Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung zwischen

Firmenname Rechtsform
Straße Hausnummer
PLZ Ort

(Verantwortlicher, nachfolgend „Auftraggeber“ genannt)

und

AS-Trainer GmbH
Schopenstehl 22
20095 Hamburg

(Auftragsverarbeiter, nachfolgend „Auftragnehmer“ genannt)

§ 1 Auftragsgegenstand, verarbeitete Daten und betroffene Personengruppen

(1) Der Auftraggeber lässt durch den Auftragnehmer auf Grundlage des Vertrags zur Nutzung des AS-Trainer „PLEGRO Online-Schulungssystem“ personenbezogene Daten im Auftrag verarbeiten. Zur Durchführung des Vertrags beauftragt der Auftraggeber den Auftragnehmer mit einer Verarbeitung im Auftrag gem. Art. 28 DSGVO.

(2) Ziel der Verarbeitung personenbezogenen Daten durch den Auftragnehmer ist die Erbringung in Anlage 1 aufgeführten Leistungen. Auftragsgegenstand, Kategorien verarbeiteter Daten und betroffene Personengruppen werden detailliert in Anlage 1 geregelt.

§ 2 Beginn und Laufzeit der Vereinbarung

(3) Beginn und Laufzeit richten sich nach den entsprechenden Regelungen des Hauptvertrags.

(4) Eine vom Hauptvertrag isolierte Kündigung ist nur aus wichtigem Grund möglich, es sei denn diese Vereinbarung oder zwingende gesetzliche Vorschriften bestimmen etwas anderes. In diesem Fall ist der Auftragnehmer nach Kündigung dieser Vereinbarung zur Kündigung des Hauptvertrages zum selben Zeitpunkt berechtigt.

(5) Diese Vereinbarung gilt unbeschadet der Absätze (3) und (4) so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet. Hierzu gehören auch zu Zwecken der Datensicherheit oder der Datenschutzkontrolle verarbeitete Daten (z. B. Backups).

§ 3 Ort der Auftragsverarbeitung, internationale Datentransfers

(1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Jede Verlagerung in ein Drittland und jede Änderung an den vereinbarten Garantien bedürfen der vorherigen Zustimmung des Auftraggebers oder dessen dokumentierter Weisung. Sie dürfen nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(3) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

(4) Die Verarbeitung von diesem Vertrag unterliegenden Daten in Privatwohnungen ist nicht gestattet. Soweit dennoch ausnahmsweise die Daten in einer Privatwohnung verarbeitet werden sollen, ist dies nur nach der vorherigen, ausdrücklichen Zustimmung des Auftraggebers zulässig. Der Auftragnehmer ist dafür verantwortlich, dass angemessene und geeignete technische und organisatorische Maßnahmen gem. § 7 getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Auftragnehmer ist zudem dafür verantwortlich, die erforderlichen Besichtigungs- und Kontrollrechte des Auftraggebers nach § 9 für diesen durchzuführen. Der Auftragnehmer wird auf erstes Anfordern Auskunft über die Ergebnisse der notwendigen Inspektionen erteilen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner der jeweiligen Privatwohnung über diese Regelung informiert und mit dieser einverstanden sind. Kann das Besichtigungs- und Kontrollrecht für den Auftraggeber nicht gewährleistet werden, so hat der Auftragnehmer zu gewährleisten, dass die Verarbeitung in Privatwohnungen unterbleibt.

(5) Die Verarbeitung von diesem Vertrag unterliegenden Daten in öffentlich zugänglichen Räumen ist verboten.

§ 4 Verantwortlichkeit und Weisungsrecht des Auftraggebers

(1) Der Auftraggeber ist für die Zwecke der Auftragsverarbeitung der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Übermittlung der Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung durch diesen, verantwortlich.

(2) Der Auftraggeber hat jederzeit das Recht, ergänzende Weisungen über Art, Umfang und Verfahren der Verarbeitung der personenbezogenen Daten zu erteilen. Diese Weisungen können auch vom Hauptvertrag abweichen. Weisungen können mündlich oder in Textform erfolgen.

