Vertrag zur Auftragsverarbeitung zwischen

_____

_____

_____

– nachfolgend Auftraggeberin genannt –

und

snapADDY GmbH
Haugerkirchgasse 7, 97070 Würzburg
– nachfolgend Auftragnehmerin genannt –

§ 1 Gegenstand und Dauer des Auftrags

(1) Die Auftragnehmerin führt die im Anhang 1 beschriebenen Dienstleistungen für die Auftraggeberin durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange die Auftragnehmerin für die Auftraggeberin personenbezogene Daten verarbeitet.

§ 2 Weisungen der Auftraggeberin

(1) Die Auftraggeberin ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Die Auftragnehmerin verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen der Auftraggeberin und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn die Auftraggeberin dies anweist.

(3) Die Verarbeitung erfolgt nur auf Weisung der Auftraggeberin, es sei denn, die Auftragnehmerin ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt die Auftragnehmerin der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von der Auftraggeberin zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn die Auftragnehmerin dies verlangt.

(5) Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Vorschriften verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

(1) Die Auftragnehmerin verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und im Anhang 3 dieses Vertrages zu

dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Die Auftragnehmerin darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss die Auftragnehmerin der Auftraggeberin nur wesentliche Anpassungen mitteilen.

(3) Die Auftragnehmerin gewährleistet in ihrem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung. Die Auftragnehmerin hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten der Auftraggeberin mitzuwirken. Die Auftragnehmerin wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat der Auftraggeberin alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

§ 4 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Die Auftragnehmerin bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sie überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Die Auftragnehmerin darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten der Auftraggeberin zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt die Auftragnehmerin einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden der Auftraggeberin zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(6) Die Auftragnehmerin darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(7) Die Auftragnehmerin unterstützt die Auftraggeberin mit geeigneten technischen und organisatorischen Maßnahmen, damit diese ihre bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Die Auftragnehmerin benennt einen Ansprechpartner, der die Auftraggeberin bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt der Auftraggeberin dessen Kontaktdaten unverzüglich mit. Soweit die Auftraggeberin besonderen gesetzlichen

Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt die Auftragnehmerin die Auftraggeberin hierbei. Auskünfte an die betroffene Person oder Dritte darf die Auftragnehmerin nur nach vorheriger Weisung der Auftraggeberin erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber der Auftragnehmerin geltend macht, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Die Auftragnehmerin darf Unterauftragnehmer nur beauftragen, wenn sie die Auftraggeberin über eine beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter in Textform informiert, wodurch die Auftraggeberin die Möglichkeit erhält, gegen derartige Änderungen innerhalb einer Frist von 2 Wochen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen. Sofern dem Einspruch nicht abgeholfen werden kann, steht den Parteien ein Sonderkündigungsrecht nach den allgmeinen Regelungen des zugrundeliegenden Vertrags zu.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn die Auftragnehmerin weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn die Auftragnehmerin durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.

(4) Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

§ 6 Kontrollrechte der Auftraggeberin

Die Auftragnehmerin erklärt sich damit einverstanden, dass die Auftraggeberin oder eine von ihr beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder ggfls. durch Zutritt zu den Arbeitsräumen der Auftragnehmerin zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht der Auftragnehmerin zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

§ 7 Mitzuteilende Verstöße der Auftragnehmerin

Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten der Auftraggeberin mit sich bringen, sowie bei Verdacht auf

Datenschutzverletzungen im Zusammenhang mit den Daten der Auftraggeberin. Gleiches gilt, wenn die Auftragnehmerin feststellt, dass die bei ihr getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Der Auftragnehmerin ist bekannt, dass die Auftraggeberin verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird die Auftragnehmerin die Auftraggeberin bei der Einhaltung ihrer Meldepflichten unterstützen. Sie wird die Verletzungen der Auftraggeberin unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,
b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat die Auftragnehmerin alle personenbezogenen Daten zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Weitere personenbezogene Daten auf Backup-Systemen werden innerhalb von 3 Monaten gelöscht.

