more security. usd

Allgemeine Einkaufs-bedingungen für Dienst- und Werkleistungen der usd AG

Stand: 24.11.2026

Allgemeine Einkaufsbedingungen (AEB) für Dienst- und Werkleistungen der usd AG

(Stand 24.11.2026)

more security. usd

§ 1 Allgemeines, Geltungsbereich, Vertragsschluss

(1) Die usd AG, im Folgenden auch „Auftraggeber", ist ein international tätiges Beratungshaus für IT- und Informationssicherheit. Der Auftraggeber erbringt für seine Kunden, im Folgenden auch „Endkunde" genannt, Beratungs- und Dienstleistungen.

(2) Diese Allgemeinen Einkaufsbedingungen (AEB) regeln die Rahmenbedingungen für den Einkauf von Dienst- und Werkleistungen durch den Auftraggeber.

(3) Die konkreten Parameter des jeweiligen Auftrags wie beispielsweise die zu erbringenden Leistungen, der zeitliche Umfang und Ort sowie die Vergütung werden mittels einer vom Auftraggeber erstellten Bestellung mit dem Auftragnehmer (einzeln jeweils eine „Partei" und gemeinsam die „Parteien") vereinbart. Bei Widersprüchen zwischen den Regelungen der AEB und der Bestellung haben die Regelungen der Bestellung Vorrang.

(4) Für alle vom Auftraggeber erteilten Aufträge gelten für die Dauer der Geschäftsverbindung nur die nachstehenden AEB. Allgemeine Geschäftsbedingungen des Auftragnehmers haben auch dann keine Gültigkeit, wenn der Auftraggeber ihnen im Einzelfall nicht ausdrücklich widerspricht und der Auftragnehmer erklärt, nur zu seinen Bedingungen liefern zu wollen, es sei denn, dass der Auftraggeber diese Bedingungen vorher ausdrücklich und schriftlich anerkannt hat. Mit der Annahme des Auftrages, spätestens jedoch mit dem Beginn seiner Ausführung erkennt der Auftragnehmer die ausschließliche Geltung der AEB an. Die AEB gelten nur gegenüber Unternehmern im Sinne von § 310 Abs. 1 BGB.

(5) Verträge kommen mit der schriftlichen Annahme der schriftlichen Bestellung des Auftraggebers durch den Auftragnehmer zustande. An Bestellungen hält sich der Auftraggeber fünf (5) Tage ab Bestelldatum gebunden soweit nicht in der jeweiligen Bestellung eine abweichende Bindungsfrist angegeben ist. Eine verspätete Annahme durch den Auftragnehmer gilt als neues Angebot und bedarf der ausdrücklichen schriftlichen Annahme durch den Auftraggeber. Zur Wahrung der Schriftform nach diesem Absatz genügt eine einfache E-Mail oder die Übermittlung per Software.

§ 2 Zusammenarbeit der Vertragspartner

(1) Der Auftragnehmer erbringt eigenverantwortlich und selbstständig Dienst- und/oder Werkleistungen für den Auftraggeber und/oder Endkunden.

(2) Der Auftragnehmer ist bei der Erbringung der Leistung grundsätzlich weisungsfrei. Der Auftragnehmer ist dabei verpflichtet, die reibungslose Zusammenarbeit mit dem Endkunden, dem Auftraggeber und anderen Projektbeteiligten zu gewährleisten. Der Auftragnehmer sowie etwaige eingesetzte eigene Mitarbeiter und Unterauftragnehmer sind bei der Erbringung der Leistung grundsätzlich weisungsfrei.

(3) Es besteht keine Eingliederung der eingesetzten Personen in die Organisation des Auftraggebers und/oder Endkunden.

(4) Der Auftragnehmer verpflichtet sich, dem Auftraggeber (oder dessen Beauftragten), auf dessen Wunsch, zum Zwecke eines Saldenabgleichs innerhalb angemessener Frist eine Auflistung der zu einem vom Auftraggeber festgelegten Stichtag offenen Posten gegenüber dem Auftraggeber zukommen zu lassen.

§ 3 Rechte an den Leistungsergebnissen, Schutzrechte Dritter

(1) Soweit in der Bestellung nichts anderes vereinbart ist, räumt der Auftragnehmer dem Auftraggeber zum Zeitpunkt der Leistungserbringung ein zeitlich, räumlich und inhaltlich unbeschränktes sowie ausschließliches Nutzungsrecht an den Leistungsergebnissen ein.

(2) Der Auftragnehmer steht dafür ein, dass die im Rahmen des Vertrages erbrachten Leistungsergebnisse frei von Schutzrechten sind und dass nach seiner Kenntnis auch keine sonstigen Rechte bestehen, die eine Nutzung entsprechend § 3 Abs. 1 einschränken oder ausschließen. Der Auftragnehmer stellt insbesondere durch Vereinbarungen mit seinen Mitarbeitenden oder Beauftragten sicher, dass der in § 3 Abs. 1 vorgesehene Nutzungsumfang nicht durch eventuelle Miturheber- oder sonstige Rechte beeinträchtigt wird. Der Auftragnehmer stellt den Auftraggeber von allen Ansprüchen frei, die von Dritten gegen den Auftraggeber wegen der Verletzung von Schutzrechten durch die Nutzung der Leistungsergebnisse geltend gemacht werden. Der Auftraggeber benachrichtigt den Auftragnehmer unverzüglich in Textform, wenn derartige Ansprüche von Dritten gegen ihn geltend gemacht werden.

§ 4 Personal des Auftragnehmers, Unterauftragnehmer

(1) Die vom Auftragnehmer eingesetzten Personen müssen über die notwendige Kompetenz und Erfahrung verfügen, um die bestellten Leistungen gemäß den technischen und zeitlichen Anforderungen abwickeln zu können, die neben den Anforderungen des Auftraggebers und/oder des Endkunden einzuhalten sind. Der Auftragnehmer trägt Sorge für eine hohe personelle Kontinuität und wird daher Mitarbeitende oder Unterauftragnehmer nur auswechseln, wenn hierfür ein wesentlicher Grund vorliegt. Der Auftraggeber kann den Wechsel bzw. Tausch von eingesetzten Personen verlangen, soweit diese nicht die erforderlichen Voraussetzungen erfüllen oder sonst ein wesentlicher Grund vorliegt (z.B. nachhaltige Schlechtleistung, Aufforderung zum Austausch durch den Endkunden). Die mit dem Wechsel verbundenen Kosten, insbesondere Einarbeitungs- und Schulungskosten trägt der Auftragnehmer.