(3) Mündliche Weisungen des Auftraggebers sind durch diesen unverzüglich, mind. in Textform zu bestätigen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Auffassung ist, eine Weisung verstoße gegen gesetzliche Regelungen. Solange die Parteien die Bedenken des Auftragnehmers nicht ausgeräumt haben, ist der Auftragnehmer berechtigt, die Durchführung der betreffenden Weisung auszusetzen. Wenn die Parteien keine Einigung erzielen können und der Auftraggeber an seiner Weisung festhält, ist der Auftragnehmer zu einer Kündigung dieser Vereinbarung mit angemessener Frist, die zwei Wochen nicht unterschreiten soll, berechtigt. Sofern in diesem Fall der Hauptvertrag nicht durchgeführt werden kann, ist der Auftraggeber berechtigt diesen zu kündigen, wenn der Hauptvertrag nur mittels Umsetzung der rechtswidrigen Weisung durchgeführt werden könnte und dies für keine Partei bei Vertragsschluss erkennbar war.

(5) Sofern der Auftragnehmer der Auffassung sein sollte, eine Weisung des Auftraggebers aus technischen Gründen nicht befolgen zu können, wird er den Auftraggeber hierüber in Textform informieren und sich unverzüglich zum weiteren Vorgehen mit diesem abstimmen.

§ 5 Pflichten des Auftragnehmers

(1) Jegliche Verarbeitung der personenbezogenen Daten erfolgt ausschließlich entsprechend den Vorgaben des Hauptvertrags, entsprechend dieser Vereinbarung, sowie den ggf. vom Auftraggeber erteilten Weisungen. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Dieser Absatz (1) gilt nicht, wenn der Auftragnehmer zu der Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer bestätigt, dass er einen externen Datenschutzbeauftragten benannt hat:

Herr Dipl.-Inform. Tobias Mauß, Mauß Datenschutz GmbH,
040 / 999 99 52-0, datenschutz@datenschutzbeauftragter-hamburg.de
Jegliche Änderung bezüglich der Benennung eines Datenschutzbeauftragten ist dem Auftraggeber unverzüglich in Textform mitzuteilen.

(3) Der Auftragnehmer hat die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit zu verpflichten, sofern sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen. Der Umfang der Verpflichtung hat in einem angemessenen Verhältnis zu den verarbeiteten Daten und den Folgen einer etwaigen Verletzung des Schutzes der personenbezogenen Daten zu stehen. Sie hat sich ferner auf alle personenbezogenen Daten zu beziehen, die der Auftragnehmer für den Auftraggeber verarbeitet. Der Inhalt und die Tatsache der Verpflichtung ist dem Auftraggeber auf Wunsch nachzuweisen. Etwaige weitergehende Verpflichtungen, die aus einer gesondert zwischen den Parteien abgeschlossenen Geheimhaltungsvereinbarung folgen, bleiben hiervon unberührt.

(4) Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten unterstützen. Hierfür wird er insbesondere die in dieser Vereinbarung vorgesehenen Leistungen erbringen.

(5) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit den Aufsichtsbehörden für den Datenschutz bei der Erfüllung ihrer Aufgaben zusammen.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde für den Datenschutz informieren, soweit sich diese auf im Rahmen dieser Vereinbarung verarbeiteten Daten beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(7) Soweit der Auftraggeber seinerseits einer Kontrolle durch eine Aufsichtsbehörde für den Datenschutz, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit dieser Vereinbarung ausgesetzt ist, wird ihn der Auftragnehmer nach besten Kräften unterstützen.

(8) Soweit erforderlich unterstützt der Auftragnehmer den Auftraggeber bei der Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und wird ihm alle hierfür aus seiner Sphäre erforderlichen Informationen und Nachweise überlassen. Er ist entsprechend verpflichtet, wenn der Auftraggeber eine vorherige Konsultation nach Art. 36 DSGVO mit einer Aufsichtsbehörde durchführen muss.

(9) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt.

(10) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden oder ist es zu entsprechenden Maßnahmen gekommen, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber umfassend zu informieren, es sei denn, dies ist ihm gesetzlich nicht gestattet. Ferner ist der Auftragnehmer verpflichtet, alle insoweit relevanten Dritten darauf hinweisen, dass es sich bei den Daten um personenbezogene Daten handelt, für die der Auftragsgeber Verantwortlicher im Sinne der DSGVO ist und er selbst nur als Auftragsverarbeiter tätig ist.

