more security. usd

Allgemeine Nutzungsbedingungen für die PCI Plattform der usd AG

Stand: 24.11.2026

Allgemeine Nutzungsbedingungen für die PCI Plattform der usd AG (Stand: 24.11.2026)

Teil A Allgemeiner Teil

Teil B Auftragsverarbeitungsvertrag (AVV)

Teil C Technische und organisatorische Maßnahmen (TOM)

Teil A: Allgemeiner Teil

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

§ 1 Vertragsgegenstand; Geltungsbereich

(1) Die usd (Anbieterdaten siehe Impressum: https://www.usd.de/impressum) ist Anbieter der usd PCI Plattform (https://my-pci.usd.de) (nachfolgend Plattform genannt).

(2) Innerhalb der Plattform bietet usd abrufbare, digitale Angebote.

(3) Den Zugang und die Nutzung der Plattform bietet usd Unternehmen (nachfolgend Auftraggeber genannt) und deren verantwortlich agierenden, internen wie externen Mitarbeitern sowie ggf. dritten Partnern (nachfolgend Nutzer genannt) an.

(4) Diese Allgemeinen Nutzungsbedingungen (nachfolgend ANB genannt) gelten für alle Auftraggeber und Nutzer der Plattform mit dem ersten Zugriff auf die auf der Plattform bereitgehaltenen öffentlichen und nichtöffentlichen Inhalte und Internetdienste.

(5) Gegenbestätigungen der Auftraggeber und Nutzer unter Hinweis auf ihre eigenen Geschäfts- und/oder Einkaufsbedingungen wird hiermit widersprochen. Individuelle Vereinbarungen bleiben hiervon unberührt.

(6) Die Auftraggeber und Nutzer sind berechtigt, die auf der Plattform bereitgestellten Dienste und Informationen nach den folgenden Bestimmungen zu nutzen.

(7) Dieser allgemeine Teil A der ANB wird durch den Auftragsdatenverarbeitungsvertrag (Teil B) sowie die technischen und organisatorischen Maßnahmen gemäß DSGVO (Teil C) in ihrer jeweils aktuellen Fassung ergänzt.

§ 2 Leistungen; Preise

(1) Die Plattform ermöglicht Auftraggebern und Nutzern nach einer Registrierung und nach Zulassung durch den Anbieter gemäß §3 Informationen aus den geschlossenen Bereichen der Plattform abzurufen, Informationen, Nachrichten, Kommentare und Dokumente auszutauschen und Services zu bestellen.

(2) Die auf der Plattform angebotenen Leistungen bestehen unter anderem aus Sicherheitsüberprüfungen und ergänzende Dienstleistungen gemäß PCI DSS:

- Der Anbieter erbringt seine Leistungen unabhängig davon, ob Auftraggeber gemäß PCI DSS verpflichtet sind, eine PCI DSS-Zertifizierung zu erreichen.

- Mit seiner Zulassung gemäß §3 kann der Auftraggeber einzelne Services auf der Plattform gemäß Produktbeschreibung bestellen und deren Durchführung abhängig von den zur Verfügung stehenden Kapazitäten und zeitlichen Einschränkungen des Anbieters terminieren.

- Sofern der Auftraggeber eine Zertifizierung nach PCI DSS anstrebt, richtet sich Art, Umfang und Häufigkeit der durchzuführenden Zertifizierungsmaßnahmen nach seiner Klassifizierung und Einstufung.

- Mit bzw. nach seiner Registrierung legt der Auftraggeber alle zur Klassifizierung und Einstufung nach PCI DSS erforderlichen Daten auf der Plattform fest oder übermittelt diese an den Anbieter zur zweckgebundenen Verarbeitung und Nutzung.

- Die über den Zugriff auf die Plattform zur Verfügung gestellten Applikationen und angebotenen Services bestehen unter anderem aus:

  - PCI DSS konforme IT-Sicherheitsüberprüfungen (nachfolgend ASV Scans genannt) der über das Internet erreichbaren Infrastruktur des Kunden, inklusive Berichterstellung
  - Online Self-Assessment Questionnaires
  - Bereitstellung von Berichten, Zertifikaten und Siegeln
  - Unterstützungsleistungen des PCI Competence Centers der usd
  - Beratungs-, Dienst- und Unterstützungsleistungen für Kunden entsprechend gesonderter Vereinbarung mit dem Anbieter

- Im Rahmen der angebotenen ASV Scans überprüfen Auftraggeber ihre über das Internet erreichbare IT-Infrastruktur auf die durch den PCI DSS vorgegebenen Anforderungen. Auftraggeber nutzen dazu die auf der Plattform zur Verfügung gestellten Applikationen und die von dem Anbieter angebotenen, ergänzenden Dienstleistungen.

- Ergebnisse und Schlussfolgerungen der ASV Scans und der ergänzenden Dienstleistungen werden dem Auftraggeber mittels eines von der Plattform herunterladbaren Berichtes (Report) zur Verfügung gestellt.

- Sofern der Auftraggeber nachweislich den Anforderungen des PCI DSS gemäß seiner Angaben auf der Plattform entspricht, stellt der Anbieter ein PCI DSS-Zertifikat sowie ein Siegel bereit. Das PCI DSS-Zertifikat und das Siegel dürfen ausschließlich über die jeweils ausgewiesene Gültigkeitsdauer der Validierung von dem Auftraggeber verwendet werden.