(2) Soweit der Auftragnehmer eine natürliche Person ist und die vereinbarten Leistungen in eigener Person erbringt: Der Auftragnehmer erbringt seine Leistungen im eigenen Namen und auf eigene Rechnung. Er erklärt, wirtschaftlich und rechtlich selbständig zu sein und insbesondere als Unternehmer in relevantem Umfang auch für andere Vertragspartner tätig zu sein. Diesbezügliche Änderungen während der Dauer des Vertrages wird der Auftragnehmer dem Auftraggeber unverzüglich mitteilen.

(3) Dem Auftragnehmer steht es frei, Unterauftragnehmer einzusetzen. Sollten durch den Einsatz im Einzelfall berechtigte Interessen des Auftraggebers beeinträchtigt werden, so hat der Auftragnehmer auf Aufforderung den weiteren Einsatz zu unterbinden. Berechtigte Interessen des Auftraggebers sind vor allem dann beeinträchtigt, wenn die eingesetzten Unterauftragnehmer nicht über die erforderlichen Qualifikationen und Berufserfahrungen verfügen, die für die effiziente und erfolgreiche Erfüllung der Aufgaben erforderlich sind. Im Falle eines Einsatzes von Unterauftragnehmern durch den Auftragnehmer ist der Auftragnehmer ge-

genüber dem Auftraggeber und/oder dem Endkunden dafür verantwortlich, dass alle sich aus der jeweiligen Bestellung ergebenden Rechte und Pflichten durch den Unterauftragnehmer erfüllt werden. Auf Verlangen des Auftraggebers belegt der Auftragnehmer die Erfüllung dieser Pflicht binnen 14 Tagen durch schriftliche Nachweise.

(4) Schaltet der Auftragnehmer ohne vorherige Abstimmung mit dem Auftraggeber Unterauftragnehmer zur Durchführung der Bestellung des Auftraggebers ein, so ist der Auftraggeber zur fristlosen Kündigung der Bestellung berechtigt und kann Ersatz des entstandenen Schadens fordern.

§ 5 Vergütung und Abrechnung

(1) Für alle vertraglichen Leistungen gelten die in der Bestellung festgelegten Stunden- oder Tagessätze bzw. Festpreise.

(2) Tagessätze verstehen sich als Tagespauschale für Leistungszeiten. Sofern mehr als acht Stunden an einem Kalendertag geleistet werden, sind die Mehrstunden nicht abrechenbar. Zuschläge, welcher Art auch immer, werden nicht vergütet. Sofern weniger als 8 Stunden geleistet werden, ist jede volle geleistete Stunde mit 1/8 des Tagessatzes zu vergüten.

(3) Festpreise verstehen sich als Gesamtpreise für die Erbringung eines spezifischen Leistungsergebnis für den Auftraggeber und/oder den Endkunden. Das Leistungsergebnis wird jeweils in der Bestellung beschrieben und erfordert eine (schriftliche) Abnahme durch den Auftraggeber und/oder den Endkunden.

(4) Nebenkosten einschließlich Reisekosten zu den Leistungsorten, Aufenthaltskosten und Spesen sind kalkulatorischer Bestandteil der Vergütungssätze und werden nicht gesondert erstattet, es sei denn, in der Bestellung ist etwas anderes vereinbart. Reisezeiten sind keine Leistungszeiten und werden nicht erstattet. Sofern nicht anders vereinbart, werden Einsätze an Samstagen sowie Sonn- und Feiertagen ohne Zuschläge zu den vereinbarten Tagessätzen vergütet.

(5) Der Auftragnehmer weist dem Auftraggeber die von ihm erbrachten Dienstleistungen mittels eines Leistungsnachweises für den abzurechnenden Monat nach. Ein Anspruch auf Vergütung besteht erst dann, wenn der Leistungsnachweis vom Auftraggeber und/oder dem Endkunden genehmigt wurde.

(6) Der Auftraggeber behält sich ausdrücklich vor, die Vergütung solcher Leistungen ganz oder teilweise zu verweigern, die vom Auftragnehmer nicht zweifelsfrei nachgewiesen werden oder deren Arbeitsergebnisse derart mangelhaft sind, dass eine Nachbesserung ausschließlich mit erheblichem Aufwand durch eigene Mitarbeiter des Auftraggebers erfolgen kann.

(7) Die Rechnung muss den gesetzlichen Vorschriften genügen und die Umsatzsteuer in jeweils geltender gesetzlicher Höhe gesondert ausweisen. Rechnungen müssen nach Möglichkeit als E-Rechnung erstellt und an usd AG, Frankfurter Str. 233, C1, 63263 Neu-Isenburg adressiert sein. Sie müssen die usd-Bestellnummer, den Namen des Endkunden, die auf der Bestellung angegebene Projektbezeichnung sowie den Namen der/des usd-Ansprechpartners/in enthalten. Rechnungen müssen sowohl einen Zeitnachweis als auch die Freigabe durch den Endkunden oder den usd-Projektleiter enthalten. Alle drei Dokumente sind in einem PDF zusammenzuführen; der Zeitnachweis ist zusätzlich als separates PDF beizufügen.

(8) Der Auftragnehmer ist verpflichtet, Rechnungen inklusive Zeitnachweis und Freigabe **bis spätestens zum 5. Werktag des Folgemonats** per E-Mail an rechnung@usd.de und vertrieb@usd.de zu senden.

(9) Es besteht keine Abnahmeverpflichtung durch den Auftraggeber. Sollte die Projektarbeit aus Gründen, die der Auftraggeber nicht zu vertreten hat, abgesagt, verschoben oder unterbrochen werden, besteht keine Verpflichtung des Auftraggebers zur Abnahme und Vergütung der beauftragten Leistungen. Ein Vergütungsanspruch des Auftragnehmers entsteht nur für tatsächlich erbrachte Leistungen.

(10) Rechnungen für werkvertragliche Leistungen werden, sofern nicht anders vereinbart, vom Auftragnehmer nach Abnahme der Leistung durch den Auftraggeber und/oder den Endkunden gestellt. Rechnungen für Dienstleistungen werden monatlich gestellt.

(11) Sachgerechte und unstrittige Rechnungen an den Auftraggeber sind 30 Tage nach Rechnungseingang zur Zahlung fällig. Zahlt der Auftraggeber innerhalb von 5 Arbeitstagen nach Rechnungseingang, ist er zum Abzug von 2 % Skonto berechtigt.