(11) Diese Vereinbarung entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

§ 6 Pflichten des Auftraggebers

Der Auftraggeber hat den Auftragnehmer unverzüglich unter Angabe der jeweiligen Gründe zu informieren, wenn er in den Auftragsergebnissen oder hinsichtlich der Tätigkeit des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich der Vorgaben dieser Vereinbarung oder der gesetzlichen Regelungen zum Datenschutz feststellt.

§ 7 Sicherheit der Verarbeitung

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen, insbesondere geeignete technische und organisatorische Maßnahmen, um ein dem Risiko der Datenverarbeitung und dem Schutzbedarf der verarbeiteten Daten angemessenes Schutzniveau zu gewährleisten. Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind dies die in der Anlage 3 beschriebenen Maßnahmen.

(2) Der Auftragnehmer ist zur Anpassung der getroffenen Maßnahmen an geänderte technische oder rechtliche Gegebenheiten, sowie an geänderte interne Prozesse berechtigt, Änderungen an den in Anlage 3 beschriebenen Maßnahmen vorzunehmen. Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen, eine Erhöhung der Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen oder generell eine Reduktion des vereinbaren Schutzniveaus mit sich bringen könnten, bedürfen der Zustimmung des Auftraggebers. Andere Änderungen, insbesondere eine Verbesserung der ergriffenen Maßnahmen, können vom Auftragnehmer ohne Zustimmung des Auftraggebers umgesetzt werden. Nach Vornahme solcher Änderungen passt der Auftragnehmer die Anlage 3 entsprechend an.

§ 8 Rechte betroffener Personen

(1) Der Auftragnehmer wird, soweit es ihm möglich und zumutbar ist, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel 3 der DSGVO genannten Rechte der betroffenen Personen nachzukommen. Hierfür hat der Auftraggeber den Auftragnehmer in Textform zu informieren, welche Unterstützungshandlung des Auftragnehmers er benötigt und diesem insoweit die Daten zu überlassen, die zur Erfüllung der Anfrage erforderlich sind. Soweit eine Partei weitere Informationen von der anderen Partei benötigt, wird sie diese unverzüglich in Textform darauf hinweisen. Der Auftragnehmer erbringt seine Unterstützungshandlung in angemessener Frist, so dass der Auftraggeber die ihm obliegenden Fristen, insbesondere des Art. 12 Abs. 3 DSGVO, wahren kann. Er hat den Auftraggeber unverzüglich unter Angabe der Gründe zu informieren, wenn es sich nicht in der Lage sieht, der verlangte Unterstützungshandlung zu erbringen.

(2) Wenn eine betroffene Person sich zur Ausübung der diesem aus Kapitel 3 der DSGVO zustehenden Rechte unmittelbar an den Auftragnehmer wenden sollte, wird der Auftragnehmer diese an den Auftraggeber verweisen, soweit ihm die Zuordnung zu diesem möglich ist. Sollte ihm eine Zuordnung nicht möglich und der Auftragnehmer auch nicht als Verantwortlicher unmittelbar gegenüber der betroffenen Person aus Kapitel 3 der DSGVO verpflichtet sein, wird er sie darüber informieren, dass er als Auftragsverarbeiter für Dritte tätig ist und er den Dritten hinsichtlich der betroffenen Person nicht identifizieren kann.

§ 9 Kontrollrechte des Auftraggebers

(1) Dem Auftraggeber stehen alle Kontrollrechte, insbesondere Inspektionen, zu, die zur Wahrung der ihm nach den Vorgaben der DSGVO obliegenden Pflichten erforderlich sind. Das Kontrollrecht ist mit einer angemessenen Ankündigungsfrist und zu den üblichen Geschäftszeiten des Auftragnehmers auszuüben. Der Auftragnehmer ist zur Reduktion der Auswirkungen von Inspektionen auf seinen Geschäftsbetrieb berechtigt, diese mit denen anderer Auftraggeber zu verbinden, soweit dies dem Auftraggeber zumutbar ist (z.B. gemeinsame Inspektionstermine, die in angemessener Frist durchgeführt werden). Der Auftraggeber wird Sorge dafür tragen, dass Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers nicht unverhältnismäßig zu stören.

