Version Juli 2023

Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen

“dem Verantwortlichen”

(Angaben zu Name und Adresse siehe Seite 11 dieser Vereinbarung)

- nachstehend Auftraggeber genannt -

und

“dem Auftragsverarbeiter”

HELLMUT RUCK GmbH Daimlerstr. 23, 75305 Neuenbürg

- nachstehend Auftragnehmer genannt -

§ 1 Allgemeines

1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DS-GVO als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag 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 i.S.d. Art. 28 DS-GVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Auftragsverarbeitung.

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, Anonymisieren, Pseudonymisieren, Verschlüsseln oder sonstige Nutzung von Daten.

§ 2 Gegenstand und Dauer des Auftrags

1) Der Auftraggeber nutzt die vom Auftragnehmer bereitgestellte Anwendung “pododesk”. Sie ist erreichbar unter https://www.pododesk.net.

2) Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 1 (einem) Monat schriftlich zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 3 Konkretisierung des Auftragsinhalts Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten

1) Der Auftraggeber erfasst die Daten über die Software pododesk sämtliche Daten, die der Auftraggeber durch die Nutzung der Anwendung an pododesk übermittelt, werden auf der Kommunikationsstrecke mittels SSL verschlüsselt.

2) Der Auftragnehmer erhebt, nutzt und verarbeitet die Daten ausschließlich im Rahmen der getroffenen Nutzungsvereinbarung. Er verwendet die Daten ausschließlich zur Erbringung der vertragsgemäßen Leistungen. Der Auftragnehmer ist nicht befugt, die ihm überlassenen Daten an Dritte weiterzugeben, sofern dies nicht zur Erbringung der vereinbarten Leistung erforderlich ist. Kopien und Duplikate

bedürfen der vorherigen Zustimmung des Auftraggebers. Hiervon ausgenommen sind Sicherungskopien zur Einhaltung einer ordnungsgemäßen Datenverarbeitung.

3) Die Verarbeitung und Nutzung der Daten findet ausschließlich in einem Mitgliedstaat 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 DS-GVO erfüllt sind.

4) Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien, sofern diese vom Auftraggeber der Anwendung erfasst und eingegeben werden:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Ärztliche Anweisungen und Verordnungen
- Daten und Bilder über den Gesundheitszustand
- Daten und Bilder über die Behandlungsdurchführung und deren Ergebnisse

5) Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- Kunden/Patienten
- Interessenten
- ggfs. Betreuer oder Vertreter der vorgenannten
- externe Dienstleister
- Beschäftigte
- Lieferanten/Handelsvertreter
- Ärzte

§ 4 Technisch-organisatorische Maßnahmen

1) Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der gesetzlich vorgeschriebenen technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Eine Beschreibung der zugesicherten technischen und organisatorischen Maßnahmen liegt dem Vertrag bei und ist Vertragsbestandteil.

2) Die Datenverarbeitung findet auf IT-Systemen statt, für die technischen und organisatorischen Maßnahmen nach der Anlage gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO zum Schutz der Daten getroffen wurden.

3) Insgesamt handelt es sich bei den getroffenen Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich

- ○ Organisationskontrolle ○ Zutrittskontrolle
- ○ Zugangskontrolle
- ○ Zugriffskontrolle
- ○ Weitergabekontrolle
- ○ Verfügbarkeitskontrolle
- ○ Trennungsgebots

4) In diesem Rahmen gewährleistet der Auftragnehmer dem Auftraggeber die Umsetzung aller Maßnahmen gemäß Anlage 1 dieses Vertrages.

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

§ 5 Rechte und Pflichten des Auftraggebers

1) Der Auftraggeber ist verantwortliche Stelle für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber.

2) Der Auftraggeber ist als verantwortliche Stelle für die Wahrung der Betroffenenrechte verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen.

3) Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Konformität der geltenden Gesetzgebung durch die beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit (siehe Anlage 1) zur geltenden Gesetzeslage zu überzeugen. Der Auftraggeber ist verpflichtet, das Ergebnis in geeigneter Weise zu dokumentieren.

4) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen oder Weisungen in Textform (z.B. E-Mail) sind unverzüglich vom Auftraggeber schriftlich zu bestätigen.

5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Die Benennung erfolgt auf Seite 11 dieser Vereinbarung.
Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dem Auftragnehmer dies schriftlich oder in Textform mitteilen.

6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

7) Für den Fall, dass eine Informationspflicht gegenüber Dritten besteht, ist der Auftraggeber für die Erfüllung der Pflichten verantwortlich.

§ 6 Berechtigung, Einschränkung und Löschung von Daten

1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, zu loschen 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.

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

§ 7 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags ggfs. gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er soweit erforderlich insbesondere die Einhaltung folgender Vorgaben:

1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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.

3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

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

5) 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.

6) 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.

7) 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.

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

§ 8 Unterauftragnehmerverhältnisse

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 Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Derzeit arbeitet der Auftragnehmer mit den in Anlage 2 genannten Unterauftragnehmer zusammen.

3) Die Auslagerung auf Unterauftragnehmer oder der Wechsel von bestehenden Unterauftragnehmern sind zulässig, soweit:

a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

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

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 Zustimmung des Hauptauftragnehmers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 2 genannten Subunternehmer (Unterauftragsverhältnisse) durchgeführt.

§ 9 Kontrollrechte des Auftraggebers

1) Der Auftraggeber bleibt Herr der Daten. Er ist für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer, sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er ist weiterhin verantwortlich für die Beurteilung der Zulässigkeit der Datenverarbeitung, sowie für die Wahrung der Rechte der Betroffenen.

2) Der Auftraggeber hat das Recht, im Benehmen Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchfuhren zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

3) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren,

Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

§ 10 Mitteilung bei Verstößen des Auftragnehmers

1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzung 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, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

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 A

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

§ 11 Weisungsbefugnis des Auftraggebers

1) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften.

Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

§ 12 Löschung und Rückgabe von personenbezogenen Daten

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

2) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Datenbestände im Sinne dieser Vereinbarung, 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 der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber üb

§ 13 Geheimhaltungspflichten

1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 14 Rechtswahl

Für diese Vereinbarung und sämtliche Verträge zwischen den Parteien gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG).

§ 15 Erfüllungsort – Gerichtsstand

Es gilt der Sitz der HELLMUT RUCK GmbH als Erfüllungsort und ausschließlicher Gerichtsstand. Die HELLMUT RUCK GmbH kann jedoch nach eigener Wahl auch am allgemeinen Gerichtsstand des Auftraggebers klagen.

Anlage 1 - Allgemeine technische und organisatorische Maßnahmen

Anlage 2 - Genehmigte Subunternehmer / weiter Auftragsverarbeiter

Unterschriften

Mit der Unterschrift unter dieser Vereinbarung zur Auftragsverarbeitung, in der Fassung vom 17.05.2023, schließen der Auftraggeber und der Auftragnehmer eine Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO zu den vor- und nachgenannten Regelungen.

Der Auftraggeber und der Auftragnehmer verständigen sich darauf, dass die Unterschrift und Rücksendung dieser Seite 11 zur Dokumentation der Unterzeichnung der gesamten Vereinbarung ausreichend ist.

(Wenn Sie mehrere Niederlassungen betreiben, genügt eine Anschrift / die Anschrift die Sie im übrigen Geschäftsverkehr als Hauptanschrift verwenden.)