(3) Soweit die digitalen Angebote nicht kostenfrei durch den Anbieter erbracht werden, sind die Preise für die einzelnen Leistungen den aktuellen Preisangaben auf der Plattform oder durch Kontaktaufnahme mit dem Vertrieb der usd AG zu entnehmen. Für die Preisbestimmung der einzelnen Leistung ist die zum Zeitpunkt des Vertragsabschlusses mit dem Anbieter (Bestellung) jeweils aktuelle Preisangabe maßgeblich.

(4) 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.

(5) 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.

§ 3 Nutzungsvoraussetzungen; Registrierung; Zulassung

(1) Voraussetzung für die Nutzung der Plattform und Inanspruchnahme der angebotenen Services ist der Abschluss eines Nutzungsvertrages. Das Nutzungsverhältnis umfasst den Zugang des Nutzers zur Plattform sowie die Nutzung der darauf angebotenen kostenfreien und ggf. zusätzlich gebuchten kostenpflichtigen Leistungen. Der Nutzer kann die Plattform ausschließlich mit kostenfreien Leistungen oder zusätzlich mit kostenpflichtigen Leistungen nutzen.

(2) Der Auftraggeber nimmt hierzu ein Vertragsangebot des Anbieters durch einen vertretungsberechtigten Nutzer an, in dem er die von ihm mit den Mindestangaben versehene Registrierung online an den Anbieter sendet und die Geltung dieser ANB durch Mausklick anerkennt. Zur Registrierung als Auftraggeber sind ausschließlich steuerpflichtige Unternehmer/ Unternehmen, Verbände, Vereine, öffentlich-rechtliche Körperschaften, Anstalten und Stiftungen sowie deren nachgelagerten Behörden und Organisationseinheiten berechtigt, sofern sie bei der Inanspruchnahme der auf der Plattform angebotenen Internetdienste in Ausübung ihrer gewerblichen oder selbständigen beruflichen oder dienstlichen Tätigkeit handeln. Zur Registrierung als Nutzer sind interne und externe Mitarbeiter von Auftraggebern berechtigt, die die digitalen Angebote der Plattform im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken in Anspruch nehmen.

In Einzelfällen kann für die Nutzung der Plattform ein Vertrag mit dem Anbieter schriftlich oder in Textform abgeschlossen werden. Der Auftraggeber beauftragt die Nutzung der Plattform in diesem Fall schriftlich oder in Textform und bestätigt die Geltung dieser ANB mit seiner Unterschrift.

(3) Die Registrierung ermöglicht den verantwortlich agierenden Nutzern des Auftraggebers Zugriff auf exklusive Leistungen und Inhalte im geschlossenen Bereich der Plattform zu

nehmen. Der Zugriff auf diese Inhalte ist von einer jeweiligen Anerkennung der ANB durch den Auftraggeber und Nutzer und einer jeweiligen Zulassung durch den Anbieter abhängig. In allen Fällen bleibt die Überprüfung der vom Auftraggeber angegebenen Unternehmensdaten auf Plausibilität vorbehalten.

(4) Ein Anspruch auf Nutzung der Plattform und auf Zulassung der Nutzungsmöglichkeit besteht nicht. Die Nutzungsmöglichkeit und/oder die Zulassung zur Plattform entfallen bei Fortfall der dafür vorgesehenen Voraussetzungen. Der Anbieter kann im Rahmen ordnungsgemäßer Erwägungen die Nutzungsmöglichkeit jederzeit und ohne Angabe von Gründen einschränken oder ausschließen.

§ 4 Rechte und Pflichten der Auftraggeber und Nutzer

(1) Auftraggeber und Nutzer sind berechtigt, die Leistungen der Plattform im Rahmen der ihnen vom Anbieter eingeräumten Zugriffsmöglichkeiten ordnungsgemäß und eigenverantwortlich zu nutzen. Sie sind verpflichtet, sämtliche Sicherheitsbestimmungen des Anbieters zu beachten sowie rechtswidrige Handlungen und Missbrauch der Zugriffsmöglichkeiten auf die auf der Plattform bereitgehaltenen Internetdienste zu unterlassen.

(2) Auftraggeber und Nutzer sind verpflichtet, ihre Unternehmensdaten bzw. Nutzerstammdaten fortlaufend auf ihre sachliche Richtigkeit hin zu überprüfen bzw. zu aktualisieren. Eingestellte Informationen, Content, Neuigkeiten und Nachrichten sowie Dateien dürfen keine Inhalte aufweisen, die [bzw. deren intendierter Vertrag] gegen gesetzliche oder behördliche Vorschriften und/oder gegen Rechte Dritter und/oder die guten Sitten verstoßen.

(3) Auftraggeber und Nutzer sind gegenüber dem Anbieter berechtigt – und vor Einleitung eines gerichtlichen Verfahrens gegen den Anbieter gehalten – die Sperrung oder Entfernung von eingestellten Informationen, Content, Neuigkeiten und Nachrichten sowie Dateien zu verlangen, deren sachliche Richtigkeit zweifelhaft ist, gegen gesetzliche oder behördliche Vorschriften oder gegen die guten Sitten verstößt sowie den Auftraggeber oder deren Nutzer oder Dritte in den Rechten verletzt (Notice-and-take-down-Verfahren).