(2) Der Auftraggeber ist berechtigt, die Ausübung der Kontrollrechte auf einem von diesem beauftragten Dritten zu übertragen. Sollte der Dritte in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, hat dieser gegen dessen Tätigkeit ein Einspruchsrecht.

(3) Der Auftragnehmer hat an der Ausübung der Kontrollrechte im erforderlichen Umfang mitzuwirken. Er darf Kontrollen durch den Auftraggeber von der Unterzeichnung einer üblichen und angemessenen Verschwiegenheitserklärung abhängig machen, soweit dies zum Schutz seiner Geschäftsgeheimnisse nach den gesetzlichen Vorgaben erforderlich ist.

(4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann nach Wahl des Auftragnehmer erfolgen durch Nachweis der Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, einer Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, durch Vorlage aktueller Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) sowie durch eine geeignete Zertifizierung gemäß einem IT-Sicherheits- oder Datenschutzstandard (z.B. nach VDS 10.000 oder BSI-Grundschutz).

§ 10 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsdienstleistungen oder Bewachungsdienstleistungen in Anspruch nimmt. Die Vernichtung und/oder Entsorgung von Datenträgern erfolgt auftragsübergreifend und gem. DIN/EN/ISO 66399, mindestens Sicherheitsstufe P-5. Sie stellt ebenfalls kein Unterauftragsverhältnis dar.

(2) Wartungsleistungen, Prüfleistungen sowie Benutzerservice stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden.

(3) Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(4) Der Auftragnehmer setzt für die Verarbeitung die in der Anlage 2 benannten Unterauftragsverarbeiter ein.

(5) Der Auftragnehmer wird den Auftraggeber in Textform über Änderungen an der Beauftragung von Unterauftragsverarbeitern informieren. Der Auftraggeber kann innerhalb einer Frist von zwei Wochen seit Zugang der Information der Änderung widersprechen. Der Auftragnehmer setzt die Änderung nicht vor Ablauf der Widerspruchsfrist um.
Der Auftragnehmer wird dem Auftraggeber vor der Änderung an der Beauftragung von Unterauftragsverarbeitern folgende Informationen in Textform übersenden:

   a) Beschreibung der geplanten Änderung;
   b) Name und Anschrift des Unterauftragsverarbeiters;
   c) welche Leistungen der Unterauftragsverarbeiter erbringen soll und welche personenbezogenen Daten und welche Kategorie von Betroffenen hiervon betroffen sind;
   d) den Inhalt der entsprechenden Vereinbarungen mit dem Unterauftragsverarbeiter sowie ggf. alle Nachweise zur Einhaltung des Kapitels 5 der DSGVO;
   e) die vorstehenden Informationen sind ebenfalls für alle weiteren Unterauftragsverarbeiter zur Verfügung zu stellen, die unterhalb des Unterauftragsverarbeiters entsprechende Leistungen erbringen sollen.

(6) Der Auftragnehmer setzt die Änderung nicht vor Ablauf der Widerspruchsfrist um. Im Falle eines Widerspruchs ist der Auftragnehmer berechtigt, diese Vereinbarung mit einer Frist von mindestens einem Monat zu kündigen, sofern die Änderung dem Auftraggeber zumutbar gewesen wäre und der Widerspruch dem Auftragnehmer unzumutbar ist.
Zumutbarkeit für den Auftraggeber ist gegeben, wenn mit der Änderung keine Nachteile für ihn zu befürchten gewesen wären und insbesondere sichergestellt gewesen wäre, dass die Vorgaben dieser Vereinbarung und der DSGVO bei Umsetzung der Änderung weiter eingehalten worden wären. Unzumutbarkeit für den Auftragnehmer ist gegeben, wenn er seine Auftragsverarbeitungsleistungen als im Wesentlichen gleichförmigen Prozess für eine Vielzahl von Auftraggebern erbringt und individuelle Abweichungen bei den Unterauftragsverarbeitern für den Auftragnehmer nicht einfach umzusetzen sind (z.B. alle Auftraggeber nutzen dieselbe, standardisierte Softwareplattform).