(12) Der Auftragnehmer ist verpflichtet, geschuldete Umsatzsteuer ordnungsgemäß an das Finanzamt abzuführen sowie Vergütungen eigenständig und ordnungsgemäß zu versteuern.

§ 6 Abnahme von Leistungen

(1) Hat der Auftragnehmer die vereinbarten Leistungen vollständig erbracht, stellt er die Leistungsergebnisse dem Auftraggeber und/oder dem Endkunden zu dem im Leistungs- und Fristenplan vereinbarten Termin zur Prüfung und Abnahme zur Verfügung.

(2) Die Abnahme erfolgt nach fachlicher und vertraglicher Prüfung der Leistungsergebnisse daraufhin, ob diese den vereinbarten Anforderungen, dem Leistungsumfang sowie den qualitativen und methodischen Vorgaben entsprechen. Die Prüfung beginnt spätestens innerhalb von drei Arbeitstagen nach Zurverfügungstellung der Leistungsergebnisse.

(3) Der Auftraggeber und/oder der Endkunde erklärt die Abnahme unverzüglich schriftlich oder teilt festgestellte Mängel mit.

(4) Im Falle festgestellter wesentlicher Mängel setzt der Auftraggeber und/oder der Endkunde dem Auftragnehmer eine angemessene Frist zur Beseitigung der Mängel. Nach deren Beseitigung stellt der Auftragnehmer die Leistungsergebnisse erneut zur Prüfung und Abnahme zur Verfügung. Der in Abs. 1 vereinbarte Zeitplan beginnt erneut.

(5) Teilabnahmen finden nur statt, wenn sie ausdrücklich vereinbart sind. In diesem Fall beschränkt sich die Abnahme auf die jeweils vereinbarten Teilleistungen. Die Erklärung der Gesamtabnahme bleibt hiervon unberührt.

§ 7 Verzug

(1) Der Termin- und Leistungsplan wird nach Vertragsschluss bzw. Projektstart zwischen den Parteien abgestimmt. Soweit nicht anders vereinbart, sind solche Termine verbindlich einzuhalten. Bei Verzögerungen, die der Auftragnehmer nicht zu vertreten hat, verschieben sich die von der Verzögerung betroffenen Ausführungsfristen angemessen; die gesetzlichen Ansprüche der Parteien bleiben hiervon unberührt.

(2) Im Falle eines vom Auftragnehmer verschuldeten Verzuges stehen dem Auftraggeber die gesetzlichen Rechte zu.

§ 8 Schlechtleistung

Wird eine Leistung nicht vertragsgemäß erbracht, ist der Auftraggeber berechtigt, vom Auftragnehmer zu verlangen, die Leistung ohne Mehrkosten für den Auftraggeber innerhalb angemessener Frist vertragsgemäß zu erbringen. Dies gilt nicht, wenn der Auftragnehmer die Pflichtverletzung nicht zu vertreten hat. Die sonstigen Ansprüche des Auftraggebers, insbesondere auf Schadens- oder Aufwendungsersatz und sein Recht zur Kündigung aus wichtigem Grund, bleiben hiervon unberührt.

§ 9 Datenschutz, Geheimhaltung und Sicherheit

(1) Mit seiner schriftlichen Bestätigung einer Bestellung durch den Auftraggeber verpflichtet sich der Auftragnehmer zur Einhaltung des Vertrages zur Auftragsverarbeitung (Anhang B).

(2) Der Auftragnehmer trägt dafür Sorge, dass er und alle Personen, die von ihm mit der Bearbeitung oder Erfüllung der Bestellung betraut sind, die gesetzlichen Bestimmungen über den Datenschutz, insbesondere gemäß der EU-Datenschutz-Grundverordnung und dem Telekommunikation-Telemedien-Datenschutz-Gesetz, beachten (Anhang A). Die nach Datenschutzrecht erforderliche Verpflichtung auf das Datengeheimnis ist spätestens vor der erstmaligen Aufnahme der Tätigkeit vorzunehmen und dem Auftraggeber auf Verlangen nachzuweisen.

(3) Der Auftragnehmer trägt dafür Sorge, dass er und alle Personen, die von ihm mit der Beauftragung oder Erfüllung der Bestellung betraut sind, verpflichtet wurden, die Regelungen zur Einhaltung des Sozialgeheimnisses und des Bankgeheimnisses einzuhalten (Anhang A).

(4) Die Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten vertraulichen Informationen, Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln, insbesondere nicht an Dritte weiterzugeben oder anders als zu vertraglichen Zwecken zu verwerten. Der Auftragnehmer trägt dafür Sorge, dass er und alle Personen, die von ihm mit der Bearbeitung oder Erfüllung der Bestellung betraut sind, auf die Einhaltung der Vertraulichkeit verpflichtet wurden. Die Erfüllung gesetzlicher Pflichten bleibt hiervon unberührt.

(5) Vertrauliche Informationen sind Informationen, die ein verständiger Dritter als schützenswert ansehen würde oder die als vertraulich gekennzeichnet sind; dies können auch solche Informationen sein, die während einer mündlichen Präsentation oder Diskussion bekannt werden. Die Verpflichtung zur Vertraulichkeit gilt nicht für Informationen, die den Parteien bereits vor Vertragsabschluss rechtmäßig bekannt waren oder außerhalb des Vertrages ohne Verstoß gegen eine Vertraulichkeitsverpflichtung bekannt werden.

(6) Mit seiner schriftlichen Bestätigung einer Bestellung durch den Auftraggeber verpflichtet sich der Auftragnehmer zur Einhaltung der Anforderungen des Auftraggebers an die Informations- und IT-Sicherheit (Anhang C).

(7) Der Auftragnehmer ist nur dann berechtigt, vertrauliche Informationen an Unterauftragnehmer weiterzugeben, wenn und soweit diese vertraulichen Informationen für die Erbringung der jeweiligen Leistungen durch den Unterauftragnehmer erforderlich sind (Need-to-know-Prinzip). Dies gilt auch dann nur, wenn sich der Unterauftragnehmer zuvor dem Auftragnehmer gegenüber mindestens in gleichem Umfang zum Datenschutz, zur Geheimhaltung und Sicherheit verpflichtet hat, wie der Auftragnehmer gegenüber dem Auftraggeber.

§ 10 Corporate Social Responsibility

Der Auftragnehmer verpflichtet sich, den Ethik und Verhaltenskodex des Auftraggebers zu beachten (Anhang D).