(4) Wird der Anbieter aufgrund eines der unter Ziffern §4(1) bis §4(2) genannten Verstöße von Dritten oder einem Auftraggeber oder Nutzer in Anspruch genommen, verpflichtet sich der für den Verstoß verantwortliche Auftraggeber und Nutzer, den Anbieter von jeglichen Ansprüchen freizustellen. Die Freistellungspflicht bezieht sich auf alle Aufwendungen, die dem Anbieter aus der Inanspruchnahme durch einen Dritten notwendigerweise erwachsen. Die Geltendmachung eines darüberhinausgehenden Schadensersatzes behält sich der Anbieter ausdrücklich vor.

(5) Der Auftraggeber hält seine auf der Plattform agierenden Nutzer – unabhängig davon, ob mit den Nutzern ein eigenständiger Nutzungsvertrag zustande kommt – zur entsprechenden Einhaltung seiner Verpflichtungen aus diesen ANB an.

(6) Für die Nutzung der Plattform gelten die nachfolgenden Sonderregelungen:

(6.1) Im Rahmen seiner Registrierung und bei der Eingabe bzw. Übermittlung zertifizierungsrelevanter Informationen ist der Auftraggeber verpflichtet, wahrheitsgemäße Angaben zu machen und diese fortlaufend auf ihre sachliche Richtigkeit hin zu überprüfen bzw. zu aktualisieren.

(6.2) Der Auftraggeber ist verpflichtet, lediglich IT-Systeme zu scannen, soweit er hierzu berechtigt ist. Die Berechtigung besteht in der Regel, wenn der Auftraggeber Inhaber der Scankomponenten (IP-Adressen bzw. Domains) sowie entweder Eigentümer der zu den Scankomponenten zugehörigen IT-Systemen ist oder die schriftliche Erlaubnis vom Eigentümer der IT-Systeme zur Durchführung der ASV Scans eingeholt hat.

(6.3) Sofern der Auftraggeber eine Zertifizierung nach PCI DSS anstrebt, ist er verpflichtet, alle Scankomponenten (IP-Adressen bzw. Domains) anzugeben, die im Rahmen der PCI DSS Compliance mit einem ASV Scan geprüft werden müssen. Dies sind zum Beispiel Webserver, Applikationsserver, Router, Firewalls und Load Balancer.

(6.4) Der Auftraggeber ist verpflichtet, für den Zeitraum des ASV Scans seine Intrusion Detection Systems bzw. Intrusion Prevention Systeme (nachfolgend IDS/IPS genannt) so zu konfigurieren, dass die den ASV Scan ausführenden IT-Systeme des Anbieters uneingeschränkten Zugriff auf die zu scannenden Komponenten des Auftraggebers erhalten.

(6.5) Wird der Anbieter aufgrund eines der unter §4 Ziffer (6.1), (6.2), (6.3) und (6.4) genannten Verstoßes von Dritten oder einem Kunden in Anspruch genommen, verpflichtet sich der für den Verstoß verantwortliche Auftraggeber, den Anbieter von jeglichen Ansprüchen freizustellen. Die Freistellungspflicht bezieht sich auf alle Aufwendungen, die dem Anbieter aus der Inanspruchnahme durch einen Dritten notwendigerweise erwachsen. Die Geltendmachung eines darüberhinausgehenden Schadensersatzes behält sich der Anbieter ausdrücklich vor.

(7) Das PCI Security Standards Council (PCI SSC) gibt dem Auftraggeber die Möglichkeit, zentral Rückmeldung über die durchgeführten ASV Scans des Auftragnehmers zu geben. Unter dem folgenden Link steht dem Auftraggeber der Feedbackbogen des PCI SSC zur Verfügung:

https://listings.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors_feedback

§ 5 Rechte und Pflichten des Anbieters

(1) Der Anbieter verpflichtet sich, eigene redaktionelle Beiträge und sonstige Leistungen bestmöglich auf Aktualität, sachliche Korrektheit, Vollständigkeit und Sicherheit zu überprüfen.

(2) Bei Veranlassung und nach Ermessen prüft der Anbieter, ob Auftraggeber und deren Nutzer die allgemeinen Gesetze und das Vertrags- und Regelwerk bei der Inanspruchnahme der auf der Plattform angebotenen Leistungen beachten. Der Anbieter geht plausiblen Beschwerden von Auftraggebern und Nutzern über Regelverstöße und Mitteilungen über etwaig rechtswidrige Inhalte auf der Plattform nach und entscheidet, welche Maßnahmen im Fall von Regelverstößen zu treffen sind.

(3) Der Anbieter behält sich vor, eingestellte Informationen, Inhalte, Neuigkeiten und Nachrichten sowie Dateien, deren sachliche Richtigkeit zweifelhaft sind, die gegen gesetzliche oder behördliche Vorschriften, gegen die Rechte Dritter, gegen die guten Sitten verstoßen oder von Viren befallen sind, nach Kenntniserlangung und je nach Schwere der im Raum stehenden Verletzung auch ohne vorherige Anhörung und Ankündigung zu sperren oder zu entfernen (Notice-and-take-down-Verfahren). Ansprüche, die aufgrund der Entfernung solcher Informationen oder Dateien hergeleitet werden, können nicht gegen den Anbieter geltend gemacht werden.