(7) Der Auftragnehmer wird für sämtliche Unterauftragnehmer die in den Absätzen 2 und 4 des Art. 28 DSGVO genannten Bedingungen einhalten. Er hat ferner sicherzustellen, dass die sonst mit dem Auftraggeber insoweit getroffenen Vereinbarungen sowie die ggf. ergänzende Weisungen des Auftraggebers auch von den Auftragsverarbeitern eingehalten werden. Er hat dies dem Auftraggeber auf dessen Wunsch nachzuweisen.

(8) Der Auftragnehmer vereinbart mit sämtlichen Unterauftragnehmern eine Drittbegünstigtenklausel, wonach der Auftraggeber – im Falle, dass der Auftragnehmer faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragnehmer anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

(9) Die Weitergabe von personenbezogenen Daten des Auftraggebers an Unterauftragnehmer und deren erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(10) Eine weitere Auslagerung durch Unterauftragnehmer ist zulässig.

§ 11 Verstöße des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften, gegen die getroffenen Vereinbarungen und/oder die erteilten Weisungen unverzüglich, in Textform mitzuteilen. Die entsprechende Meldung soll zumindest die in Art. 33 Abs. 3 DSGVO definierten Informationen umfassen.

(2) Jegliche, etwaige erforderliche Meldung an eine Aufsichtsbehörde oder Benachrichtigung betroffener Personen obliegt allein dem Auftraggeber. Der Auftragnehmer wird hieran im erforderlichen Umfang mitwirken.

(3) Der Auftragnehmer ist weiter verpflichtet, den Verstoß im erforderlichen Umfang unverzüglich aufzuklären und dem Auftraggeber eine entsprechende Dokumentation zu überlassen. Die Dokumentation hat eine Darstellung zu umfassen, welche Maßnahmen der Auftragnehmer ergriffen hat, um weitere Verstöße zu unterbinden und warum er der Auffassung ist, dass die ergriffenen Maßnahmen ausreichend sind, um den Vorgaben dieser Vereinbarung und der gesetzlichen Vorschriften zu genügen.

§ 12 Vergütungsansprüche

Dem Auftragnehmer steht für die von ihm unter dieser Vereinbarung erbrachten Leistungen kein gesondertes Entgelt zu, sofern nicht an anderer Stelle in dieser Vereinbarung vereinbart. Insbesondere stehen dem Auftragnehmer keine Vergütungsansprüche für Unterstützungsleistungen im Rahmen von Kontrollen durch den Auftraggeber gem. § 9 dieser Vereinbarung zu.

§ 13 Haftung

Die Haftung der Parteien richtet sich nach den Vereinbarungen des Hauptvertrages. Die unmittelbare Haftung der Parteien gegenüber einer betroffenen Person aus gesetzlichen Bestimmungen des Datenschutzes bleibt unberührt.

§ 14 Folgen der Beendigung dieser Vereinbarung

(1) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen/vernichten oder nach vorheriger Aufforderung an den Auftraggeber zu übergeben.

(2) Test- und Ausschussmaterial ist zu vernichten.

(3) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren.

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

(5) Jegliches Zurückbehaltungsrecht des Auftragnehmers hinsichtlich der verarbeiteten Daten und der ggf. vom Auftraggeber übergebenen zugehörigen Datenträger ist im Übrigen ausgeschlossen.

(6) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 15 Schlussbestimmungen

(1) Diese Vereinbarung zur Auftragsverarbeitung geht im Fall von Widersprüchen dem Hauptvertrag vor.

(2) Im Übrigen gelten die Schlussbestimmungen des Hauptvertrags.

Anlage 1 – Auftragsgegenstand, Datenkategorien, betroffene Personengruppen, Sonderregelungen, Regelungen zur Laufzeit

Anlage 2 – Genehmigte Unterauftragnehmer

Anlage 3 – Technische und organisatorische Maßnahmen

_____	_____
Ort, Datum	Auftraggeber
_____	_____
Ort, Datum	Auftragnehmer

Anlage 1 – Auftragsgegenstand, Datenkategorien, betroffene Personengruppen

Auftragsgegenstand

Der Gegenstand des Auftrags wird wie folgt beschrieben:
Der Auftragnehmer stellt dem Auftraggeber ein Online-Schulungssystem zur Verfügung, mit dem die folgenden Leistungen erbracht werden:

- Durchführung von Online-Schulungen von Mitarbeitern des Auftraggebers zu diversen vom Auftraggeber festzulegenden Themen
- Überprüfung des Schulungserfolgs mithilfe eines Online-Tests
- Erzeugung von Schulungszertifikaten
- Speicherung von Schulungszertifikaten sowie Bereitstellung derselben zum Online-Abruf
- Funktionalitäten zur Online-Pflege von Mitarbeiterstammdaten
- Die Bedienung des Schulungssystems erfolgt durch den Auftraggeber selbst, insbesondere die Anlage und Pflege der Mitarbeiter inkl. aller personenbezogenen Stammdaten.

Kategorien personenbezogener Daten

- Benutzername
- Ggf. Anrede
- Ggf. Titel
- Vorname
- Nachname
- Ggf. E-Mail
- Ggf. Gruppe/Abteilung
- Ggf. Rolle für besondere Tätigkeiten, die einer speziellen Schulung bedürfen (z.B. Sicherheitsbeauftragter, Ersthelfer etc.)
- Schulungen, die einem einzelnen Benutzer zugewiesen wurden
- Definition der Gruppenleiter- oder Administratorfunktion (Zugriffsberechtigungen)
- Bei Bedarf können weitere Daten hinterlegt werden (Personal-Nr., Kategorie, Funktion, Telefon)

Kategorien der von der Auftragsverarbeitung betroffenen Personen

Mitarbeiter des Auftraggebers (Beschäftigte i. S d. § 26 Abs. 8 BDSG)

Anlage 2 – Genehmigte Unterauftragnehmer

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu:

Unterauftragnehmer	Anschrift/Land	Leistung
PlusServer GmbH	Hohenzollernring 72 50672 Köln	Leistung: Hosting inkl. Datensicherung Betroffene Daten: alle von diesem Vertrag betroffenen Daten. Möglichkeit der Einsichtnahme, sowie aktive Verarbeitung im Rahmen der Datensicherung und ggf. Wiederherstellung.

Anlage 2 – Technische und organisatorische Maßnahmen

1. Vertraulichkeit (confidentiality)

- Der körperliche Zutritt von Personen in Räumlichkeiten von AS-Trainer GmbH ist nur nach vorheriger Legitimation möglich. Zum Einsatz kommen herkömmliche Sicherheitsschlösser, zu denen die Schlüssel ausschließlich an berechtigte Mitarbeiter ausgegeben werden. Die Ausgabe der Schlüssel erfolgt durch die Geschäftsleitung.
- Der Kreis der Zutrittsberechtigten ist festgelegt.
- Die Räume werden durch eine Alarmanlage geschützt.
- Besucher, Lieferanten, Dienstleister und sonstige Externe werden durchgehend begleitet. Mit dem externen Dienstleister für die Unterhaltsreinigung wurde eine Vertraulichkeitsvereinbarung geschlossen.
- AS-Trainer GmbH betreibt keine eigenen Server und somit auch keinen eigenen Serverraum. Die Server, auf denen Kundendaten im Auftrag verarbeitet werden, werden von dem Dienstleister Plusserver AG zur Verfügung gestellt und gewartet. Plusserver übernimmt einen Teil der Pflichten, die AS-Trainer treffen als Subunternehmer Auftragsverarbeitung. Ein entsprechender Vertrag zur Auftragsverarbeitung mit Plusserver als Subauftragnehmer wurde geschlossen.
- Der Zugang zu Workstations und Notebooks ist über individuelle Benutzerkonten geschützt.
- Kein Einsatz von Sammelusern.
- Die Vergabe jeglicher Benutzerkonten wird durch die Geschäftsleitung freigegeben.
- Zugangsberechtigungen zu den Rechnern werden personengebunden vergeben.
- Der Kreis der jeweils befugten Personen ist auf das betriebsnotwendige Maß eingeschränkt.
- Zugriffsberechtigungen werden in den Anwendungen rollenbasiert vergeben. Es wird nach dem Prinzip „need-to-know“ und „need-to-do“ verfahren.
- Jeder Zugangsberechtigte kann nur auf Daten zugreifen, die er zur Ausübung der ihm übertragenen Aufgaben und Funktionen benötigt.
- Die Mitarbeiter sind schriftlich auf die Vertraulichkeit, bzw. das Datengeheimnis verpflichtet.
- Auf den Rechnern in den Räumen von AS-Trainer GmbH werden mit Ausnahme von E-Mails, welche personenbezogene Daten enthalten können, keinerlei personenbezogene Daten der Auftraggeber gespeichert.
- Logische Mandantentrennung in den Anwendungen von AS-Trainer GmbH.
- Es werden getrennte Systeme für Test, Entwicklung und Produktion eingesetzt.
- Die Datenübertragung mit und zwischen den Systemen von AS-Trainer GmbH erfolgt verschlüsselt.
- Im Rahmen von Auftragsverarbeitungen verarbeitet AS-Trainer GmbH die überlassenen personenbezogenen Daten ausschließlich aufgrund und anhand von vertraglich vereinbarten oder dokumentierten Weisungen des Auftraggebers.
- Mit Dienstleistern und Subunternehmern werden Verträge zur Auftragsverarbeitung geschlossen, welche Regelungen enthalten, mit denen die in dieser Bestätigung enthaltenen Maßnahmen als Mindest-Standard auch den Dienstleistern auferlegt werden.
- Das genutzte externe Rechenzentrum ist nach ISO 27001 zertifiziert.

