more security. usd

Allgemeine Geschäftsbedingungen für Dienstleistungen der usd AG

Stand: 24.11.2026

Allgemeine Geschäftsbedingungen für Dienstleistungen der usd AG (Stand: 24.11.2026)

Teil A Allgemeiner Teil

Teil B Technische Sicherheitsanalysen & Pentests

Teil C Security Audits

Teil D Vertrag zur Auftragsverarbeitung (AVV)

Teil E Technische und organisatorische Maßnahmen (TOM)

Teil A: Allgemeiner Teil

Verträge mit der usd AG (nachfolgend „usd“ oder „Auftragnehmer“) im Kontext von Beratungsdienstleistungen werden ausschließlich zu diesen Allgemeinen Geschäftsbedingungen abgeschlossen und durchgeführt. Entgegenstehende Bedingungen des Auftraggebers haben keine Gültigkeit, sofern und solange sie nicht schriftlich vom Auftragnehmer anerkannt wurden.

§ 1 Leistungen des Auftragnehmers

(1) Die Tätigkeit des Auftragnehmers besteht – sofern nicht im Einzelfall anders vereinbart – in der unabhängigen und weisungsfreien Beratung des Auftraggebers als Dienstleistung.

(2) Sofern der Auftragnehmer für den Auftraggeber als Auftragsverarbeiter im Sinne der europäischen Datenschutz-Grundverordnung (EU-DSGVO) tätig wird, verpflichtet er sich, geeignete technische und organisatorische Maßnahmen zu ergreifen, um zu gewährleisten, dass die Verarbeitung im Einklang mit der EU-DSGVO erfolgt.

(3) Der konkrete Inhalt und Umfang der zu erbringenden Tätigkeit wird im Leistungsangebot des Auftragnehmers beschrieben und mittels schriftlicher Angebotsannahme bzw. Bestellung vom Auftraggeber bestätigt.

(4) Ergibt sich die Notwendigkeit von Zusatz- oder Ergänzungstätigkeiten, wird der Auftragnehmer den Auftraggeber hierauf aufmerksam machen. In diesem Fall erfolgt eine Auftragserweiterung durch den Auftragnehmer auch dadurch, dass der Auftraggeber die Zusatz- oder Ergänzungstätigkeit anfordert oder aber entgegennimmt.

(5) Die Erbringung rechts- oder steuerberatender Tätigkeiten ist als Vertragsinhalt ausgeschlossen.

(6) Die Leistungserbringung erfolgt in einem Zeitraum von einem Jahr ab Angebotsannahme bzw. Bestellung. Sollte der Leistungszeitraum von einem Jahr überschritten werden, behält sich der Auftragnehmer vor, das Projekt vorzeitig abzuschließen. Für die Erbringung weiterer Leistungen ist dann eine separate Angebotsannahme bzw. Bestellung erforderlich.

(7) Der Auftraggeber entscheidet in alleiniger Verantwortung über die Art, den Umfang sowie den Zeitpunkt der Umsetzung der vom Auftragnehmer empfohlenen oder abgestimmten Maßnahmen. Dies gilt selbst dann, wenn der Auftragnehmer die Umsetzung abgestimmter Planungen oder Maßnahmen durch den Auftraggeber begleitet.

(8) Die Weitergabe oder Präsentation schriftlicher Ausarbeitungen oder Ergebnisse des Auftragnehmers durch den Auftraggeber gegenüber Dritten bedürfen der vorherigen Zustimmung des Auftragnehmers und erfolgen allein im Interesse und im Auftrag des Auftragnehmers. Der Dritte wird hierdurch nicht in den Schutzbereich des Auftrages zwischen dem Auftraggeber und dem Auftragnehmer einbezogen. Dies gilt auch dann,

wenn der Dritte ganz oder teilweise die Vergütung der Tätigkeit des Auftragnehmers für den Auftraggeber trägt oder diese übernimmt.

(9) Nicht abgerufene Leistungen verfallen ein Jahr nach Eingang der Beauftragung.

§ 2 Mitwirkungspflichten des Auftraggebers

(1) Der Auftraggeber benennt einen zuständigen Ansprechpartner, der sämtliche erforderlichen Fragen beantworten und alle damit zusammenhängenden Entscheidungen treffen kann. Ergänzend stellt der Auftraggeber dem Auftragnehmer die zur Auftragsdurchführung erforderlichen Informationen und Unterlagen vollständig und inhaltlich zutreffend zur Verfügung.

(2) Der Auftraggeber bestätigt dem Auftragnehmer, dass die von ihm zur Verfügung gestellten Informationen und Unterlagen vollständig und richtig sind und keine Anhaltspunkte vorliegen bzw. bekannt sind, welche geeignet sind, deren Vollständigkeit und Richtigkeit in Frage zu stellen. Zur Überprüfung der Richtigkeit, Vollständigkeit oder Ordnungsmäßigkeit oder zur Durchführung eigener Recherchen ist der Auftragnehmer nicht verpflichtet. Dies gilt auch dann, wenn im Rahmen des erteilten Auftrages vom Auftragnehmer Plausibilitätsprüfungen vorzunehmen sind, die allein an die vom Auftraggeber mitgeteilten Informationen, Angaben oder Unterlagen anknüpfen und nicht deren Überprüfung zum Inhalt haben.

(3) Erbringt der Auftraggeber nach Aufforderung des Auftragnehmers die ihm obliegenden Mitwirkungshandlungen nicht oder nicht vollständig, ist der Auftragnehmer nach vorheriger schriftlicher Ankündigung berechtigt, aber nicht verpflichtet, den abgeschlossenen Vertrag fristlos zu kündigen. In diesem Fall kann der Auftragnehmer dem Auftraggeber entweder die bis zum Kündigungszeitpunkt tatsächlich erbrachten Leistungen oder aber stattdessen die vereinbarte bzw. prognostizierte Gesamtvergütung abzüglich durch die vorzeitige Vertragsbeendigung ersparte Aufwendungen in Rechnung stellen.

(4) Die gesamte Kommunikation mit dem Auftraggeber erfolgt in den Sprachen Deutsch oder Englisch. Außerdem ist der Auftraggeber verpflichtet, notwendige Unterlagen in Deutsch oder Englisch zur Verfügung zu stellen. Sollten im Rahmen der angebotenen Leistungen Mitarbeitergespräche erforderlich sein, stellt der Auftraggeber sicher, dass diese in Englisch oder Deutsch geführt werden können. Die Unterstützung weiterer Sprachen ist vom Auftraggeber vor Auftragserteilung anzufordern und von usd nach Möglichkeit zu bestätigen.

(5) Leistungsspezifische Mitwirkungspflichten können von den allgemeinen Mitwirkungspflichten abweichen und werden in den Teildokumenten B und C oder aber in dem jeweiligen Leistungsangebot geregelt.