§ 11 Überprüfung der Einhaltung

Der Auftragnehmer berechtigt den Auftraggeber, die Einhaltung der Verpflichtungen aus § 9 und § 10 bei hinreichendem Anlass zu überprüfen und wirkt bei der Prüfung konstruktiv mit.

§ 12 Kündigung

(1) Beide Parteien können das Vertragsverhältnis mit einer Frist von zwei Wochen kündigen. Dies gilt auch, wenn ein bestimmter Leistungszeitraum / eine Laufzeit in der Bestellung genannt ist.

(2) Im Falle einer Kündigung nach § 12 Abs. 1 hat der Auftragnehmer einen Anspruch auf Vergütung nur der bis zum Eintreten der Kündigungsfrist ordnungsgemäß erbrachten Leistungen. Weitergehende Schadensersatz- oder Aufwendungsersatzansprüche des Auftragnehmers bestehen nicht.

(3) Die Kündigung ist per E-Mail an vertrieb@usd.de zu erklären.

(4) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund zur fristlosen Kündigung liegt insbesondere – aber nicht ausschließlich – vor, wenn der Auftragnehmer seinen Pflichten gemäß § 9 Abs. 1, Abs. 2, Abs. 3 und Abs. 4 schuldhaft innerhalb einer gesetzten angemessenen Frist nicht nachkommt oder dem Auftraggeber ein weiteres Festhalten am Vertrag nicht zumutbar ist, weil der Auftragnehmer die Verpflichtungen aus Anhang A vorsätzlich oder grob fahrlässig verletzt hat.

§ 13 Pflichten nach Vertragsende

(1) Mit Vertragsende hat der Auftragnehmer unverzüglich und unaufgefordert sämtliche vom Auftraggeber bzw. vom Endkunden erhaltenen Unterlagen, Hilfsmittel, Materialien oder Gegenstände herauszugeben, die ihm zum Zwecke der Vertragsausführung bestimmungsgemäß nicht dauerhaft überlassen wurden. Dies gilt auch für alle Kopien. Des Weiteren sind alle Leistungsergebnisse in jeglicher Form an den Auftraggeber bzw. den Endkunden zu übergeben.

(2) Der Auftraggeber ist berechtigt, an Stelle der Herausgabe ganz oder teilweise die sichere Löschung oder Vernichtung zu verlangen. Diese ist dem Auftraggeber auf Verlangen und nach seiner Wahl durch entsprechende Erklärung oder anderweitig nachzuweisen. Gesetzliche Aufbewahrungspflichten bleiben hiervon unberührt.

§ 14 Treuepflichten

(1) Während der Leistungserbringung für einen konkreten Endkunden verpflichtet sich der Auftraggeber, bei diesem Endkunden ausschließlich Vertriebsaktivitäten zugunsten des Auftraggebers durchzuführen, das heißt etwaige akquirierte Aufträge bei diesem Endkunden werden vertraglich über den Auftraggeber abgewickelt. Dies gilt bis zu sechs Monate nach Ende der jeweiligen Leistungserbringung.

(2) Der Auftragnehmer wird die Verpflichtungen nach Abs. 1 auch den von ihm im jeweiligen Einzelprojekt eingesetzten Personen oder Unterauftragnehmern auferlegen.

§ 15 Haftpflichtversicherung

Der Auftragnehmer ist verpflichtet, seine Leistungen im Rahmen der einzelnen Bestellungen durch eine Haftpflichtversicherung in angemessener Höhe, mindestens jedoch in Höhe von 250.000,- Euro (zweihundertfünfzigtausend Euro) zu decken, deren Bestehen auf Anforderung nachzuweisen ist.

§16 Einsatz von Künstlicher Intelligenz

(1) Der Einsatz von Systemen der künstlichen Intelligenz (KI), insbesondere von automatisierten, selbstlernenden oder generativen Systemen, durch den Auftragnehmer im Rahmen der Leistungserbringung ist nur nach Maßgabe dieses Absatzes zulässig.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich und unaufgefordert in Textform darüber zu informieren, ob, in welchem Umfang und zu welchem Zweck KI-Systeme bei der Leistungserbringung eingesetzt werden. Dies gilt auch für den Einsatz von KI durch Subunternehmer oder sonstige Dritte.

(3) Der Einsatz von KI-Systemen,

a) die personenbezogene Daten, vertrauliche Informationen oder Geschäftsgeheimnisse des Auftraggebers oder von Endkunden verarbeiten,

b) deren Entscheidungen oder Ergebnisse gegenüber Endkunden verwendet werden, oder

c) bei denen Daten des Auftraggebers oder von Endkunden zu Trainings-, Lern- oder Optimierungszwecken genutzt werden können,

ist nur mit vorheriger ausdrücklicher Zustimmung des Auftraggebers in Textform zulässig.

(4) Sofern der Einsatz von KI-Systemen zugelassen wird, stellt der Auftragnehmer sicher, dass

a) keine Daten des Auftraggebers oder von Endkunden zur Weiterentwicklung, zum Training oder zur Verbesserung der KI-Systeme verwendet werden,

b) keine unbefugte Weitergabe von Daten an Dritte erfolgt, und

c) sämtliche gesetzlichen und regulatorischen Anforderungen eingehalten werden.

(5) Der Auftragnehmer bleibt uneingeschränkt verantwortlich für die vertragsgemäße Erbringung der Leistungen sowie für sämtliche durch den Einsatz von KI-Systemen verursachten Ergebnisse, Fehler oder Rechtsverletzungen. Eine Haftungs- oder Verantwortungsverlagerung auf den Auftraggeber ist ausgeschlossen.

(6) Der Auftraggeber ist berechtigt, den Einsatz von KI-Systemen aus sachlichem Grund mit Wirkung für die Zukunft zu untersagen, sofern hierdurch berechtigte Interessen des Auftraggebers, insbesondere rechtliche, regulatorische oder reputationsbezogene Interessen, beeinträchtigt werden können.

§ 17 Schlussbestimmungen

(1) Die Parteien vereinbaren, dass Änderungen und Ergänzungen dieses Vertrags der Schriftform bedürfen. Ist eine Regelung dieses Vertrages unwirksam oder nicht durchsetzbar, so bleiben die restlichen Regelungen hiervon unberührt.

(2) Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechtes (CISG); keine Anwendung finden ebenso die Vorschriften des internationalen Privatrechts.