Auftraggeber

_____ Firmen-/Praxisbezeichnung Auftraggeber

_____ Firmen-/Praxisanschrift

_____ Ort, Datum

_____ Name in Druckbuchstaben

Unterschrift Praxisinhaber

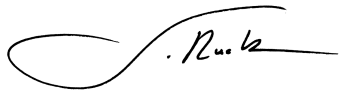
_____
ggfs. benannte “weisungsberechtigte Person” gem. § 5 dieser Vereinbarung (s. S. 5)

Auftragnehmer

HELLMUT RUCK GmbH Firmenname Auftragnehmer

Daimlerstr. 23, 75305 Neuenbürg

Simeon Ruck
Name in Druckbuchstaben



Unterschrift

Anlage 1

Allgemeine technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) Zutrittskontrolle

Der physikalische Speicherort der Daten im Sinne dieser Vereinbarung, befindet sich in einer professionellen Einrichtung eines Unterauftragnehmers (der gem. § 8 dieser Vereinbarung jedoch nicht an der Auftragsverarbeitung im Sinne der DS-GVO beteiligt ist).

Die umfangreichen Maßnahmen des Rechenzentrumsbetreibers genügen den Anforderungen der Datenschutz- und Datengeheimnis-Gesetze, welche dieser Vereinbarung zu Grunde liegen.
Da die getroffenen Maßnahmen stets dem Stand der Technik entsprechen, und somit einer permanenten Weiterentwicklung und Veränderung unterliegen, können Details zu den bestehenden Kontrollmaßnahmen und Sicherheitseinrichtungen des Betreibers bei Bedarf und auf Anfrage jederzeit aktuell zur Verfügung gestellt werden.

Zugangskontrolle

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Alle verwendeten Kennworte unterliegen speziellen Kennwortanforderungen hinsichtlich der Länge und der Komplexität.
- Bei wiederholter Fehleingabe von Passwörtern werden Accounts automatisch gesperrt und können erst nach dem Ablauf einer Zeitspanne (abhängig von der Anzahl von Fehlversuchen) durch Eingabe des korrekten Passworts wieder entsperrt werden.
- Jeder Nutzer erhält nur einen persönlichen Account. Sammel- oder Funktionsaccounts sind nicht zulässig.

Zugriffskontrolle

Sämtliche System- und Datenzugriffe aller Personen die seitens des Auftragnehmers an der Auftragsdatenverarbeitung im Sinne dieser Vereinbarung beteiligt sind, sind:

- soweit eingeschränkt wie möglich, ohne die Erledigung der übertragenen Aufgaben zu verhindern. Das bedeutet, dass kein Mitarbeiter auf Daten oder Systeme zugreifen kann, die er zur Erfüllung seiner Aufgaben nicht benötigt.

- sofern möglich vollständig und lückenlos protokolliert und unmanipulierbar nachzuvollziehen. Das bedeutet, dass durch sogenannte Log-Files Operationen jedes Mitarbeiters aufgezeichnet und später eingesehen und nachvollzogen werden könne.
- soweit möglich unabhängig vom Zugriff auf die eigentlichen Daten im Sinne dieser Vereinbarung und beziehen sich somit nur auf die technischen Systeme die zur

Verarbeitung der Daten verwendet werden, nicht aber auf die Daten selbst. Dadurch ist eine Veränderung der verarbeiteten Daten ausgeschlossen, und einer Löschung durch die redundante Bereitstellung von Systemkomponenten sowie zudem durch deren separat aufbewahrte Sicherung vorgebeugt.

Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Die Nutzer werden gemäß Weisung des Auftraggebers einzelnen Mandanten zugeordnet. Durch diese Lösung wird sichergestellt, dass kein Nutzer Zugriff auf Daten in einem anderen Container hat.
- Zum Testen von neu programmierten Funktionen wird eine Testumgebung getrennt von der Produktivumgebung betrieben. Auf dieser Testumgebung wird die Anwendung Stresstests unterzogen. Erst nach erfolgreichen Tests werden die neu programmierten Funktionen auf der Produktivumgebung allen Nutzer zur Verfügung gestellt.