(6) Der Auftraggeber verpflichtet sich, dem Auftragnehmer (oder dessen Beauftragten), auf dessen Wunsch, zum Zwecke eines sogenannten Saldenabgleichs innerhalb angemessener Frist eine Auflistung der zu einem vom Auftragnehmer festgelegten Stichtag offenen Posten gegenüber dem Auftragnehmer zukommen zu lassen. Die Aufstellung muss mindestens alle offenstehenden Rechnungen, Gutschriften, nicht abgeglichenen Zahlungen, Überzahlungen, Posten auf dem Zwischenkonto und alle sonstigen Posten betreffend den Auftragnehmer enthalten.

§ 3 Projektbeendigung und Vorlauf bei Kündigung durch den Auftraggeber

(1) Eine unmittelbare oder fristlose Kündigung einzelner Projekte oder Projektbestandteile durch den Auftraggeber ist ausgeschlossen, soweit nicht ein gesetzlich zwingender Kündigungsgrund vorliegt, der aus einer vom Auftragnehmer zu vertretenden wesentlichen Pflichtverletzung resultiert.

(2) Der Auftraggeber hat bei der Kündigung eines Projekts einen angemessenen Vorlauf zur geordneten Beendigung der Tätigkeiten zu gewähren. Der erforderliche Vorlauf bemisst sich insbesondere nach Umfang, Dauer, Komplexität sowie dem wirtschaftlichen Gesamtvolumen des Projekts und beträgt mindestens sechs (6) Wochen.

(3) Ziel des Vorlaufs ist es, dem Auftragnehmer eine sachgerechte Projektabwicklung, Dokumentation, Übergabe von Arbeitsergebnissen sowie eine ordnungsgemäße Ressourcen- und Einsatzplanung zu ermöglichen. Leistungen, die bis zum Wirksamwerden der Kündigung vertragsgemäß erbracht wurden oder aufgrund des Beendigungsprozesses erforderlich sind, sind vollumfänglich zu vergüten.

§ 4 Vergütung

(1) Die Leistungen des Auftragnehmers werden, sofern nicht im Einzelfall anders vereinbart, nach Aufwand gemäß den jeweils im Leistungsangebot vereinbarten Tagessätzen (ein Tag entspricht acht Stunden), zzgl. Reisekosten und Spesen abgerechnet. Reisekosten, welche im Zusammenhang mit einer Flugreise entstehen, dürfen die Zahlung einer CO2-Kompensation enthalten (max. 200, - Euro/Flug bzw. max. 20 % des Flugpreises).

(2) Zeit- und Vergütungsprognosen des Auftragnehmers in Bezug auf die Ausführung eines Auftrages stellen eine unverbindliche Schätzung dar. Abweichungen zu der Schätzung können vom Auftragnehmer nicht ausgeschlossen werden, da der erforderliche zeitliche Aufwand von Faktoren abhängen kann, die vom Auftragnehmer nicht beeinflusst werden können.

(3) Beruht die Überschreitung des prognostizierten Zeit- oder Vergütungsumfangs auf Umständen, die vom Auftraggeber zu verantworten sind (z.B. unzureichende Mitwirkungshandlungen des Auftraggebers) ist der hieraus resultierende Mehraufwand entsprechend den vereinbarten Tagessätzen zu vergüten.

(4) Liegt die tatsächliche Bearbeitungszeit um mehr als 30 % über dem prognostizierten Zeit- oder Vergütungsumfang, besitzt der Auftraggeber nach Information durch den Auftragnehmer ein Wahlrecht entweder den Auftrag zu beenden und die bis dahin erbrachte Leistung zu den vereinbarten Konditionen zu vergüten oder den Auftrag fortzusetzen und die überschrittene Arbeitszeit zusätzlich auf Tagessatzbasis zu bezahlen.

(5) Bei Stornierung von vereinbarten Leistungsinhalten durch den Auftraggeber zahlt dieser für Absagen mit einer kürzeren Vorlaufzeit als 10 Werktage vor Durchführungstermin 100 % des vereinbarten Honorars als Ausfallhonorar, sofern der Auftragnehmer den durch die Terminabsage freigewordenen Zeitraum nicht anderweitig wirtschaftlich einsetzen kann. Gleiches gilt für den Fall einer kurzfristigen Terminverschiebung durch den Auftraggeber. Absagen oder Terminverschiebungen müssen stets in Textform per E-Mail, Fax oder Brief erfolgen. Zu diesem Zeitpunkt nicht mehr erstattungsfähige Reisekosten (Hotel, Bahnfahrten, Flüge etc.) werden dem Auftraggeber vollumfänglich in Rechnung gestellt.

(6) Für Einsätze, die auf Wunsch des Auftraggebers, werktags (Montag - Freitag) zwischen 20:00 Uhr - 6:00 Uhr (CET/CEST) erfolgen, werden die gebuchten und abrechenbaren Aufwände mit dem Faktor 1,5 multipliziert. An Samstagen, Sonn- und Feiertagen werden diese mit dem Faktor 2,0 multipliziert. Vom Auftraggeber gewünschte Tätigkeiten außerhalb der regulären Arbeitszeiten sind vom Auftraggeber vor Auftragserteilung anzufordern und von der usd zu bestätigen.

(7) Eine Abrechnung der Leistungen zum Festpreis ist möglich, sofern die zu erbringende Leistung eine Leistung darstellt, die als Gewerk erbracht und durch den Auftragnehmer abgenommen werden kann. Sofern eine Leistung zum Festpreis erbracht wird, ist der Auftragnehmer nicht zu einer Schätzung oder Dokumentation der Aufwände verpflichtet. Sofern nicht im Einzelfall schriftlich etwas anderes vereinbart ist, sind Reisekosten und Spesen im Festpreis enthalten.

(8) Die Projektkosten erhöhen sich ggf. um allgemeine Spesen für beispielsweise Bankgebühren, Büromaterial oder Kommunikation. Diese werden 2 % des Honorarvolumens nicht ohne Rücksprache mit dem Auftraggeber überschreiten.

§ 5 Zahlungsmodalitäten

Die Rechnungserstellung erfolgt im ZUGFeRD-Format. Leitweg-IDs sind dem Auftragnehmer im Zuge der Beauftragung vorab mitzuteilen. Der Rechnungsversand erfolgt ausschließlich auf elektronischem Weg per E-Mail. Rechnungen werden ohne Abzüge mit Zugang beim Auftraggeber fällig. Rechnungen sind spätestens am 14. Kalendertag nach Rechnungsdatum auf das vom Auftragnehmer angegebene Konto zu überweisen.

§ 6 Steuerliche Regelungen

(1) Bei der mit dem Auftragnehmer vereinbarten Vergütung handelt es sich um Netto-Preise, die zuzüglich der jeweils geltenden gesetzlichen nationalen Umsatzsteuer zu zahlen sind.