(2) Die Auftraggeberin kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn die Auftragnehmerin einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeberin aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Haftung

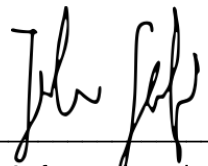
Die Haftung des Auftragnehmers für schuldhafte Verletzungen dieses Vertrags bestimmen sich nach den gesetzlichen Regelungen. Zudem stellt der Auftraggeber den Auftragnehmer von Schadensersatzansprüchen Betroffener frei, sofern die haftungsbegründende Pflichtverletzung nicht auf den Auftragnehmer zurückzuführen ist.

§ 10 Schlussbestimmungen

(1) Sollte das Eigentum der Auftraggeberin bei der Auftragnehmerin durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmerin die Auftraggeberin unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände der Auftraggeberin ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was ab dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.

(3) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

_____	_____ | Würzburg, 20.01.2020		
Ort, Datum	Auftraggeberin	Ort, Datum	Auftragnehmerin

Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Der Auftraggeber nutzt die Software snapADDY VisitReport zur schnellen Erfassung von Visitenkarten und Besuchsberichten auf Messen, Veranstaltungen und bei Kundenbesuchen oder -gesprächen.
Art und Zweck der Verarbeitung	Elektronische Erfassung von Daten mittels PC oder mobilen Geräten (z. B. von Visitenkarten oder anderen Quellen), Übertragung der Daten in CRM-Systeme oder andere weiterverarbeitende Systeme, Aktualisierung oder Validierung von bestehenden Daten in weiterverarbeitenden Systemen.
Art der personenbezogenen Daten	Namen, Vornamen, E-Mail-Adressen, Telefonnummern, Straße, Hausnummer, PLZ, Ort, Firma, Firmenanschrift (teils von Visitenkarten oder anderen öffentlich zugänglichen Quellen).
Kategorien betroffener Personen	Kunden, Lieferanten, Messebesucher, Geschäftspartner, Interessenten, Bewerber, Mitarbeiter des Auftraggebers und ähnliches

Name und Kontaktdaten des Datenschutz-beauftragten der Auftraggeberin (sofern benannt)	
Name und Kontaktdaten des Datenschutz-beauftragten der Auftragnehmerin (sofern benannt)	datenschutz süd GmbH Dr. iur. Christian Borchers, Volljurist Geschäftsführer Telefon: +49 (0) 931 304 976 0 office@datenschutz-sued.de Wörthstraße 15 DE-97082 Würzburg

Anhang 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Verarbeitungsstandort**	**Art der Dienstleistung**
Amazon Web Services Inc. 410 TerryAvenue North Seattle, WA 98109-5210 USA	AWS Region Frankfurt, Deutschland (eu-central-1)	Rechenzentrum zum Serverhosting
Google Ireland Limited Gordon House, Barrow Street Dublin 4 Irland	europe-west3-Region, Frankfurt	Cloud-Dienste wie z.B.Texterkennung (OCR)

Anhang 3: Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Im Zuge der Einholung dieser Auskünfte gibt der Auftragnehmer dem Auftraggeber nachfolgende Informationen zu den eingerichteten technischen und organisatorischen Maßnahmen:

Vertraulichkeit [Art. 32 Abs. 1 lit. b DSGVO]

a) Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu den Serversystemen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

Die Rechenzentren sind 24/7 personell besetzt. Der Zutritt zu den Sicherheitsbereichen wird durch ein elektronisches Zugangskontrollsystem mit Protokollierung geschützt.
Die Ausgabe von Schlüssel der Büroschließanlage für die Mitarbeiter wird zentral verwaltet, überwacht und dokumentiert. Die Zutrittsbereiche sind durch Videoüberwachung abgesichert. Besucher müssen sich am Empfang identifizieren und werden nur in Begleitung zu ihren Ansprechpartnern in den jeweiligen Bereichen geführt.

b) Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

Die Datenverarbeitungssysteme werden insbesondere durch Anti-Viren-Software, Firewall-Systeme (Software) und Proxy-Server geschützt. Die Verwaltung der Sicherheitssoftware wird regelmäßig sichergestellt und erfolgt nur durch autorisiertes Personal. Die Autorisierung des Personals wird durch zugeordnete Benutzerrechte bzw. Benutzerprofile sichergestellt. Über diese Profile kann eine Anmeldung an den jeweiligen IT-Systemen durch eine Zwei-Faktor-Authentifizierung erfolgen. Diese erfolgt mittels Benutzername und Passwort (mind. 8-stellig, 1 Klein-, 1 Großbuchstabe, 1 Zahl) sowie einem 6-stelligen Einmal-Code, der über eine App oder per SMS an das Smartphone des Benutzers gesandt wird.
Zugriffe auf Datenverarbeitungssysteme erfolgen über gesicherte Verbindungen (u.a. SSL-Zertifikate). Der elektronische Datenverkehr zwischen Auftraggeber und Auftragnehmer wird durch Verschlüsselungstechnologie abgesichert.

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen und personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

Die Rechtevergabe wird gemäß Berechtigungskonzept umgesetzt und die Verwaltung obliegt den Systemadministratoren. Das Konzept sowie die vergebenen Rechte werden jährlich einer Eigenprüfung unterzogen und das Vorgehen überwacht.

Grundsätzlich ist die Anzahl der Administratoren nur auf das „Notwendigste“ beschränkt. Um den Zugriff auf Daten nur autorisiertem Personal zu ermöglichen, werden Datenträger und Daten verschlüsselt und der Zugriff über die Nutzerrechte reguliert. Der Zugriff auf Systeme und Anwendungen erfolgt passwortgestützt mittels einer Zwei-Faktor-Authentifizierung und ist rechtegebunden - jeder Mitarbeiter kann im Rahmen seines Tätigkeitsbereiches nur auf die notwendigen Funktionen zum Verrichten seiner Tätigkeiten zugreifen. Der unrechtmäßige Zugriff auf Systeme oder auf die Datenintegrität über Sicherheitslücken in Programmen wird durch regelmäßiges Monitoring der Infrastruktur und umgehende Behebung gefundener Probleme verhindert. Sowohl externe als auch interne Zugriffe werden dadurch erkannt und deren Auswirkungen minimiert.
Kundendaten auf den Servern des Hosting-Dienstleisters werden AES256-verschlüsselt gespeichert und sind damit auch von diesem selbst nicht lesbar.

d) Pseudonymisierung

Die Pseudonymisierung (Art. 32 Abs. 1 lit. a, Art. 25 Abs. 1 DSGVO) gewährleistet, dass Identifikationsmerkmale personenbezogener Daten, sofern dies zum Schutz der betroffenen Personen erforderlich ist oder aus datenschutzrechtlicher Sicht geboten ist, bestimmter oder bestimmbarer Personen durch Kennzeichen ersetzt werden und daher die Zuordnung zur betroffenen Person nicht ohne zusätzliche Informationen möglich ist.
Folglich können Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen

betroffenen Person zugeordnet werden. Diese zusätzlichen Informationen müssen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Kundendaten auf den Servern des Hosting-Dienstleisters werden AES256-verschlüsselt gespeichert und sind damit auch von diesem selbst nicht lesbar.

Integrität [Art. 32 Abs. 1 lit. b DSGVO]

e) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Der elektronische Datenaustausch wird durch Sicherungssysteme überwacht, hierbei werden alle Daten SSL-verschlüsselt übertragen (TLS 1.2 (protocol), ECDHE_RSA with P-256 (key exchange), and AES_128_GCM (cipher)). Das unbefugte Entfernen von Datenträgern im Rechenzentrum wird durch Sicherheitsbereiche und Zugangskontrolle eingeschränkt. Für die jeweiligen Bereiche sind Richtlinien erlassen, die ein unberechtigtes Entfernen von Datenträgern verhindern. Ausrangierte Datenträger werden gemäß Vorgabe vernichtet.
Außerdem erfolgt eine Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf den Servern durch ein Berechtigungskonzept. Alle Mitarbeiter werden vertraglich auf das Datengeheimnis verpflichtet.

e) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

Durch die restriktive Vergabe von Rechten durch individuelle Benutzer wird die Eingabe, Änderung oder Entfernung von personenbezogenen Daten in Datenverarbeitungssystemen eingeschränkt. Es wird jede Eingabe, Änderung und Entfernung von Daten protokolliert.