(3) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesen Bedingungen ist Frankfurt am Main, sofern der Auftragnehmer Kaufmann ist. Der Auftraggeber bleibt berechtigt, am allgemeinen Gerichtsstand des Auftragnehmers Klage oder andere gerichtliche Verfahren zu erheben oder einzuleiten. Das Recht beider Parteien, einstweiligen Rechtsschutz vor den nach den gesetzlichen Bestimmungen zuständigen Gerichten nachzusuchen, bleibt unberührt.

(4) Der deutsche Vertragstext der AEB und ihrer Bestandteile sowie die Bestellung des Auftragnehmers besitzen im Zweifelsfall Vorrang gegenüber Übersetzungen in anderen Sprachen.

Der Auftragnehmer bestätigt mit Unterzeichnung der Bestellung, sich persönlich an die unter § 9 Abs. 2 und Abs. 3 der AEB definierten Verpflichtungen zu halten und alle Personen, die von ihm mit der Bearbeitung oder Erfüllung der vom Auftraggeber aufgegebenen Bestellung betraut sind, auf die Einhaltung der nachfolgenden Regelungen vor Auftragsbearbeitung zu verpflichten.

Datengeheimnis gemäß Datenschutz-Grundverordnung der EU

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (Betroffener) beziehen.

Für personenbezogene Daten gelten die jeweils einschlägigen gesetzlichen Vorschriften zum Datenschutz wie z.B. die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union und das Bundesdatenschutzgesetz (BDSG).

Nach den Vorgaben der DSGVO dürfen personenbezogene Daten nur dann verarbeitet werden, wenn es hierzu eine Rechtsgrundlage gibt oder der Betroffene eingewilligt hat. Die Daten dürfen grundsätzlich nur zu den vorgesehenen Zwecken verwendet werden. Bei der Verarbeitung der Daten ist insbesondere zu gewährleisten, dass die Integrität, Verfügbarkeit und Vertraulichkeit der personenbezogenen Daten gewährleistet ist.

Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein;
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Fernmeldegeheimnis gemäß § 3 TDDDG

Sofern der Auftragnehmer oder die von ihm mit der Erfüllung der Bestellung betrauten Personen während Ihres Einsatzes bei der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirken, sind der Auftragnehmer oder die von ihm mit der Erfüllung der Bestellung betrauten Personen aufgrund von § 3 TDDDG zur Wahrung des Fernmeldegeheimnisses verpflichtet.

Unter das Fernmeldegeheimnis fallen die Inhalte von Telekommunikation, wie z.B. Telefongespräche oder E-Mails. Dazu zählen aber auch die Begleitumstände der Telekommunikation, wie z.B. wer an einem Gespräch teilgenommen hat oder von wem an wen eine E-Mail geschickt wurde. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Es ist dem Auftragnehmer oder den von ihm mit der Erfüllung der Bestellung betrauten Personen verboten, über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes der technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Wenn der Auftragnehmer oder die von ihm mit der Erfüllung der Bestellung betrauten Personen jedoch Kenntnis von diesen Informationen haben, dürfen sie diese nicht an unberechtigte Mitarbeitende oder Personen weitergeben. Sollte der Auftragnehmer oder die von ihm mit der Erfüllung der Bestellung betrauten Personen um solche Informationen gebeten werden, ist vor der Weitergabe der zuständige Ansprechpartner des Auftraggebers und/oder Endkunden um Erlaubnis zu fragen.

Sozialgeheimnis gemäß § 35 Sozialgesetzbuch I (SGB I)

Falls der Auftragnehmer oder die von ihm mit der Erfüllung der Bestellung betrauten Personen bei der Tätigkeit mit Sozialdaten in Kontakt kommen, ist es gemäß § 35 SGB I untersagt, unbefugt Sozialdaten zu erheben, zu verarbeiten oder zu nutzen.

Sozialdaten sind gemäß § 67 Abs. 1 SGB X Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden. Hierbei ist unbeachtlich, ob die in Frage stehende Information schützenwert erscheint oder nicht.

Bankgeheimnis

Im Rahmen der Tätigkeit bei einem Kreditinstitut ist der Auftragnehmer oder die von ihm mit der Erfüllung der Bestellung betrauten Personen zur Wahrung des Bankgeheimnisses verpflichtet. Dies bedeutet insbesondere, dass der Auftragnehmer oder die von ihm mit der Erfüllung der Bestellung betrauten Personen keine unter das Bankgeheimnis fallenden Informationen, die bei der Tätigkeit bekannt werden, an Dritte weitergeben dürfen.

Berufsgeheimnis

Aufgrund vertraglicher Vereinbarungen der usd mit ihren Kunden aus bestimmten Branchen, besteht die Möglichkeit, bei der Ausübung der Tätigkeit mit gesetzlich geschützten Geheimnissen gem. § 203 Strafgesetzbuch (StGB) von Berufsgeheimnisträgern in Berührung zu kommen. Der Auftragnehmer verpflichtet sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Erfüllung der Tätigkeit erforderlich ist. Zudem ist der Auftragnehmer verpflichtet, über die ihm bei der Ausübung oder bei Gelegenheit der Tätigkeit bekannt gewordenen Geheimnisse Stillschweigen zu bewahren und diese keinesfalls unbefugt Dritten zu offenbaren. Der Auftragnehmer wird darüber belehrt, dass er sich nach § 203 Abs. 4 S. 1 StGB strafbar macht, wenn er unbefugt ein fremdes Geheimnis offenbart.

Der Auftraggeber verarbeitet im Auftrag der Endkunden unter zur Hilfenahme von Leistungen des Auftragnehmers Daten als Auftragsverarbeiter. Der Auftraggeber tritt nicht als Verantwortlicher der Datenverarbeitung, sondern selbst als Auftragsverarbeiter des Endkunden auf. Der Endkunde trägt die datenschutzrechtliche Verantwortung.

Sofern in dieser Konstellation gemäß § 9 Abs. 1 der AEB der Abschluss einer Vereinbarung zur Auftragsverarbeitung erforderlich ist, schließen die Parteien folgenden Vertrag.

§ 1 Präambel

(1) Der Auftragnehmer verarbeitet personenbezogene Daten vom Endkunden für den Auftraggeber. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 Datenschutz-Grundverordnung (DSGVO) als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Auftragsverarbeitung ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i.S.d. Art. 28 DSGVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten.

§ 2 Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus der zugehörigen Bestellung, auf welche hier verwiesen wird.

(2) Die Dauer des Auftrags (Laufzeit) entspricht der Laufzeit der Bestellung.

§ 3 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der Aufgabe des Auftragnehmers sind der Bestellung zu entnehmen und kann die potenzielle Verarbeitung personenbezogener Daten im Rahmen von Beratungs- und Zertifizierungsprojekten sowie technischen Sicherheitsanalysen beinhalten.