(2) Der Auftraggeber ist verpflichtet, die usd mit Auftragserteilung über die Rechnungsadresse und den jeweiligen Ort der Leistungserbringung zu informieren. Gilt dieser Ort der Leistungserbringung als eine Betriebsstätte des Auftraggebers, ist er als Leistungsort zu berücksichtigen und bei der Rechnungsstellung die für diesen Ort korrekte, steuerliche Regelung anzuwenden. Erfolgt hierzu keine gesonderte Information des Auftraggebers geht die usd davon aus, dass die im Angebot genannte Adresse sowohl als Rechnungsadresse als auch als Ort der Leistungserbringung anzunehmen ist.

(3) Unabhängig davon ist der Auftraggeber verpflichtet, bei einem bzw. mehreren Leistungsorten außerhalb von Deutschland, der usd folgende Informationen mit Auftragserteilung zu übermitteln:

a) Leistungsort außerhalb von Deutschland aber innerhalb der EU:
Angabe der gültigen Umsatzsteuer-Identifikationsnummer (VAT-Nummer) der gemäß Absatz 2 an die usd kommunizierten Leistungsorte.

b) Leistungsort außerhalb von Deutschland und außerhalb der EU:
Vorlage einer vom zuständigen, ausländischen Finanzamt ausgestellten „Bescheinigung über die Eintragung als Steuerpflichtiger (Unternehmer)“ der gemäß Absatz 2 an die usd kommunizierten Leistungsorte.

(4) Befindet sich der Leistungsort außerhalb von Deutschland, weist die usd keine Umsatzsteuer bei der Rechnungsstellung aus, sofern der Auftraggeber der usd vor der ersten Rechnungsstellung die unter Absatz 3 a) und b) aufgeführten erforderlichen Angaben bzw. Unterlagen für die Berücksichtigung der Umsatzsteuer zeitgerecht übergibt. Werden die erforderlichen Nachweise nicht zeitgerecht übermittelt, ist die usd berechtigt, die Rechnung unter Ausweis der zu diesem Zeitpunkt geltenden gesetzlichen Mehrwertsteuer (nach derzeitiger Rechtslage 19 %) zu stellen und an das zuständige deutsche Finanzamt abzuführen.

(5) Die Rechnungstellung erfolgt entsprechend des deutschen Umsatzsteuergesetzes (UStG) und ggf. der europäischen Mehrwertsteuersystem-Richtlinie. Demnach ist die Erbringung einer sonstigen Leistung an einen im Drittland ansässigen Unternehmer nicht in Deutschland steuerbar. Dies hat zur Folge, dass die Rechnung ohne Ausweis von Umsatzsteuer (netto) gestellt wird.

Es wird vereinbart, dass eventuell nach anderen als den Deutschen Gesetzen anfallende Steuern und Abgaben der Auftraggeber (wirtschaftlich) schuldet und die Verantwortung für eine ordnungsgemäße Deklaration gegenüber dem lokalen Fiskus trägt. Diese Vereinbarung umfasst alle Steuerarten insbesondere auch die Umsatzsteuer und

sämtliche Quellensteuern. Alternativ erhöht sich der Preis für die erbrachten Leistungen um diese Steuern und Abgaben. Der Auftragnehmer ist zur Nachforderung dieser Steuern und Abgaben beim Auftraggeber auch über den Zeitpunkt des Abschlusses des Leistungsaustauschs berechtigt.

§ 7 Haftung

(1) Mündliche oder fernmündliche Auskünfte, Erklärungen, Beratungen oder Empfehlungen erfolgen nach bestem Wissen und Gewissen. Sie sind jedoch nur verbindlich, wenn sie schriftlich bestätigt werden.

(2) Eine Haftung oder Gewährleistung für den Erfolg der vom Auftragnehmer erbrachten Leistungen sowie empfohlener Maßnahmen ist ausgeschlossen. Dies gilt auch dann, wenn der Auftragnehmer die Umsetzung abgestimmter oder empfohlener Planungen oder Maßnahmen begleitet.

(3) Der Auftragnehmer haftet bei Vorsatz oder grober Fahrlässigkeit unbegrenzt. Bei leichter Fahrlässigkeit ist die Haftung auf den typischerweise vorhersehbaren Schaden, maximal jedoch auf 25.000, - Euro, begrenzt.

(4) Die Haftung des Auftragnehmers entfällt, falls der eingetretene Schaden auf unrichtige oder unvollständige Informationen bzw. Unterlagen des Auftraggebers zurückzuführen ist oder durch Vorsatz oder grobe Fahrlässigkeit des Auftraggebers verursacht wurde. Dasselbe gilt, falls haftungsbegründende Umstände durch den Auftraggeber nicht innerhalb von 14 Kalendertagen nach Kenntniserlangung schriftlich gegenüber dem Auftragnehmer gerügt wurden.

(5) Die vorstehenden Regelungen gelten auch zugunsten der Mitarbeiter und sonstiger Erfüllungsgehilfen des Auftragnehmers.

(6) Die vorstehenden Haftungsbeschränkungen und Ausschlüsse betreffen nicht die Ansprüche des Auftraggebers aufgrund einer Verletzung des Lebens, des Körpers und der Gesundheit. Von dem Haftungsausschluss ebenfalls ausgenommen ist eine Produkthaftung.

(7) Dem Auftragnehmer steht der Einwand eines Mitverschuldens des Auftraggebers zu.

(8) Sollte der Auftragnehmer nicht in der Lage sein über einen bestimmten Zeitraum die vereinbarten Leistungen zu erbringen, wird der Auftraggeber unverzüglich darüber informiert. Der Auftragnehmer verpflichtet sich, für entsprechenden Ersatz zu sorgen.

(9) Der Auftragnehmer haftet nicht für einen mangelnden wirtschaftlichen Erfolg des Auftraggebers.

(10) Macht höhere Gewalt (z.B. Naturkatastrophen, Krieg, Terroranschlag, Epidemie) die Leistungserbringung dauerhaft unmöglich, ist eine Leistungspflicht des Auftragnehmers ausgeschlossen; bereits an den Auftragnehmer gezahlte Honorare für noch nicht erbrachte Leistungen werden in diesem Fall zurückerstattet.

§ 8 Geheimhaltung

(1) "Vertrauliche Informationen" sind, unabhängig davon, ob als "vertraulich" bezeichnet oder nicht, sämtliche Informationen (ob schriftlich, elektronisch, mündlich, digital verkörpert oder in anderer Form), die die Parteien zum vorgenannten Zweck miteinander austauschen. Als Vertrauliche Informationen in diesem Sinne gelten insbesondere:

- Angebots- und Vertragsunterlagen, Projektinhalte- und Ergebnisse, Spezifikationen, Zeichnungen, Softwarematerialien, Daten, Know-how oder Geschäftsgeheimnisse;
- Jegliche Unterlagen und Informationen des Inhabers, die Gegenstand technischer und organisatorischer Geheimhaltungsmaßnahmen sind und als vertraulich gekennzeichnet oder nach der Art und Information oder den Umständen der Übermittlung als vertraulich anzusehen sind;
- Das Bestehen dieser Vereinbarung und ihr Inhalt.

