
Termin- und Anwesenheitsdaten	Anmeldung, Warteliste, Anwesenheit	Wie Abschlussdaten.
Kursfeedback	Sterne, Kommentar	Während Vertragslaufzeit; Löschung mit dem Mandanten.
Technische Logs	Anmeldezeitpunkte, IP-Adresse, Browser, technische Ereignisse	Bis zu 12 Monate, soweit keine längere Aufbewahrung zur Störungsanalyse oder Rechtsverteidigung erforderlich ist.
Importdaten	Nutzerlisten, Verzeichnisabgleich	Nur zur Anlage/Aktualisierung; per E-Mail übermittelte Dateien werden nach dem Import gelöscht.
Sicherungen	Datenbank und Dateien	Bis zu 12 Monate (14 tägliche, 8 wöchentliche, 12 monatliche Stände); automatische Löschung danach.
Supportdaten	Chatnachrichten, E-Mail-Anfragen, Fehlerbeschreibungen, Screenshots	Während Vertragslaufzeit; danach Löschung/Anonymisierung, soweit nicht eigene Nachweis-/Vertragszwecke entgegenstehen.
Content-Produktionsdaten	Nur bei individuellen E-Learnings: Fotos, Videos, Sprachaufnahmen, Fallbeispiele, interne Dokumente	Zweckgebunden; nur bei Bereitstellung/Freigabe durch den Auftraggeber; bevorzugt anonymisiert/fiktiv.