(2) 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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff DSGVO erfüllt sind.

(3) Potenziell können die Daten jeglichen Kategorien angehören die auf den Systemen des Auftraggebers und/oder des Endkunden verarbeitet werden. Sowohl der Auftraggeber als auch der Auftragnehmer können im Vorfeld des Auftrags nicht absehen, welche Informationen verarbeitet werden.

(4) Potenziell können sämtliche Personen betroffen sein deren personenbezogene Daten in Bezug auf den Auftrag des Endkunden auf den Systemen des Auftraggebers und/oder des Endkunden verarbeitet werden. Der Auftraggeber und der Auftragnehmer können im Vorfeld des Auftrags nicht absehen, welche Informationen verarbeitet werden.

§ 4 Technisch-organisatorische Maßnahmen

(1) Der Auftraggeber hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten, erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung gegenüber dem Endkunden, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und diesem zur Prüfung zu übergeben. Bei Akzeptanz durch den Endkunden werden die dokumentierten Maßnahmen Grundlage des Auftrags. Demnach sind die mit dem Endkunden vereinbarten technischen und organisatorischen Maßnahmen ebenfalls von dem Auftragnehmer einzuhalten. Die Regelungen finden sich in Anhang D. Soweit eine Prüfung/ein Audit des Endkunden einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (siehe Anhang D).

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

§ 5 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Endkunde ist für die Wahrung der Betroffenenrechte allein verantwortlich.

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

(3) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 6 Qualitätssicherung, sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Vertrages gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Sofern hierzu eine gesetzliche Pflicht besteht, benennt der Auftragnehmer einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

Die Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber vor Beauftragung zur Verfügung zu stellen.

Ist der Auftragnehmer nicht zur Benennung eines Datenschutzbeauftragten verpflichtet, stellt der Auftragnehmer dem Auftraggeber die Kontaktdaten eines betrieblichen Ansprechpartners für das Thema Datenschutz zur Verfügung.

Ein Wechsel des Datenschutzbeauftragten oder des Ansprechpartners ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Die Verpflichtung der Beschäftigten ist dem Auftraggeber auf Anfrage nachzuweisen.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Anhang D).

d) Der Endkunde, der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) 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 und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 9 dieses Vertrages.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber und/oder Endkunden bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

§ 7 „Mobile Office"-Regelung

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten des Endkunden beauftragt sind, die Verarbeitung von personenbezogenen Daten im Mobile Office erlauben.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im Mobile Office der Beschäftigten des Auftragnehmers gewährleistet ist.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im Mobile Office die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im Mobile Office verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer verpflichtet seine Beschäftigten im Rahmen einer Mobile Office Richtline auf die datenschutzkonforme Verarbeitung personenbezogener Daten.

§ 8 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, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

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

(2) Der Einsatz von Unterauftragnehmern (weitere Auftragsverarbeiter) seitens des Auftragnehmers ist bei der Erbringung der vereinbarten Auftragsverarbeitung nicht vorgesehen. Die Auslagerung auf Unterauftragnehmer oder ein anschließender Wechsel der bestehenden Unterauftragnehmer ist zulässig, soweit

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Endkunden/des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Information und Zustimmung des Auftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(7) Der Auftragnehmer führt regelmäßige Kontrollen der Unterauftragnehmer durch. Diese Kontrollen sind zu dokumentieren und nach Anfrage dem Auftraggeber zur Verfügung zu stellen.

§ 9 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, die in der Regel rechtzeitig, mindestens 14 Tage vorher, anzumelden sind, sofern nicht eine Kontrolle ohne vorherige Anmeldung erforderlich erscheint, weil anderenfalls der Kontrollzweck gefährdet wäre.

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

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, eigener Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder durch eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001).

(4) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse und -rechte des Auftraggebers und von Aufsichtsbehörden auch gegenüber Unterauftragnehmern gelten. Es ist zudem vertraglich zu regeln, dass eingebundene Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen, die rechtzeitig, mindestens 14 Tage vorher, anzumelden sind, zu dulden haben. Ausgenommen sind anlassbezogene Kontrollen.

(5) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer, gemäß Ziffer 11 dieser Vereinbarung, zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

(6) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals. Ein Vergütungsanspruch besteht nicht, sofern die Kontrollen aufgrund des begründeten Verdachts eines Verstoßes des Auftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers erfolgen.

§ 10 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

b) die Verpflichtung, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere die Informationen gem. Art. 33 Abs. 3 lit. a bis d DSGVO beinhalten.

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

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

§ 11 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. 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. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Der Auftragnehmer hat dem Auftraggeber die Person(en) zu benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Bei einem Wechsel oder einer längerfristigen Verhinderung der Person(en) ist dem Auftraggeber unverzüglich schriftlich der bzw. die Nachfolger bzw. Vertreter mitzuteilen.

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

§ 12 Löschung und Rückgabe von personenbezogenen Daten

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

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Bestellung – hat der Auftragnehmer sämtliche in

seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

§ 13 Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

§ 14 Haftung

Es gelten die Haftungsregeln nach Art. 82 DSGVO.

§ 15 Sonstiges

(1) Sollte das Eigentum des Auftraggebers und/oder des Endkunden beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung oder Beschlagnahmung oder durch sonstige Ereignisse gefährdet sein, hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer weist die Dritten darauf hin, dass die Verantwortlichkeit und das Eigentum an den Daten ausschließlich beim Auftraggeber und/oder Endkunden liegen.

(2) Änderungen und Ergänzungen dieses Vertrages und aller Bestandteile bedürfen einer Zusatzvereinbarung in Textform.

(3) Sollte eine oder mehrere Klauseln aus diesem Vertrag unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Der Auftragnehmer verpflichtet sich, die nachfolgenden Informationssicherheitsanforderungen gem. § 9 Abs. 6 der AEB einzuhalten.

§ 1 Organisation der Informationssicherheit

(1) Der Auftragnehmer benennt eine Person, die die Verantwortung für die Informationssicherheit trägt und die Umsetzung der Informationssicherheitsanforderungen steuert.

(2) Der Auftragnehmer verpflichtet Unterauftragnehmer, die Einfluss auf die Informationssicherheit des Auftraggebers haben, auf die gleichen oder äquivalente Sicherheitsanforderungen.