Keine Vertraulichen Informationen sind solche Informationen, hinsichtlich derer diejenige Partei, die die betreffende Vertrauliche Information erhalten hat, beweisen kann, dass die Vertrauliche Information:

- zum Zeitpunkt der Offenlegung öffentlich bekannt ist und dieser Umstand nicht auf ihr Fehlverhalten zurückzuführen ist; oder
- zum Zeitpunkt der Offenlegung an die entgegennehmende Partei dieser bereits uneingeschränkt, d.h. rechtmäßig und ohne Vertraulichkeitspflicht, bekannt waren, wobei sich ein entsprechender schriftlicher Nachweis im Besitz dieser Partei befindet; oder
- unabhängig von den offenbarten Informationen von der entgegennehmenden Partei selbst entwickelt wurde, was durch Einsicht in die schriftlichen Akten nachweisbar ist; oder
- der entgegennehmenden Partei von einem berechtigten Dritten ohne Verstoß gegen eine Geheimhaltungspflicht übergeben oder zugänglich gemacht wurde; oder
- gemäß schriftlicher Zustimmung durch die offenbarende Partei von derartigen Einschränkungen befreit ist.

(2) Die Parteien versprechen einander:

a) Dass sie Vertrauliche Informationen mindestens mit dem gleichen Maß an Sorgfalt, das sie gewöhnlich für den Schutz ihrer eigenen vertraulichen oder urheberrechtlich geschützten Informationen zugrunde legen, als vertraulich behandeln;

b) Dass sie Vertrauliche Informationen nur zu dem in dieser Vereinbarung vorgesehenen Zweck verwenden;

c) Die Offenlegung solcher Informationen auf den Kreis der Mitarbeiter zu beschränken, die diese Kenntnisse für den vorgesehenen Zweck benötigen und die berechtigten Mitarbeiter über die in dieser Vereinbarung eingegangenen Verpflichtungen zu unterrichten. Durch die Parteien wird sichergestellt, dass sämtliche berechtigte Mitarbeiter vom wesentlichen Inhalt dieser Vereinbarung Kenntnis nehmen;

d) Sofern die Parteien im Rahmen der Geschäftsbeziehung zwischen den Parteien Verträge mit Dritten eingehen, mit diesen Dritten Vereinbarungen zu schließen, die dieser Vereinbarung inhaltlich entsprechen und deren Einhaltung sicherzustellen;

e) Angaben über angebotene, ausgehandelte oder geänderte Beträge von Entgelten, Verrechnungspreisen, Provisionen oder sonstige im Rahmen eines Vertragsverhältnisses vereinbarten Zahlungen keinesfalls Dritten offenzulegen und Sorge dafür zu tragen, dass nur solche ihrer Mitarbeiter Kenntnis von diesen Angaben erlangen, für die es zur Entscheidung über die Eingehung eines Vertragsverhältnisses oder die Durchführung eines geschlossenen Vertrages unbedingt erforderlich ist;

f) Die Vertraulichen Informationen ebenfalls durch angemessene Geheimhaltungsmaßnahmen gegen den unbefugten Zugriff durch Dritte zu sichern und bei der Verarbeitung der Vertraulichen Informationen die gesetzlichen und vertraglichen Vorschriften zum Datenschutz einzuhalten. Dies beinhaltet auch dem aktuellen Stand der Technik angepasste technische Sicherheitsmaßnahmen (Art. 32 DSGVO) und die Verpflichtung der Mitarbeiter auf die Vertraulichkeit personenbezogener Daten und die Beachtung des Datenschutzes i. S. d. Art. 28 Abs. 3 lit. b DSGVO.

Jede Vertragspartei ist zur Weitergabe von Vertraulichen Informationen berechtigt, soweit sie aufgrund einer Rechtsvorschrift oder behördlicher Anordnung dazu verpflichtet ist, die andere Partei (soweit rechtlich möglich und praktisch umsetzbar) über die beabsichtigte Weitergabe schriftlich informiert hat und die nach Gesetz vorgesehene und angemessene Vorkehrungen getroffen hat, um den Umfang der Weitergabe so gering wie möglich zu halten.

§ 9 Datenschutz

(1) Im Rahmen der Leistungserbringung ist es möglich, dass die Berater des Auftragnehmers Einsicht in die von dem Auftraggeber etwaig gespeicherten, personenbezogenen Daten nehmen. Die Einsichtnahme ist datenschutzrechtlich als Übermittlungsvorgang zu qualifizieren.

(2) Mit Unterzeichnung der Leistungsvereinbarung bzw. des Angebotes, die Bestandteil des intendierten Vertrages ist, versichert der Auftraggeber, dass er zur etwaigen Übermittlung von personenbezogenen Daten berechtigt ist. Andernfalls schließt der Auftraggeber die Einsichtnahme von personenbezogenen Daten durch geeignete Maßnahmen (z.B. Pseudonymisierung oder Anonymisierung) aus.

(3) Der Auftragnehmer hat alle Mitarbeiter, die mit der Vertragserfüllung betraut sind, auf die strenge Einhaltung der anwendbaren datenschutzrechtlichen Vorschriften verpflichtet. Etwaige im Rahmen der Leistungserbringung eingesehen personenbezogene Daten wird der Auftragnehmer nicht speichern oder nur speichern, nutzen oder verarbeiten, soweit und solange dies zur Erfüllung des jeweiligen Vertrages zwingend erforderlich ist.

(4) Im Übrigen erfolgt jede weitere Verarbeitung von personenbezogenen Daten durch den Auftragnehmer ausschließlich auf Weisung des Auftraggebers. Der Auftragnehmer darf die Daten des Auftraggebers nur im Rahmen dieser Weisung verarbeiten oder nutzen. Im Teil D schließen die Parteien einen Auftragsverarbeitungsvertrag ab.

§ 10 Loyalitätsverpflichtung

Auftraggeber und Auftragnehmer verpflichten sich zur gegenseitigen Loyalität. Insbesondere die Abwerbung von Mitarbeitern, die im Zusammenhang mit der Auftragsdurchführung tätig gewesen sind, vor Ablauf von zwei Jahren nach Beendigung der Zusammenarbeit, ist zu unterlassen.

§ 11 Sonstige Tätigkeiten

Dem Auftragnehmer steht es frei, für andere Auftraggeber tätig zu werden. Einer vorherigen Zustimmung des Auftraggebers bedarf es hierfür nicht.

§ 12 Urheber-, Nutzungs- und Verwertungsrechte

Der Auftraggeber ist berechtigt, die vertragsgegenständliche Leistung für den vertraglich vorausgesetzten Zweck ohne örtliche, persönliche oder quantitative Einschränkungen zu gebrauchen. Hierzu räumt der Auftragnehmer dem Auftraggeber das unwiderrufliche, weltweite, zeitlich unbefristete und nicht-ausschließliche Nutzungsrecht ein. Die übertragenen Rechte unterliegen keinen Verfügungsbeschränkungen.