(4) Verstößt der Auftraggeber bzw. deren Nutzer gegen eine Pflicht gemäß §4 und §5 ist der Anbieter berechtigt, die entsprechenden Daten zu löschen bzw. die Zugriffsmöglichkeit auf die Plattform ganz oder teilweise zu entziehen. Gleiches gilt sowohl bei sonstigen schwerwiegenden Vertragsverletzungen des Auftraggebers oder Nutzers als auch aufgrund begründeter Beschwerden von Auftraggebern und deren Nutzer nach dem Notice-and-take-down-Verfahren.

(5) Die inhaltliche und technische Ausgestaltung, insbesondere Form und Inhalt der Plattform liegen ausschließlich im Ermessen des Anbieters. Der Anbieter behält sich insoweit das Recht vor, alle kostenfrei angebotenen Leistungen jederzeit einzustellen, einzuschränken, zu erweitern, zu ergänzen oder zu verbessern.

(6) Der Anbieter ist berechtigt, alle Angaben des Auftraggebers auf ihre sachliche und tatsächliche Richtigkeit hin zu überprüfen und hierfür ggf. gesonderte schriftliche Zusicherungen vom Auftraggeber sowie Auskünfte von Dritten einzuholen.

Für den Fall von ernsthaften Zweifeln an der Richtigkeit der vom Auftraggeber gemachten Angaben ist der Anbieter berechtigt, die Zugriffsmöglichkeit auf die Plattform ganz oder teilweise zu entziehen und den Vertrag außerordentlich zu kündigen. Gleiches gilt bei Verstößen des Auftraggebers gegen seine Pflichten gemäß §4 Ziffer (6.1), (6.2), (6.3) und (6.4) und bei sonstigen schwerwiegenden Vertrags-

verletzungen des Kunden. Das Recht des Anbieters zur Geltendmachung von Schadensersatz bleibt hiervon unberührt.

(7) Im Rahmen des ASV-Zertifizierungsverfahrens obliegt die Beurteilung, ob der Ist-Zustand des zu überprüfenden IT-Systems dem geforderten Soll-Zustand entspricht, allein dem Anbieter. Ein Anspruch des Auftraggebers auf Erteilung des Zertifikats besteht im Falle einer negativen Abweichung des Ist- vom Soll-Zustand nicht.

(8) Der Anbieter vergibt die Zeiten, zu denen ASV Scans durchgeführt werden, nach der zeitlichen Reihenfolge des Eingangs der vom Auftraggeber vorgenommenen Terminierungen unter Berücksichtigung der zur Verfügung stehenden Kapazitäten des Anbieters.

Der Auftraggeber hat keinen Anspruch auf Durchführung von Zertifizierungsmaßnahmen zu einem bestimmten Zeitpunkt, sofern der Anbieter zu diesem Zeitpunkt keine freien Kapazitäten zur Verfügung hat.

§ 6 Systemausfall: Verfügbarkeit der Leistungen und Rückerstattung der Gegenleistung

(1) Die Plattform und die über diese Plattform angebotenen Leistungen werden ohne jegliche Zusicherung in Bezug auf Verfügbarkeit bereitgestellt.

(2) Die Verfügbarkeit berechnet sich auf der Grundlage der in der Vertragslaufzeit auf den jeweiligen Kalendermonat entfallenden Zeit abzüglich der planmäßigen Wartungs- und Ausfallzeiten, die nicht im Einflussbereich des Anbieters (höhere Gewalt, Verschulden Dritter etc.) liegen.

(3) Die planmäßigen Wartungsarbeiten finden bevorzugt außerhalb der Kernarbeitszeiten (Montag bis Freitag 08:00 Uhr bis 18:00 Uhr MEZ) statt.

(4) Während der Wartungsarbeiten kann es vorkommen, dass die vorgenannten Leistungen kurzfristig nicht zur Verfügung stehen. Entsprechende Leistungen werden von dem Anbieter in Abstimmung mit dem Auftraggeber und den Nutzern zum nächstmöglichen Zeitpunkt nachgeholt, sofern dies für den Auftraggeber zumutbar ist.

(5) Der Anbieter betreibt die Plattform über eine Internetanbindung mit mindestens 2 MBit/s Datenrate. Die Antwortzeit zum Aufruf einer einzelnen Webseite liegt im Mittel unterhalb von 2 Sekunden. Der Anbieter protokolliert die Auslastung der Anbindung und die Antwortzeiten.

(6) Der Zugang zu der Plattform erfolgt ausschließlich authentisiert, das heißt nach Eingabe von User ID und Passwort. Die Nutzung der angebotenen Funktionalität setzt auf Seiten der Nutzer Arbeitsplatzrechner voraus, die den stets aktuellen Anforderungen an Internetbrowser und zusätzlicher Add-Ons entsprechen.

§ 7 Vertragslaufzeit; Kündigung, Aufbewahrungs- und Löschfristen

(1) Das Nutzungsverhältnis (kostenfreie Registrierung und Nutzung kostenloser Leistungen) ist unbefristet. Der Auftraggeber kann das Nutzungsverhältnis jederzeit in Textform kündigen. Besteht zum Zeitpunkt der Kündigung ein laufender Vertrag über kostenpflichtige Leistungen, wird die Kündigung zum Ende der Vertragslaufzeit der letzten dieser Leistungen wirksam; bestehen keine kostenpflichtigen Leistungen, wird die Kündigung sofort wirksam.