§ 2 Verwaltung von Assets

Der Auftragnehmer führt ein Inventar aller Assets, die im Rahmen der Dienstleistungserbringung zum Einsatz kommen. Dies umfasst z.B. IT-Systeme, Software und Drittdienstleister.

§ 3 Zutritt-, Zugangs- und Zugriffskontrolle

(1) Firmenfremde werden durch firmeneigenes Personal in Empfang genommen und zum Ort der Dienstleistungserbringung begleitet bzw. an den/die firmeneigene Ansprechpartner*in übergeben. Sofern vertrauliche oder sensible Bereiche betreten werden, so ist der/die Firmenfremde dauerhaft zu begleiten.

(2) Der Auftragnehmer nutzt ein Zugriffs- und Zugangsverwaltungssystem, das komplexe Passwörter voraussetzt, um Nutzer vor Gewährung des Systemzugangs zu authentifizieren und deren Berechtigungen zu kontrollieren. Er nutzt Zwei-Faktor-Authentifizierung bei Fernzugriffen auf vertrauliche Daten.

(3) Der Auftragnehmer vergibt personalisierte Zugangs- und Zugriffsberechtigungen für eingesetzte IT-Systeme, die Auswirkungen auf die Informationssicherheit des Auftraggebers haben, ausschließlich nach dem „Least Privilege"-Prinzip, prüft sie regelmäßig und entzieht sie, wenn sie nicht mehr benötigt werden.

(4) Der Auftragnehmer verwaltet sein IT-Netzwerk so, dass verschiedene Netzzonen existieren (sofern notwendig) und durch eine Firewall oder eine gleichwertige Einrichtung getrennt sind.

§ 4 Personalsicherheit

(1) Der Auftragnehmer schult alle für die Informationssicherheit des Auftraggebers relevanten Personen einmal jährlich zu aktuellen Themen der Informationssicherheit.

(2) Der Auftragnehmer überprüft die mit der Leistungserbringung betrauten Personen anhand eines polizeilichen Führungszeugnisses oder einem äquivalenten Nachweis.

(3) Der Auftragnehmer verpflichtet die zur Leistungserbringung eingesetzten Personen zum sicheren Umgang mit vertraulichen Daten des Auftraggebers (z.B. Geheimhaltung von Kundendaten, sicherer Versand per E-Mail, sichere Entsorgung).

§ 5 Daten- und Kommunikationssicherheit

(1) Der Auftragnehmer sichert eingesetzte, tragbare IT-Geräte (z.B. Laptops) mit einer Festplattenverschlüsselung.

(2) Der Auftragnehmer überträgt und speichert vertrauliche Daten des Auftraggebers verschlüsselt nach Stand der Technik.

(3) Der Auftragnehmer verwendet keine Wechseldatenträger im Umgang mit vertraulichen Daten des Auftraggebers.

(4) Der Auftragnehmer löscht vertrauliche Daten des Auftraggebers nach Vertragsende sicher.

§ 6 Beschaffung, Wartung und Entwicklung von Systemen

(1) Der Auftragnehmer setzt IT-Systeme ein, die über ein gehärtetes Betriebssystem, Schutz vor Schadsoftware sowie hostbasierte Sicherheitssoftware verfügen und berücksichtigt Informationssicherheitsanforderungen bereits bei der Beschaffung.

(2) Der Auftragnehmer wartet eingesetzte IT-Systeme kontinuierlich und installiert verfügbare Sicherheitsupdates zeitnah.

(3) Der Auftragnehmer entwickelt Software sicher unter Berücksichtigung aktueller Branchenstandards (z.B. OWASP).

§ 7 Sicherheit im IT-Betrieb

(1) Der Auftragnehmer legt die für die Leistungserbringung relevanten IT-Systeme hinreichend redundant aus.

(2) Der Auftragnehmer bewahrt Ereignisprotokolle relevanter IT-Systeme sicher auf und überwacht diese, um den Zugang zu vertraulichen Daten und IT-Systemen zurückzuverfolgen und Sicherheitsvorfälle zu identifizieren.

(3) Der Auftragnehmer unterzieht alle aus dem Internet erreichbaren IT-Systeme, die die Informationssicherheit des Auftraggebers betreffen, technischen Sicherheitsanalysen. Kritische Schwachstellen werden zeitnah vom Auftragnehmer korrigiert.

(4) Der Auftragnehmer führt regelmäßige Datensicherungen für alle nicht beim Auftraggeber gespeicherten Daten durch, schützt diese vor unbefugten Zugriffen und sichert die Funktionstüchtigkeit durch regelmäßige Überprüfungen.

§ 8 Informationssicherheitsvorfälle

Der Auftragnehmer meldet Vorfälle, die die Informationssicherheit des Auftraggebers betreffen, innerhalb von zwei Werktagen dem Auftraggeber per E-Mail an partner-management@usd.de.

§ 9 IT-Risikomanagement

Der Auftragnehmer identifiziert, bewertet und evaluiert mit der Dienstleistung einhergehende IT-Risiken und implementiert ggf. notwendige Sicherheitsmaßnahmen.

§ 10 Geprüfte Informationssicherheit

(1) Der Auftragnehmer prüft jährlich die Einhaltung der Informationssicherheitsanforderungen und dokumentiert das Ergebnis in einem Prüfbericht. Alternativ kann sich der Auftragnehmer auf Prüfberichte unabhängiger Dritter (z.B. ISO 27001) stützen. Auf Anfrage wird dem Auftraggeber der Prüfbericht bereitgestellt.

(2) Der Auftragnehmer räumt dem Auftraggeber ein Auditrecht ein, sofern kein Prüfbericht vorgelegt wird oder es zu einem für den Auftraggeber relevanten Sicherheitsvorfall kommt.

Der Auftraggeber bekennt sich zu seiner Verantwortung im ökonomischen, ökologischen und gesellschaftlichen Sinne im Bestreben nach einer nachhaltigen Geschäftsausrichtung und orientiert sich hierbei an den 10 Prinzipien des United Nations Global Compact (UNGC) und, seit Verabschiedung der Agenda 2030 für nachhaltige Entwicklung der Vereinten Nationen, auch an den damit festgelegten 17 Nachhaltigkeitszielen. Das langfristige Ziel des Auftraggebers ist, dass alle Auftragnehmer im Laufe der Geschäftsbeziehung Bestrebungen aufzeigen dieser Verantwortung ebenfalls nachzukommen. Mit Annahme der Bestellung bestätigt der Auftragnehmer in Anlehnung an das Lieferkettensorgfaltspflichtengesetzes (LkSG) die Einhaltung der folgenden Vereinbarungen.