§ 13 Rückmeldung zu den Leistungen des Auftragnehmers

Um die Leistungen kontinuierlich zu verbessern und an die Bedürfnisse des Auftraggebers anzupassen, bittet der Auftragnehmer den Auftraggeber, nach der Durchführung der angebotenen Leistungen Rückmeldung über die Zufriedenheit zu geben.

§ 14 Referenzkundennennung

Der Auftragnehmer ist berechtigt, den Auftraggeber nach erfolgreichem Abschluss des Projekts als Referenzkunden zu benennen und dessen Firmenlogo in Referenzlisten (Print, Webseite, Social Media, Präsentationen, Angeboten und Ausschreibungen) zu verwenden. Die Verwendung erfolgt ausschließlich als sachlicher Hinweis auf die bestehende/abgeschlossene Zusammenarbeit und unter Einhaltung der Markenrichtlinien des Auftraggebers.

Eine Veröffentlichung weitergehender Informationen (wie bspw. Pressemitteilungen, Case Studies, Testimonials oder eine detaillierte Darstellung des Projekts) erfolgt ausschließlich nach vorheriger Abstimmung mit dem Auftraggeber.

Vertrauliche Informationen und sicherheitsrelevante Details werden nicht veröffentlicht; § 8 [Geheimhaltung] bleibt unberührt.

Auf Wunsch verpflichtet sich der Auftragnehmer jederzeit Auskunft zu erteilen, wie und in welchem Umfang eine Nutzung erfolgt; entsprechende Informationen sind dem Auftraggeber auf Wunsch kostenlos zur Verfügung zu stellen.

Der Auftraggeber kann sein Einverständnis jederzeit und ohne Angabe von Gründen ganz oder teilweise widerrufen. Der Auftragnehmer setzt den Widerspruch spätestens binnen 10 Werktagen um.

§ 15 Schlussbestimmungen

(1) Alle Anhänge der Leistungsvereinbarung bzw. des Angebotes sind Bestandteil des Vertrages zwischen Auftragnehmer und Auftraggeber. Die Regelungen in den Leistungsvereinbarungen ersetzen bei Abweichungen die AGB.

(2) Änderungen oder Ergänzungen des Auftrages oder dieser Allgemeinen Geschäftsbedingungen bedürfen zu ihrer Wirksamkeit der Einhaltung der Schriftform. Eine stillschweigende Änderung des Auftrages oder der Allgemeinen Geschäftsbedingungen wird ausgeschlossen.

(3) Sollte eine Regelung aus einer Leistungsvereinbarung oder dieser Geschäftsbedingungen rechtsunwirksam sein oder werden, berührt dies die Rechtswirksamkeit der übrigen Regelungen des Auftrages sowie dieser Geschäftsbedingungen nicht. Für diesen Fall ist zwischen den Vertragsparteien eine rechtswirksame Regelung zu vereinbaren, die dem Sinn und Zweck sowie der wirtschaftlichen Zielsetzung der unwirksamen Klausel am nächsten kommt. Entsprechend ist zu verfahren, falls der Auftrag oder diese Geschäftsbedingungen eine regelwidrige Lücke aufweisen sollten, die durch eine ergänzende Vertragsauslegung zu schließen ist.

(4) Es gilt ausschließlich das Recht der Bundesrepublik Deutschland unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG).

(5) Der ausschließliche Gerichtsstand ist Frankfurt am Main, soweit der Auftraggeber Kaufmann ist. Der Auftragnehmer ist daneben berechtigt, auch am allgemeinen Gerichtsstand des Auftraggebers zu klagen.

(6) Der deutsche Vertragstext der Allgemeinen Geschäftsbedingungen und ihrer Bestandteile sowie die Leistungsangebote des Auftragnehmers besitzen im Zweifelsfall Vorrang gegenüber Übersetzungen in anderen Sprachen.

(7) Leistungsspezifische AGB können von den allgemeinen AGB abweichen und werden in den Einzelvereinbarungen, Leistungsinhalten oder in den AGB Teildokumenten B und C geregelt.

(8) Der Auftragnehmer hält die im Rahmen der beauftragten Tätigkeit gefertigten Ausarbeitungen und Ergebnisse für die Dauer von 6 Jahren nach Abschluss der beauftragten Tätigkeit für den Auftraggeber zum Abruf bereit. Vor Ablauf dieses Zeitraums kann der Auftraggeber von dem Auftragnehmer jederzeit die Löschung der Ausarbeitungen und Ergebnisse verlangen. 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. Ebenfalls nicht erfasst sind Nachweise hinsichtlich der auftrags- und ordnungsgemäßen Erbringung der vereinbarten Tätigkeit. Diese werden über das Vertragsende hinaus entsprechend den jeweilig zu beachtenden Aufbewahrungsfristen aufbewahrt.

Teil B: Technische Sicherheitsanalysen & Pentests

§ 1 Haftung, Haftungsbegrenzung, Haftungsausschluss

(1) Der Auftragnehmer ist nicht verpflichtet zu überprüfen, ob der Auftraggeber die vollumfänglichen und uneingeschränkten Rechte an dem zu testenden IT-System und/oder der Applikation innehat.

(2) Die Haftung für Datenverluste wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrentsprechender Anfertigung von Sicherungskopien eingetreten wäre. Der Auftragnehmer haftet nicht für solche Schäden, die darauf beruhen, dass der Auftraggeber die technische Sicherheitsanalyse während der Ausführung unterbricht.

§ 2 Freistellungsverpflichtung des Auftraggebers

(1) Wird der Auftragnehmer von einem Dritten (z.B. ein Kunde oder Dienstleister des Auftraggebers) aufgrund etwaiger Auswirkungen der technischen Sicherheitsanalyse auf das IT-System und/oder die Applikation in Anspruch genommen, verpflichtet sich der Auftraggeber, den Auftragnehmer von jeglichen Ansprüchen freizustellen, sofern

a) die technische Sicherheitsanalyse einem anerkannten und angemessenen Standard entsprach (andernfalls gilt „Teil A Haftung" entsprechend) oder

b) der Schaden aufgrund einer Pflichtverletzung des Auftraggebers (mit-) verursacht wurde, weil der Auftraggeber

- ein fremdes IT-System/eine fremde Applikation ohne entsprechende Erlaubnis hat testen lassen,
- betroffene Dritte nicht oder nicht mit angemessener Frist über die stattfindende technische Sicherheitsanalyse informiert hat oder
- über keine datenschutzrechtliche Erlaubnis zur Übermittlung von personenbezogenen Daten verfügt hat.