Integrität (integrity)

- Zugriffsberechtigungen werden in den Anwendungen rollenbasiert vergeben. Es wird nach dem Prinzip „need-to-know“ und „need-to-do“ verfahren.
- Jeder Zugangsberechtigte kann nur auf Daten zugreifen, die er zur Ausübung der ihm übertragenen Funktionen benötigt.
- Die Mitarbeiter sind schriftlich auf die Vertraulichkeit, bzw. das Datengeheimnis verpflichtet.
- Personenbezogene Daten werden bei Wegfall des Verarbeitungsgrunds gelöscht. Gesetzliche sowie vertragliche Aufbewahrungspflichten werden dabei beachtet.
- Die Bearbeitungsschritte, die Benutzer vornehmen, sind dem Grunde nach nachvollziehbar.
- Im Rahmen von Datenverarbeitungen im Auftrag verarbeitet AS-Trainer GmbH die überlassenen personenbezogenen Daten ausschließlich aufgrund und anhand von vertraglichen vereinbarten oder dokumentierten Weisungen des Auftraggebers.
- Kompetenzen und Kontrollmaßnahmen werden in Abstimmung mit dem Auftraggeber und technisch oder organisatorisch in die Betriebsabläufe eingebunden.
- Die Software zur Verarbeitung der Daten der Auftraggeber ist mandantenfähig.
- Es werden getrennte Systeme für Test, Entwicklung und Produktion eingesetzt.
- Die Datenübertragung mit und zwischen den Systemen von AS-Trainer GmbH erfolgt verschlüsselt.

Verfügbarkeit (availability) und Belastbarkeit (resilience)

- Die Vergabe jeglicher Benutzerkonten wird durch die Geschäftsleitung freigegeben.
- Zugangsberechtigungen zur Rechnern werden personengebunden vergeben.
- Der Kreis der jeweils befugten Personen ist auf das betriebsnotwendige Maß eingeschränkt.
- Zugriffsberechtigungen werden in den Anwendungen rollenbasiert vergeben. Es wird nach dem Prinzip „need-to-know“ und „need-to-do“ verfahren.
- Jeder Zugangsberechtigte kann nur auf Daten zugreifen, die er zur Ausübung der ihm übertragenen Funktionen benötigt.
- Die Bearbeitungsschritte, die Benutzer vornehmen, sind dem Grunde nach nachvollziehbar.
- Es findet keine lokale Datenhaltung von Daten aus Kundenaufträgen auf Workstations statt.
- Es werden getrennte Systeme für Test, Entwicklung und Produktion eingesetzt.
- AS-Trainer GmbH nutzt gespiegelte Rechenzentren an unterschiedlichen Standorten (betrieben von Plusserver an den deutschen Standorten Hürth und Frankfurt/Main).
- Backups werden vom Dienstleister Plusserver gem. einem Backup-Konzept erstellt.
- Das genutzte externe Rechenzentrum ist nach ISO 27001 zertifiziert.