(2) Das Recht des Anbieters, die Zugriffsmöglichkeiten des Auftraggebers auf die Plattform ganz oder teilweise gem. Ziffer 5.4 zu entziehen, bleibt unberührt.

(3) Kostenpflichtige Kontingente für ASV-Scans haben eine befristete Vertragslaufzeit; Einmal-Scans sind ab dem Tag der Bereitstellung 60 Tage sowie Jahres-Pakete ab dem Tag der Bereitstellung 15 Monate verfügbar. Nach Ablauf der Vertragslaufzeit verfallen nicht genutzte, bereitgestellte Kontingente. Abweichende Regelungen können in gesonderten Einzelvereinbarungen abgeschlossen werden. Eine Kündigung verkürzt nicht die Vertragslaufzeit bereits gebuchter, kostenpflichtiger Leistungen; sie wird erst nach deren Ablauf wirksam. Eine Erstattung für ungenutzte Kontingente erfolgt nicht.

(4) Kündigungen sind in Textform (E-Mail) an pci@usd.de oder an kontakt@usd.de zu richten (ergänzende Kontaktkanäle gemäß Impressum bleiben unberührt).

(5) Der Anbieter ist berechtigt, das Nutzungsverhältnis jederzeit ordentlich mit einer Frist von einem Monat zu kündigen, sofern keine kostenpflichtigen Leistungen mit laufender Vertragslaufzeit mehr bestehen. Der Anbieter wird dem Auftraggeber auf Wunsch den Kündigungsgrund in Textform mitteilen. Rechte und Pflichten aus bereits gebuchten, kostenpflichtigen Leistungen bleiben bis zu deren Vertragsende unberührt.

(6) Jede Partei ist zur außerordentlichen Kündigung aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt für den Anbieter insbesondere vor bei schwerwiegenden Verstößen gegen diese ANB, deliktischen Handlungen oder der Eröffnung des Insolvenzverfahrens über das Vermögen des Auftraggebers bzw. der Abweisung des entsprechenden Eröffnungsantrags mangels Masse.

(7) Der Anbieter ist berechtigt, das Nutzungsverhältnis jederzeit ordentlich zu kündigen, wenn für ein Nutzerkonto für einen zusammenhängenden Zeitraum von sechs (6) Monaten weder ein Login des Nutzers erfolgt noch Leistungen der Plattform (kostenfrei oder kostenpflichtig) genutzt werden und keine kostenpflichtigen Leistungen mit laufender Vertragslaufzeit mehr bestehen. Die Kündigung wird dem Auftraggeber mindestens einen Monat vorab in Textform angekündigt. Rechte und Pflichten aus bereits gebuchten, kostenpflichtigen Leistungen bleiben bis zu deren Vertragsende unberührt.

(8) Mit Wirksamwerden der Kündigung endet das Nutzungsverhältnis. Sämtliche Leistungen (kostenfrei und kostenpflichtig) werden beendet. Das zugehörige Nutzerkonto wird geschlossen und deaktiviert; für die zu dem Konto gehörenden Datensätze beginnen die jeweiligen Aufbewahrungsfristen.

(9) Für Datensätze mit offiziellen PCI-Dokumenten gilt eine Aufbewahrungsfrist von drei (3) Jahren; für sonstige Datensätze gilt eine Aufbewahrungsfrist von einem (1) Jahr. Kopien in Sicherungs- oder Archivsystemen können aus technischen Gründen kurzfristig länger bestehen bleiben; die Löschung erfolgt nach den einschlägigen technischen und organisatorischen Maßnahmen des Anbieters.

(10) Nach Ablauf der Aufbewahrungsfristen werden Nutzerkonten und die damit verbundenen personenbezogenen Daten endgültig gelöscht.

(11) Unberührt bleiben gesetzliche, behördliche oder vertragliche Aufbewahrungspflichten sowie berechtigte Interessen des Anbieters an der Aufbewahrung (z. B. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen). Die Rechte betroffener Personen (z. B. Auskunft, Löschung, Widerspruch) nach Art. 12 ff. DSGVO bleiben unberührt; sie werden in der Datenschutzerklärung des Anbieters konkretisiert.

§ 8 Haftung; Haftungsausschlüsse; Haftungsbegrenzung

(1) Der Anbieter haftet für Schäden, die der Auftraggeber erleidet, nur, soweit diese durch vorsätzliche oder grob fahrlässige Handlungen oder durch die Verletzung wesentlicher Vertragspflichten verursacht worden sind. Im Falle der einfachen fahrlässigen Verletzung wesentlicher Vertragspflichten haftet der Anbieter nur in Höhe des vorhersehbaren, vertragstypischen, unmittelbaren Durchschnittsschadens. In der Summe ist die Haftung auf höchstens 25.000,00 Euro (i.W.: fünfundzwanzigtausend Euro) je Haftungsfall begrenzt. Im Übrigen ist die Haftung ausgeschlossen. Wesentliche Vertragspflichten sind solche, deren Erfüllung zur Erreichung des Ziels des Vertrags notwendig sind.