(2) Die Freistellungspflicht bezieht sich auf alle Aufwendungen, die dem Auftragnehmer oder dessen eingesetzten Mitarbeitern und sonstigen Erfüllungsgehilfen aus der außergerichtlichen, behördlichen und/oder gerichtlichen Inanspruchnahme durch einen Dritten notwendigerweise erwachsen. Der Auftraggeber hat dabei sämtliche Kosten und Gebühren für die notwendige rechtliche Verfolgung zu übernehmen, sowie sämtliche Schäden, Verluste und Ausgaben zu ersetzen.

§ 3 Gewährleistung

(1) Der Auftragnehmer weist den Auftraggeber ausdrücklich darauf hin, dass die technische Sicherheitsanalyse Einfluss auf die Integrität und Verfügbarkeit der getesteten IT-Systeme und/oder Applikationen haben kann.

(2) Der Auftragnehmer gewährleistet und stellt sicher, dass die für die technische Sicherheitsanalyse verwendeten Methoden und Werkzeugen einem anerkannten und angemessenen Standard entsprechen.

(3) Eine weitergehende Verpflichtung oder Gewährleistung des Auftragnehmers besteht nicht. Der Auftragnehmer unterliegt keiner Gewährleistungshaftung bei einem Schaden aufgrund einer Beeinträchtigung der Integrität und/oder der Verfügbarkeit des getesteten IT-Systems und/oder der Applikation, der durch eine ordnungsgemäße, das heißt durch eine mit anerkannten und angemessenen Standards durchgeführten technischen Sicherheitsanalyse hervorgerufen wird oder wurde.

(4) Im Übrigen gilt Teil B, §1, „Haftung, Haftungsbegrenzung, Haftungsausschluss" entsprechend.

§ 4 Mitwirkungspflichten des Auftraggebers

(1) Mit Beauftragung der Leistungsvereinbarung versichert der Auftraggeber, dass die technische Sicherheitsanalyse auf den durch den Auftraggeber zum Zweck der Durchführung schriftlich übermittelten IT-Systemen und/oder Applikationen des Auftraggebers erfolgt, bzw. erfolgen soll.

(2) Insoweit die technische Sicherheitsanalyse nicht auf den IT-Systemen und/oder Applikationen des Auftraggebers erfolgt, versichert der Auftraggeber mit Beauftragung der Leistungsvereinbarung, dass er das vollumfängliche und uneingeschränkte Recht zur Durchführung der technischen Sicherheitsanalyse auf den IT-Systemen und/oder Applikationen hat.

(3) Auf Verlangen des Auftragnehmers hat der Auftraggeber nachzuweisen, dass er über das uneingeschränkte Recht zur Beauftragung des Auftragnehmers zur Durchführung der technischen Sicherheitsanalyse und die Rechte für den Zugriff auf die IT-Systeme und/oder Applikationen verfügt.

(4) Vor der Durchführung der technischen Sicherheitsanalyse durch den Auftragnehmer, verpflichtet sich der Auftraggeber, sämtliche durch den Auftragnehmer zu prüfenden IT-Systeme und/oder Applikationen und die damit in Verbindung stehenden Daten vollumfänglich durch ein Backup zu sichern. Darüber hinaus hat der Auftraggeber sämtliche notwendigen Sicherheitsmaßnahmen, auch diejenigen, die über ein Backup hinausgehen, vor Nutzung der Dienstleistung zu treffen, um die IT-Systeme und/oder Applikationen und Daten notfalls nach der technischen Sicherheitsanalyse wieder in den ursprünglichen Zustand zurück versetzen zu können.

(5) Der Auftraggeber stellt dem Auftragnehmer abhängig von der Art der technischen Sicherheitsanalyse die zur – möglichst sicheren und schadlosen – Durchführung notwendigen Informationen und Unterlagen zur Verfügung. Vor Durchführung der technischen Sicherheitsanalyse wird der Auftragnehmer dem Auftraggeber mitteilen, welche Informationen benötigt werden. Der Auftraggeber wird dem Auftragnehmer daraufhin die erforderlichen Informationen zeitgerecht, vollständig und richtig zur Verfügung stellen.

(6) Der Auftraggeber informiert mit angemessener Frist vor Durchführung der technischen Sicherheitsanalyse etwaig betroffene Dritte über die durchzuführende technische Sicherheitsanalyse, da bei einer technischen Sicherheitsanalyse auch IT-Systeme und/oder Applikationen Dritter, wie etwa der Router des Providers oder der Webserver eines Hosters, genutzt werden und trotz ausreichender Sicherheit eine Beeinträchtigung des ordnungsgemäßen Betriebes dieser IT-Systeme und/oder Applikationen nicht ausgeschlossen werden kann.

(7) Der Auftraggeber wird ausdrücklich darauf hingewiesen, dass durch die technische Sicherheitsanalyse Schäden in bestehenden IT-Systemen und/oder Applikationen auftreten können. Insbesondere können durch die technische Sicherheitsanalyse Beeinträchtigungen und Veränderungen von Inhalten und Daten wie zum Beispiel auf einer Webseite in Form von Layout-Veränderungen oder Beeinträchtigungen des Servers des Auftraggebers auftreten. Diese Schäden sind meist nur durch das Einspielen von Backups, oder durch – teilweise umfangreiche – Nachbearbeitung durch den Auftraggeber zu beheben. Darüber hinaus wird der Auftraggeber darauf hingewiesen, dass die IT-Systeme und/oder Applikationen des Auftraggebers während der technischen Sicherheitsanalyse möglicherweise nicht nutzbar sind.

§ 5 Eingesetzte Tools und Werkzeuge

(1) Im Rahmen von technischen Sicherheitsanalysen nutzt der Auftragnehmer die weltweit besten Tools. Die Verwendung der Tools erlaubt es dem Auftragnehmer seine Prüfungen effizienter und dadurch wesentlich umfassender zu gestalten. Der Auftraggeber profitiert durch qualitativ sehr hochwertige Ergebnisse. Die daraus resultierenden Lizenzkosten sind in den jeweiligen Angeboten bereits eingepreist und werden nicht separat berechnet.

(2) Technische Sicherheitsanalysen, die von den Büros des Auftragnehmers über das Internet durchgeführt werden, erfolgen aus einem dedizierten öffentlichen Netzwerk mit bekannten, festen IP-Adressen. Dies gewährleistet, dass die Aktivitäten des Auftragnehmers von den Betriebsverantwortlichen des Auftraggebers jederzeit eindeutig zugeordnet werden können.

§ 6 Responsible Disclosure

(1) Schwachstellen in Standardprodukten, die nicht vom Auftraggeber selbst hergestellt wurden, meldet der Auftragnehmer in einem strukturierten Prozess zur verantwortungsvollen Offenlegung von Sicherheitsschwachstellen (Responsible Disclosure).

(2) Dies erfolgt streng vertraulich, schriftlich und in einer Form, die es dem Hersteller ermöglicht, die Schwachstelle nachzuvollziehen und zu schließen.

(3) Der Auftragnehmer behält sich vor, die gefundenen Schwachstellen zu veröffentlichen.