§ 1 Grundsätzliches

Der Auftragnehmer verpflichtet sich zur Einhaltung aller gesetzlicher Vorgaben und zur Einhaltung der internationalen Menschenrechte. Darüber hinaus ist sich der Auftragnehmer seiner gesellschaftlichen Verantwortung bewusst und sieht sich bei allen unternehmerischen Tätigkeiten in der Pflicht, dieser Verantwortung in vollem Maße gerecht zu werden. Der Auftragnehmer ist bestrebt das Thema Nachhaltigkeit proaktiv zu verfolgen und bemüht sich dafür um eine stetige Optimierung der betrieblichen Prozesse.

§ 2 Ethische Verantwortung

(1) Der Auftragnehmer handelt und entscheidet frei vom Einfluss sachfremder Erwägungen und Interessen und hält die diesbezüglich geltenden Anti-Korruptionsbestimmungen ein. Der Auftragnehmer darf im Geschäftsverkehr keine Leistungen anbieten, versprechen, fordern, gewähren oder annehmen, sofern sie nicht im Rahmen der direkten Zusammenarbeit angemessen sind. Der Auftragnehmer verpflichtet sich darüber hinaus zweifelhafte Fälle offenzulegen, die als Bestechlichkeit oder Korruption angesehen werden könnten.

(2) Der Auftragnehmer verpflichtet sich jegliche Art von absichtlicher Täuschung, mit dem Ziel einen unfairen oder illegalen Vermögensvorteil zu erhalten, zu unterlassen. Der Auftragnehmer beteiligt sich nicht an Handlungen, die den Zufluss unrechtmäßig erlangten Vermögens in den legalen Kreislauf der Finanz- und Wirtschaftswelt bezwecken.

(3) Der Auftragnehmer trennt seine unternehmerischen Interessen von den eigenen Interessen, die in einem Konflikt resultieren. Konflikte ergeben sich u. A. im Rahmen von persönlichen Beziehungen, finanziellen Vorteilen und/oder durch die Zusammenarbeit mit Wettbewerbern. Der Auftragnehmer entscheidet und handelt ohne sich dabei durch kommerziellen, finanziellen oder sonstigen Druck beeinflussen zu lassen.

(4) Der Auftragnehmer hält die Normen fairen Wettbewerbs ein. Dafür hält sich der Auftragnehmer an die geltenden Gesetze, die den Umgang mit Wettbewerbern in Bezug auf preis- und leistungsbeeinflussende Absprachen und Aktivitäten regeln.

§ 3 Soziale Verantwortung

(1) Der Auftragnehmer erfüllt stets alle Vorschriften anwendbarer Gesetze zum Verbot von Diskriminierung. Der Auftragnehmer duldet demnach keine Form der Diskriminierung oder Ungleichbehandlung aufgrund der ethnischen Herkunft, des Geschlechts, der Religion, der Weltanschauung, einer Behinderung, des Alters, einer Schwangerschaft, der sexuellen Orientierung sowie Identität oder jeglicher anderer Eigenschaften. Die persönliche Würde, Privatsphäre und Persönlichkeitsrechte jedes/jeder Einzelnen werden respektiert.

(2) Der Auftragnehmer gewährleistet Arbeitssicherheit und Gesundheitsschutz am Arbeitsplatz, sodass die körperliche Integrität und allgemeine Gesundheit der Mitarbeitenden zu keinem Zeitpunkt gefährdet sind.

(3) Der Auftragnehmer versichert, dass Löhne den jeweils geltenden gesetzlich vorgeschriebenen Mindestanforderungen und Industriestandards entsprechen und keinen unerlaubten Abzügen unterliegen. Der Auftragnehmer trägt dafür Sorge, dass geltende örtliche Arbeitszeitbeschränkungen eingehalten werden und der Branchenpraxis entsprechen.

(4) Der Auftragnehmer achtet auf das Recht der Koalitionsfreiheit der Mitarbeitenden im Rahmen der jeweils geltenden Rechte und Gesetze.

(5) Der Auftragnehmer lehnt jegliche Form von Sklaverei, Zwangsarbeit oder Schuldknechtschaft ab und gewährleistet seinen Mitarbeitenden das Recht und die Möglichkeit eine Beschäftigung freiwillig wieder aufzugeben. Der Auftragnehmer verpflichtet sich die internationalen Regelungen über das Mindestalter zur Zulassung zur Beschäftigung sowie das Verbot und die unverzügliche Beseitigung von Kinderarbeit einzuhalten. Strengere nationale Regelungen betreffend Kinderarbeit sind vorrangig anzuwenden.

§ 4 Nachhaltige Verantwortung

(1) Der Auftragnehmer erklärt den Umwelt- und Klimaschutz zum Bestandteil der verantwortungsvollen Unternehmensführung. Der Auftragnehmer bekennt sich nachhaltig zu dem Ziel des Umweltschutzes für die heutigen und künftigen Generationen. Dafür hält der Auftragnehmer die nationalen Rechtsnormen ein.

(2) Der Auftraggeber begrüßt Bestrebungen des Auftragnehmers hinsichtlich des Aufbaus, der Planung oder des Betriebs eines Umweltmanagementsystems, das potenziell negative Auswirkungen verhindert, mildert oder kompensiert, einschließlich Rohstoffverbrauch, Treibhausgasemissionen, Wasser, Abfall, Luftqualität und Biodiversität.

(3) Der Auftraggeber begrüßt den Einsatz erneuerbarer Energien durch den Auftragnehmer im Wertschöpfungsprozess.

§ 5 Zusammenarbeit

Der Auftraggeber betrachtet die Einhaltung dieser Standards und eine diesbezügliche ehrliche und aufrichtige Kommunikation als wesentlich für die Zusammenarbeit mit dem Auftragnehmer. Der Auftragnehmer stellt diese Erklärung allen mit ihm gemäß §§ 15 ff AktG verbundenen Unternehmen zur Verfügung. Der Auftraggeber spricht sich auch für die Anwendung auf Unterauftragnehmer und Zulieferer aus. Bei begründetem Misstrauen behält sich der Auftraggeber vor durch eine Befragung deren Einhaltung zu überprüfen. Bei einem bestätigten Verstoß gegen Regelungen aus diesem Ethik- und Verhaltenskodex behält sich der Auftraggeber nach einer eingehenden Beurteilung des jeweiligen Verstoßes vor, Konsequenzen im Hinblick auf das Vertragsverhältnis mit dem Auftragnehmer zu ziehen.