(2) Soweit die Plattform mit Links den Zugang zu anderen Websites ermöglicht, ist der Anbieter für die dort enthaltenen fremden Inhalte nicht verantwortlich. Der Anbieter macht sich die fremden Inhalte nicht zu Eigen. Die Haftung für fremde Inhalte ist ausgeschlossen. Sofern der Anbieter Kenntnis von rechtswidrigen Inhalten auf externe Websites erhält, wird der Anbieter den Link zu diesen unverzüglich beseitigen.

(3) Der Anbieter haftet nicht für die sachliche Richtigkeit von Daten sowie für die Virenfreiheit von Dateien, die auf der Plattform durch Auftraggeber und deren Nutzer eingestellt werden. Auf die Möglichkeit der Einleitung eines Notice-and-take-down-Verfahrens (Ziffern 4.3, 5.4) wird hingewiesen.

(4) Der Anbieter haftet nicht für Schäden des Auftraggebers und deren Nutzer, die aufgrund der Befolgung oder der Nichtbefolgung von Empfehlungen, Tipps, Best-Practices oder der Verwendung von Templates entstehen.

(5) Die vorstehenden Regelungen gelten auch zu Gunsten der Mitarbeiter und sonstiger Erfüllungsgehilfen des Anbieters.

(6) Die vorstehenden Haftungsbeschränkungen und Ausschlüsse betreffen nicht Ansprüche der Auftraggeber und deren Nutzer aufgrund einer Verletzung des Lebens, des Körpers, der Gesundheit und Ansprüche aufgrund der fahrlässigen Verletzung wesentlicher Vertragspflichten. Von dem Haftungsausschluss ebenfalls ausgenommen ist die Haftung aus Produkthaftung und für Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Anbieters, seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

(7) Sofern der Anbieter Leistungen bei Auftraggebern außerhalb dieser ANB oder aufgrund eines individuellen Angebotes erbringt, ist die diesbezügliche Haftung der Vertragspartner in dem hierzu gesondert geschlossenen Vertrag/Angebot geregelt.

(8) Der Anbieter gewährleistet und stellt sicher, dass der als Applikation zur Verfügung gestellte Security Scanner dem von den Kreditkartenorganisationen vorgegebenen Payment Card Industry Data Security Standard entspricht. Dies ist notwendig, um das analysierte und dem Standard entsprechende IT-System zu zertifizieren, und stellt zugleich sicher, dass das Scannen lediglich minimalen Einfluss auf das analysierte IT-System hat. Eine weitergehende Verpflichtung oder Haftung des Anbieters besteht nicht. Der Anbieter haftet nicht für Schäden aufgrund von Beeinträchtigungen der Integrität und/oder Verfügbarkeit der analysierten IT-Systeme bei ordnungsgemäßen, dem Payment Card Industry Data Security Standard entsprechenden ASV Scans.

(9) Die vorstehenden Haftungsbeschränkungen und Ausschlüsse betreffen nicht Ansprüche der Auftraggeber aus Produkthaftung. Weiter gelten die Haftungsbeschränkungen nicht für den Anbieter zurechenbare Körper- und Gesundheitsschäden von Auftraggebern.

§ 9 Datenschutz

(1) Der Anbieter hat umfassende technische wie auch organisatorische Vorkehrungen getroffen, um die vertrauliche und ausschließlich zweckbestimmte Behandlung von Daten sicherzustellen. Der Missbrauch durch rechtswidrige Handlungen Dritter kann jedoch nicht gänzlich ausgeschlossen werden.

(2) Der Anbieter verpflichtet sich, die bei der Registrierung und bei der Nutzung gespeicherten Daten lediglich zu eigenen Zwecken und zu Zwecken der Projektarbeit sowie zu Zwecken der Anbahnung oder der Abwicklung von über die Plattform

angebahnten oder abgeschlossenen Verträgen zu nutzen und nicht an außenstehende Dritte weiterzugeben, sofern hierzu keine behördlich angeordnete Verpflichtung besteht oder der Auftraggeber nicht ausdrücklich seine Einwilligung gegeben hat. Diese Regelung über den Umgang mit Daten wird durch den Datenschutzhinweis konkretisiert und ergänzt.

(3) Der Anbieter verpflichtet sich, seine Nutzer, die mit der Administration und/oder dem Betrieb der Plattform betraut sind, auf die strenge Einhaltung datenschutzrechtlicher Vorschriften zu verpflichten.

(4) Der Anbieter ist bei der Registrierung von Unternehmen als Auftraggeber berechtigt, zum Zweck der eigenen Kreditprüfung ggf. Bonitätsinformationen auf der Basis mathematisch-statistischer Verfahren von sog. Auskunfteien abzurufen und aktualisierte Auskünfte zu erhalten.

(5) Der Anbieter ist zur Gewährleistung eines ordnungsgemäßen und performanten Plattformbetriebes und zur zielgerichteten Verbesserung seiner Angebote (zielgruppengerechtes Marketing) sowie zur Bekämpfung von Missbrauch berechtigt, das Benutzungsverhalten von Auftraggebern und Nutzern zu beobachten, aufzuzeichnen und auszuwerten. Ziffer (2) gilt für solche Daten entsprechend.