(4) Innerhalb einer Frist von 60 Tagen muss der Hersteller eine Lösung bereitstellen. Sollte dies nicht geschehen, kann die Veröffentlichung nach Ablauf dieser Frist dennoch erfolgen.

(5) Von diesem Vorgehen weicht der Auftragnehmer in Fällen ab, in denen eine andere Vorgehensweise die Risiken aller betroffenen Parteien nachweislich mindern würde.

(6) Mit Beauftragung der Leistungsvereinbarung stimmt der Auftraggeber der beschriebenen Vorgehensweise zu.

Teil C: Security Audits

§ 1 Mitwirkungspflichten des Auftraggebers: KRITIS Audit (Kritische Infrastrukturen)

(1) Da der Auftragnehmer seine Qualifikation als KRITIS Auditor über das Dokument "Selbsterklärung der prüfenden Stelle" (siehe BSI Selbsterklärung) nachweist, ist der Auftraggeber verpflichtet, die Selbsterklärung zusammen mit den offiziellen Bewertungsunterlagen dem BSI vorzulegen.

(2) Darüber hinaus wird der Auftraggeber dem Auftragnehmer seinen branchenspezifischen Sicherheitsstandard (B3S) liefern.

§ 2 Mitwirkungspflichten des Auftraggebers: PCI Security Services

(1) Der Auftraggeber hat dem Auftragnehmer Informationen zu seinem Audit-Scope bereitgestellt, die im Rahmen der Angebotserstellung für die Preisermittlung herangezogen wurden. Sollte der tatsächliche Scope von dem angenommenen Scope aufgrund falscher oder unvollständiger Informationen abweichen, behält sich der Auftragnehmer vor, dadurch ggf. entstehende Mehraufwände in der Audit-Durchführung nach Rücksprache dem Auftraggeber in Rechnung zu stellen.

(2) Im Kontext von PCI SSF und PCI Secure Software Standard (Teil des PCI SSF) Assessments stellt der Auftraggeber zusätzlich die erforderliche Testumgebung (siehe aktuelles "Secure Software Template for Report on Validation", Appendix B) zur Verfügung.

§ 3 Sonstige PCI DSS Leistungen

Zur Nutzung der PCI DSS Scanleistungen, des PCI DSS Zertifikats und des PCI DSS Prüfsiegels der usd sind die Allgemeinen Nutzungsbedingungen für die Security Plattformen der usd AG zu beachten, die für diese Leistungen gelten: https://www.usd.de/rechtliche-hinweise

§ 4 Rückmeldung zu den Leistungen der usd

Das PCI Security Standards Council (PCI SSC) gibt dem Auftraggeber die Möglichkeit, zentral Rückmeldung über die erbrachten QSA Leistungen des Auftragnehmers zu geben. Unter dem folgenden Link steht dem Auftraggeber der Feedbackbogen des PCI SSC zur Verfügung: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors_feedback

§ 5 PCI Security Standards Council (PCI SSC)

(1) Das PCI SSC behält sich vor, den Assessmentbericht sowie alle im Rahmen des Assessments erstellten und bereitgestellten Unterlagen des Auftragnehmers sowie vom Auftraggeber bereitgestellte Unterlagen ohne vorheriges Einholen einer zusätzlichen

Freigabe einzusehen. Der Auftragnehmer ist in seiner Rolle als akkreditierter Assessor durch das PCI SSC verpflichtet, die Unterlagen auf Anforderung weiterzugeben. Der Auftraggeber stimmt diesem Verfahren zu.

(2) Der Auftragnehmer übernimmt grundlegend keine Kosten für Listungen bei den Payment Brands, wie beispielsweise Visa oder Mastercard, sowie bei dem PCI SSC.

Teil D: Vertrag zur Auftragsverarbeitung (AVV)

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung

zwischen dem

- Verantwortlichen - nachstehend Auftraggeber genannt –

und der

usd AG
Frankfurter Str. 233, Haus C1
63263 Neu-Isenburg

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

Präambel

(1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. 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.

1. Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus der zugehörigen Leistungsvereinbarung bzw. dem zughörigen Angebot auf welche/s hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der Aufgaben des Auftragsnehmers ist die potenzielle Verarbeitung personenbezogener Daten im Rahmen von Beratungs- und Zertifizierungsprojekten sowie technischen Sicherheits- und Schwachstellenanalysen entsprechend der Leistungs-vereinbarung.

(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 verarbeitet werden. Der Auftragnehmer kann im Vorfeld der Projekte und Analysen nicht absehen, welche Informationen im Rahmen des Auftrags verarbeitet werden.

(4) Potenziell können sämtliche Personen betroffen sein, deren personenbezogene Daten auf den Systemen des Auftraggebers verarbeitet werden. Der Auftragnehmer kann im Vorfeld der Projekte und Analysen nicht absehen, welche Informationen im Rahmen des Auftrags verarbeitet werden.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers 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 [Einzelheiten in Teil E].

(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.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftraggeber 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.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

DEUDAT GmbH
Marcel Wetzel
Wasserrolle 16
65201 Wiesbaden
Telefon: +49 611 950008-40
E-Mail: kontakt@deudat.de

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 und Art. 32 DSGVO [Einzelheiten in Teil E].

d) 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 Ziffer 8 dieses Vertrages.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12 bis 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.

6. „Mobile Office"-Regelung

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber 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. Jeder Beschäftigte arbeitet aus Gründen der Sicherheit auch im Mobile Office auf Endgeräten der usd.

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

7. 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 Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Einsatz von Unterauftragnehmern (weitere Auftragsverarbeiter) 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 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 Hauptauftraggebers (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.

8. 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 BSI-Grundschutz).

(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.

9. 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.

10. 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.

Weisungsempfangsberechtigte Personen des Auftragnehmers sind:

Herr Andreas Duchmann,
Vorstand
Telefon: +49 6102 8631-0
E-Mail: datenschutz@usd.de

Frau Andrea Tubach
Vorstandsvorsitzende
Telefon: +49 6102 8631-0
E-Mail: datenschutz@usd.de

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11. 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 Leistungsvereinbarung – 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. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. 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.

13. Haftung

Es gelten die Haftungsregeln nach Art. 82 DSGVO.

14. Sonstiges

(1) Sollte das Eigentum des Auftraggebers 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 liegen.

(2) Änderungen und Ergänzungen dieser Zusatzvereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung.

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

Teil E: Technische und organisatorische Maßnahmen (TOM)

Die nachfolgend beschriebenen allgemeinen technischen und organisatorischen Maßnahmen entsprechen Art. 32 Abs. 1 DSGVO und Art. 25 Abs. 1 DSGVO und sind gültig für alle Beratungsleistungen des Auftragnehmers.