Verfügbarkeit [Art. 32 Abs. 1 lit. b DSGVO]

g) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Um zufällige Zerstörung oder Verlust im Rahmen der auftragsbezogenen Verarbeitung von Daten einzuschränken, wurde ein Backup- & Recovery-Konzept erstellt, implementiert und die Wiederherstellung regelmäßig getestet. Die Datensicherungen werden an einem sicheren, ausgelagerten Ort verwahrt. Um auch bei Störungen im Stromnetz den regelmäßigen und sicheren Betrieb der Systeme zu gewährleisten, wird eine unterbrechungsfreie Stromversorgung (USV) eingesetzt. Der Serverraum wird durch unterschiedliche Überwachungs- und Meldesysteme abgesichert, wie insbesondere Geräte zur Überwachung von Temperatur und Feuchtigkeit sowie Feuer- und Rauchmeldeanlagen.

Kontrollmaßnahmen [Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO]

h) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Der Auftragnehmer verarbeitet die eingereichten Daten gemäß dem geschlossenen Vertrag und achtet dabei die gesetzlichen Vorschriften und per Vertrag definierten Anforderungen im Rahmen der Weisungen des Auftraggebers. Dadurch wird die Weitergabe der Daten an unbefugte Dritte vertraglich

ausgeschlossen und der Weisungsrahmen festgelegt. Bei der Festlegung werden vor allem auch die Pflichtinhalte des § 28 DSGVO berücksichtigt. Der Auftragnehmer ermöglicht dem Auftraggeber eine vorzeitige Prüfung der Dokumentationen der „technisch / organisatorischen Maßnahmen“ oder falls erforderlich, eine vor Ort Besichtigung der Datenverarbeitungsanlagen. Eine mögliche Überprüfung des Auftragnehmers sowie seiner, im Rahmen der Datenverarbeitung durchgeführten Tätigkeiten, wird durch den Auftragnehmer dadurch ermöglicht und unterstützt.

i) Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Das Trennungsgebot wird durch softwareseitige logische Mandanten-Trennung sichergestellt. Testumgebungen werden vom Produktivsystem unabhängig verwaltet – eine Überführung von Kundendaten in diese Testsysteme erfolgt nicht.

j) Datensicherheitsmanagement

Verfahren, die eine regelmäßige Überprüfung, Auswertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen gewährleisten:

Die beschriebenen Sicherheitsmaßnahmen werden regelmäßig überprüft, ausgewertet und evaluiert und dem technischen Standard angepasst, um die Wirksamkeit der technischen und organisatorischen Maßnahmen zu gewährleisten.

k) Datenschutzfreundliche Voreinstellung

Maßnahmen, um die unbefugte oder unrechtmäßige Datenverarbeitung zu verhindern, indem durch Voreinstellung die zweckgebundene Datenverarbeitung gewährleistet ist. Berücksichtigt werden müssen Menge der erhobenen Daten, Umfang der Verarbeitung, Speicherfrist und Zugänglichkeit. Insbesondere sind Maßnahmen zu treffen, die verhindern, dass personenbezogene Daten automatisiert (ohne menschliches Eingreifen) einer unbestimmten Zahl an natürlichen Personen zugänglich gemacht werden:

Durch Voreinstellungen und Warnhinweise innerhalb der Produkte, wird der Nutzer zu einer datenschutzkonformen Verwendung angeleitet. Außerdem sind die Zugriffsmöglichkeiten personalisiert vergeben und passwortgesichert.

l) Risikomanagement

Verfahren, zur Feststellung des Risikos für die Rechte und Freiheiten natürlicher Personen und bedarfsgerechter Analyse des angemessenen Schutzniveaus unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos.

Die Risiken für die Rechte und Freiheiten natürlicher Personen werden kontinuierlich geprüft und bewertet und das Schutzniveau bei Bedarf entsprechend angepasst.

Stand: Januar 2020