(6) Soweit der Auftraggeber personenbezogene Daten eines Dritten auf der Plattform einstellt, sichert er zu, dass er hierzu berechtigt ist. Der Auftraggeber ist verpflichtet, den Dritten von der Übermittlung seiner personenbezogenen Daten in Kenntnis zu setzen.

(7) Auftraggeber und Nutzer sind ausschließlich zum Zwecke der Anbahnung und zur Abwicklung von Verträgen sowie zur Projektarbeit berechtigt, die ihnen vom Anbieter oder von anderen Auftraggebern übermittelten, personenbezogenen Daten zu verwenden. Der Auftraggeber verpflichtet seine auf der Plattform agierenden Nutzer entsprechend seinen Verpflichtungen aus diesen ANB.

§ 10 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:

1. Leistungsort außerhalb von Deutschland aber innerhalb der EU:

Angabe der gültigen Umsatzsteuer-Identifikationsnummer (VAT-Nummer) der gemäß Absatz 2 an die usd kommunizierten Leistungsorte.

2. 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 Leistungsempfänger (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 Leistungserbringer ist zur Nachforderung dieser Steuern und Abgaben beim Leistungsempfänger auch über den Zeitpunkt des Abschlusses des Leistungsaustauschs berechtigt.

§ 11 Urheber- und Schutzrechte

(1) Der Anbieter ist Inhaber sämtlicher Eigentums-, Schutz- und Urheberrechte bzgl. der eigenen Beiträge und sonstiger eigener Inhalte, sofern nicht gegenteilig gekennzeichnet.

(2) An Beiträgen und Inhalten, die von Auftraggebern auf der Plattform zum Zwecke des Abrufs durch den Anbieter oder andere Auftraggeber hochgeladen werden, verbleiben die Eigentums-, Schutz- und Urheberrechte bei dem hochladenden Auftraggeber. Soweit erforderlich, räumt der hochladende Auftraggeber dem Anbieter ein einfaches Nutzungsrecht zum jeweiligen Bestimmungszweck ein, ohne dass sich der Anbieter die fremden Inhalte hierdurch zu eigen macht.

(3) Der Auftraggeber verpflichtet sich, die auf der Plattform enthaltenen Urheberrechtsvermerke oder andere Hinweise des Anbieters oder anderer Auftraggeber auf derartige Rechte weder zu entfernen noch unkenntlich zu machen.

§ 12 Ergänzende Informationen im elektronischen Geschäftsverkehr gem. § 312 i BGB i.V.m. Artikel 246 c EGBGB

(1) Im Wesentlichen informieren die Regeln dieser ANB den Nutzer über sämtliche Pflichtinformationen im elektronischen Geschäftsverkehr gem. § 312 i BGB i.V.m. Artikel 246 c EGBGB, so dass es nur noch folgender Ergänzungen bedarf:

(2) Anbieteridentität:

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

Vertretungsberechtigung:
Vorstand: Andreas Duchmann, Matthias Göhring, Christopher Kristes, Felix Schmidt, Dr. Christian Schwartz, Andrea Tubach (Vorsitz)

Aufsichtsratsvorsitzender:
Manfred Tubach

Handelsregister:
Amtsgericht Offenbach am Main
HRB 34667

USt-ID:
DE163774242

Kontakt:
Telefon: +49 6102 8631-0
Telefax: +49 6102 8631-88
E-Mail: kontakt@usd.de

(3) Die wesentlichen Merkmale der angebotenen Leistungen sowie die Gültigkeitsdauer befristeter Angebote kann den einzelnen Produkt- und/oder Leistungsbeschreibungen auf der Plattform des Anbieters entnommen werden.

(4) Die für den Vertragsabschluss zur Verfügung stehende Sprache ist ausschließlich Deutsch und Englisch.

(5) Die verschiedenen Möglichkeiten des Vertragsschlusses sind in § 3 dieser ANB beschrieben.

(6) Etwaige Eingabefehler bei Abgabe seiner Bestellung kann der Nutzer bei der abschließenden Bestellabgabe erkennen und mit Hilfe der Lösch- und Änderungsfunktion vor Absendung der Bestellung jederzeit korrigieren.

(7) Die vom Anbieter angegebenen Preise verstehen sich als Netto-Endpreise zzgl. gesetzlich gültigen Steuern innerhalb der Bundesrepublik Deutschland.

(8) Etwaige Beschwerden kann der Auftraggeber/Nutzer jederzeit an den Anbieter per Brief, Fax oder E-Mail oder telefonisch während der Geschäftszeiten richten. Der Anbieter wird sich sonach in angemessener Zeit mit dem Auftraggeber/Nutzer in Verbindung setzen.

(9) Die Haftung und Gewährleistung richtet sich nach den entsprechenden Regelungen dieser ANB; im Übrigen nach den gesetzlichen Bestimmungen.

(10) Die für die Abwicklung des Vertrages zwischen dem Auftraggeber und dem Anbieter benötigten Daten werden von dem Anbieter gespeichert. Nach Verlassen der Bestellebene bleibt die Bestellung für den Auftraggeber/Nutzer im Internet abrufbar. Es gilt Ziffer A9 dieser ANB sowie die Regelungen unseres Datenschutzhinweises (https://www.usd.de/datenschutz/).