§ 1 Maßnahmen zur Sicherstellung der Vertraulichkeit

a) Zutrittskontrolle

- Zugang zu den Räumlichkeiten erfolgt lediglich über festgelegte Eingänge.
- Kundenzutritt ausschließlich über einen festgelegten Eingang.
- 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.
- Sicherung der Geschäftsräume des Standortes Neu-Isenburg durch eine Alarmanlage mit angeschlossenem Wachdienst.
- Zugang zum Serverraum nur über ein 2-Faktor-Kontrollsystem mit personifizierter Zutrittssteuerung sowie restriktivem Zutrittskonzept.
- Zutritt zum Serverraum für Externe ausschließlich in Begleitung eines autorisierten, firmeneigenen Mitarbeiters.
- Zugang zu Housing-Provider mit restriktivem Zutrittskonzept, kontrollierten Zutrittsverfahren, personifizierter Zutrittssteuerung und vorheriger Identifizierung.
- Betrieb der usd Serversysteme bei Housing-Provider in eigenen, exklusiven und abgeschlossenen Serverschränken.
- Dokumentation der Schlüsselverwaltung.
- Etablierter Check-In/Check-Out-Prozess für Mitarbeiter.

b) Zugangskontrolle

- Komplexitätsanforderungen an Passwörter.
- Verwendete Passwörter werden gemäß dem Stand der Technik verschlüsselt.
- Personalisierte Zugänge zu Datenverarbeitungsanlagen.
- Passwortregelung/-schutz von allen PCs.
- Sperrung von Benutzerkonten nach mehrmaligen fehlgeschlagenen Anmeldeversuchen.
- Es wurde ein restriktives Rollen- und Berechtigungskonzept implementiert.
- Umsetzung eines Firewall-Konzeptes.
- Einsatz von aktuellen SPAM- und Virenfiltern.
- Sperrung des Arbeitscomputers nach Zeitablauf mit Passwortabfrage bei Reaktivierung.

c) Zugriffskontrolle

- Es wurde ein restriktives Rollen- und Berechtigungskonzept für den Zugriff auf personenbezogene Daten implementiert.
- Regelmäßige Überprüfung der festgelegten Befugnisse bzw. Zugriffsrechte der Mitarbeiter.
- Sperrung des Arbeitscomputers nach Zeitablauf mit Passwortabfrage bei Reaktivierung.
- Wartung durch externe Dienstleister ausschließlich in Anwesenheit des Systemverwalters.
- Systemhärtung und regelmäßige Systemaktualisierung mittels Softwareupdates und Patches.
- Schulung und Sensibilisierung der Mitarbeiter.
- Protokollierung relevanter Systemaktivitäten.

d) Trennungskontrolle

- Mandantentrennung.
- Rollen- und Berechtigungskonzept.

e) Pseudonymisierung

Risikoorientiert und in Abstimmung mit dem Auftraggeber können in technischen Verfahren unter Berücksichtigung der Integrität und der Aufgabenstellung personenbezogene Daten pseudonymisiert verarbeitet werden.

f) Verschlüsselung

- Eine Übertragung von Daten erfolgt ausschließlich in einer dem aktuellen Stand der Technik entsprechenden verschlüsselten Form.
- Mobile Wechseldatenträger sind standardmäßig gesperrt und werden nur in begründeten Ausnahmefällen für den verschlüsselten Dateiaustausch freigegeben.
- Festplattenverschlüsselung auf den Laptops.
- Verschlüsselungen von Backups.

§ 2 Maßnahmen zur Sicherstellung der Integrität

a) Weitergabekontrolle

- Kontrollierte datenschutzgerechte Vernichtung von Datenträgern.
- Eine Übertragung von Daten erfolgt ausschließlich in einer dem aktuellen Stand der Technik entsprechenden, verschlüsselten Form.
- Kontrollierte Übermittlung durch den jeweiligen Verantwortlichen.
- Verschlüsselung von Datenträgern.
- Eine Weitergabe von personenbezogenen Daten erfolgt ausschließlich im Rahmen der Kundenbeziehung nach vertraglichen Regelungen.
- Übermittlung von Daten erfolgt ausschließlich über definierte Schnittstellen.

b) Eingabekontrolle

- Protokollierung relevanter Systemaktivitäten.
- Es wurde ein restriktives Rollen- und Berechtigungskonzept implementiert.
- Anlassbezogene Auswertung von Protokollen.

§ 3 Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

- Vorhandensein und Umsetzung eines Konzeptes zur Durchführung von regelmäßigen Datensicherungen (Backup-Konzept).
- Umsetzung eines Firewall-Konzeptes.
- Einsatz von aktuellen SPAM- und Virenfiltern.
- Verwendung einer Notstromversorgung (USV).
- Monitoring der kritischen Netzwerk- und Serverkomponenten.
- Gewährleistung einer Verfügbarkeit entsprechend vertraglich vereinbarten SLA.

b) Rasche Wiederherstellbarkeit

Vorhandensein und Umsetzung eines Konzeptes zur Wiederherstellung von Daten und IT-Systemen auf Basis von regelmäßigen Datensicherungen und darauf aufbauendes Monitoring und Restore Tests (Backup-Konzept).

§ 4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Datenschutz-Management

- Bestehende Datenschutzorganisation, Sicherheitsorganisation und ISMS.
- Bestellter Datenschutzbeauftragter.
- Im Sinne eines KVP (Kontinuierlichen Verbesserungsprozesses) werden alle technischen und organisatorischen Maßnahmen regelmäßig auf ihre Wirksamkeit und den aktuellen Stand der Technik hin überprüft und angepasst.

b) Incident-Response-Management

Definierter Incident-Response Prozesse zur Entgegennahme von Datenschutz- und Sicherheitsvorfällen, deren Bewertung, Behandlung und Dokumentation.

c) Datenschutzfreundliche Voreinstellungen

- Die Art der Verarbeitung und der Zweck der Verarbeitung personenbezogener Daten erfolgt ausschließlich gemäß den Vorgaben des Auftraggebers und/oder entsprechend den vertraglichen Vereinbarungen.
- Mandantentrennung.

- Rollen- und Berechtigungskonzept.
- Löschung der personenbezogenen Daten entsprechend den vertraglichen Vereinbarungen.
- Es werden lediglich solche personenbezogenen Daten verarbeitet, die notwendig sind, um den vereinbarten Vertragszweck zu erfüllen.

d) Auftragskontrolle

- Dokumentation der sorgfältigen Auswahl und Kontrolle von Auftragnehmern.
- Formale Auftragserteilung.
- Abschluss von Zusatzvereinbarungen zur Auftragsverarbeitung gemäß Art. 28 DSGVO.
- Verpflichtung der Mitarbeiter (auch von Dienstleistern mit potenziellem Zugriff auf personenbezogene Daten) auf die Vertraulichkeit personenbezogener Daten gemäß DSGVO und ggf. § 3 TDDDG.
- Verarbeitung, Nutzung und Löschung von Daten findet nur entsprechend den vertraglichen Regelungen zwischen Auftraggeber und Auftragnehmer statt.