(11) Der Nutzer/Auftraggeber kann diese Informationen, die Allgemeinen Nutzungsbedingungen, den Datenschutzhinweis sowie sämtliche anderen Informationen dieser Internetseite wie folgt ausdrucken oder in wiedergabefähiger Form speichern: Die jeweilige Seite kann mit dem Browser ausgedruckt werden, indem im Hauptmenü des Browsers die Funktion "Drucken" gewählt wird. Die jeweilige Seite kann gespeichert werden, indem der Nutzer im Hauptmenü seines Browsers die Funktion "Speichern unter" wählt. Darüber hinaus werden sämtliche Vertragsbestimmungen von uns gespeichert. Die Vertragsbestimmungen senden wir Ihnen auch gerne auf Wunsch per E-Mail zu.

(12) Speziellen und vorstehend nicht erwähnten Verhaltenskodizes unterliegen wir nicht.

§ 13 Allgemeines

(1) Es gilt ausschließlich das Recht der Bundesrepublik Deutschland unter Ausschluss der Verweisungsnormen des internationalen Privatrechts (IPR) und des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG). Die usd Plattform berücksichtigen die rechtlichen Anforderungen der Bundesrepublik Deutschland. Der Anbieter übernimmt keine Verantwortung dafür, dass die usd Plattform, deren Services, Informationen und/oder Dokumentation auch an Orten außerhalb der Bundesrepublik Deutschland abgerufen oder heruntergeladen werden dürfen. Wenn Auftraggeber/Nutzer von Orten außerhalb der Bundesrepublik Deutschland auf die usd Plattform zugreifen, ist der Auftraggeber/Nutzer ausschließlich selbst für die Einhaltung der nach dem jeweiligen Landesrecht einschlägigen Vorschriften verantwortlich. Der Zugang zu den usd Plattform, deren Services, Informationen und/oder Dokumentation aus Ländern, in denen dieser Zugang etwaig rechtswidrig ist, ist nicht gestattet.

(2) Der ausschließliche Gerichtsstand ist Frankfurt am Main in der Bundesrepublik Deutschland, soweit der Auftraggeber Kaufmann oder ein rechtsfähiger Verband, Verein, eine öffentlich-rechtliche Körperschaft, Anstalt oder Stiftung ist. Der Anbieter ist daneben berechtigt, auch am allgemeinen Gerichtsstand des Auftraggebers oder Nutzers zu klagen.

(3) Der deutsche Vertragstext dieser ANB und ihrer Bestandteile besitzt im Zweifelsfall Vorrang gegenüber Übersetzungen in anderen Sprachen.

(4) Die Unwirksamkeit einer oder mehrerer Bestimmungen dieses Vertrages berührt nicht die Wirksamkeit dieses Vertrages im Übrigen.

(5) Die ergänzenden Bestandteile dieser ANB können sämtlich im öffentlichen Bereich der Plattform abgerufen werden.

(6) Diese ANB treten an die Stelle aller früheren AGB und/oder ANB und ersetzen diese. Weitere Änderungen dieser ANB werden dem Auftraggeber bzw. Nutzer vor der weiteren Inanspruchnahme der Dienste vom Anbieter auf elektronischem Wege (z.B. E-Mail, Pop-Up-Fenster, Interstitial, etc.) mitgeteilt. Widerspricht der Auftraggeber solchen Änderungen nicht innerhalb von 14 Tagen nach Zugang der Mitteilung, gelten die Änderungen als vereinbart, wenn der Auftraggeber die unter www.usd.de bereitgehaltenen Leistungen des Anbieters weiterhin in Anspruch nimmt. Auf das Widerspruchsrecht und die Rechtsfolgen des Schweigens wird der Auftraggeber im Falle der Änderung dieser ANB gesondert hingewiesen.

(7) Die ANB entsprechen dem oben genannten Stand. Wir werden Sie über zukünftige Änderungen informieren und Ihnen aktualisierte Versionen übermitteln. Dazu kontaktieren wir Sie über die in Ihrem Konto hinterlegte E-Mail-Adresse und nutzen ein

Mailingtool, mit dessen Betreiber wir hinsichtlich des Datenschutzes einen Vertrag zur Auftragsverarbeitung geschlossen haben. Ihre Daten werden nach der Mitteilung, spätestens nach vier Wochen, aus dem Mailingtool gelöscht.

Teil B: Auftragsverarbeitungsvertrag (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 zugehörigen 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 Auftragnehmers ist die potenzielle Verarbeitung personenbezogener Daten im Rahmen der Bereitstellung einer Scanning Plattform für Sicherheitsüberprüfungen und ergänzende Dienstleistungen gemäß PCI DSS oder der Bereitstellung einer Awareness Plattform zum Training und zur Sensibilisierung von Mitarbeitern.

(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 C].

(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 95008-40
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, 32 DSGVO [Einzelheiten in Teil C].

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 Telekommunikations-leistungen, 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 Auftragnehmer darf bestehende Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher Zustimmung des Auftraggebers beauftragen.

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) Für die Nutzung der Plattform gelten die nachfolgenden Sonderregelungen:

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

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Qualys Inc.	919 E Hillsdale Blvd, 4th Floor Foster City, CA 94404 USA	Qualys unterstützt bei der Erbringung von ASV Scans

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 Ausschuss-material. 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 C: 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 Anmelde-versuchen.
- 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 System-verwalters.
- 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.