Pseudonymisierung

Maßnahmen zur Verarbeitung der Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können:

- Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- Sofern für die jeweilige Datenverarbeitung möglich, werden aktuelle Verschlüsselungstechnologien eingesetzt

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO) Weitergabekontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Der Transport, die Übertragung und die Speicherung von Daten erfolgt ausschließlich verschlüsselt und passwortgeschützt. Hierfür werden Verschlüsselungstechnologien nach dem Stand der Technik eingesetzt.
- Für die Authentifizierung kommt eine elektronische Signatur zum Einsatz, mittels welcher sich der Sender und der Empfänger der Daten eindeutig identifizieren und authentifizieren.
- Alle Aktivitäten hinsichtlich der Weitergabe von Daten werden protokolliert
- Für den Fall eines physischen Datentransportes werden die Daten durch eine

  Transportsicherung geschützt.

  Eingabekontrolle

  Es ist jederzeit nachträglich überprüfbar, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.

3. Systemzugriffe werden in Logfiles gespeichert. Auf Logfiles besteht für die Benutzer kein Schreibzugriff.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
Verfügbarkeitskontrolle

Die physikalische und logische Verfügbarkeit der Daten im Sinne dieser Vereinbarung wird durch folgende Maßnahmen sichergestellt:

- Sicherung und Backup: Daten werden von den primären Systemen in regelmäßigen Zyklen automatisch gesichert, und in physikalisch getrennten Bereichen so aufbewahrt, dass eine Wiederherstellung auch bei Ausfall/Unverfügbarkeit der Primärsysteme möglich ist.
- Die physikalischen Komponenten der Primärsysteme, welche die Daten speichern, sind redundant ausgelegt (mindestens doppelt vorhanden), sodass die plötzliche Störung einzelner Bauteile keine Auswirkung auf die Verfügbarkeit der Daten hat.
- Eine unterbrechungsfreie Stromversorgung (USV) schützt die Systeme vor dem Ausfall der primären Stromzufuhr.
- Durch den Einsatz von sogenannten “Firewalls” und Virenschutzsystemen, sind die Systeme vor einem Ausfall durch unberechtigten schadhaften Zugriff (“Hacking”) sowie Schadprogramme (“Viren”) geschützt.

  Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung)

- Datenschutz-Management mit Risikoanalyse und Datenschutz-Folgenabschätzung, einschließlich regelmäßiger Mitarbeiter-Schulungen
- Ein etabliertes Incident-Response-Management inkl. definiertet Maßnahmen für relevante IS-Vorfälle mit definierten Melde- und Verhaltensregeln
- Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.
- Es erfolgt keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers. Der Auftraggeber erteilt die Weisung durch Unterzeichnung dieser Vereinbarung zur Auftragsverarbeitung

Anlage 2

Genehmigte Subunternehmer / weiter Auftragsverarbeiter

Subunternehmer / Weitere Auftragsverarbeiter	Anschrift	Zweck der Zusammenarbeit
MessageBird GmbH	MessageBird B.V. Trompenburgstraat 2C 1079 TX Amsterdam The Netherlands	SMS-Versand
Mailgun	Mailgun Technologies, Inc 112 E. Pecan St. #1135 San Antonio,TX 78205 US	Mailversand
Freshworks Inc.	Freshworks Inc.,(formerly known as Freshdesk Inc.) 2950 S. Delaware St, Suite 201, San Mateo, CA 94403, U.S.A	Kundendatenpflege
Mailjet GmbH	Alt-Moabit 2, 10557 Berlin, Germanyn Gesellschaftssitz: Alt-Moabit 2, 10557 Berlin, Germany	Mailversand
Make (ehemals Integromat LLC)	Celonis Inc. One World Trade Center Celonis Inc., 87th Floor New York, New York 10007 United States	Automatisierungen
Slack Technologies Limited	Slack Technologies Limited Level 1, Block A, Nova Atria North Sandyford Business District Dublin 18 Co. Dublin Irland	Automatisierungen

Heroku	Heroku, Inc., 1 Market St. Suite 300, San Francisco, CA 94105	Entwicklung
Amazon Web Services	Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 United States	Entwicklung
Google Ireland Limited	Google Cloud EMEA Limited Velasco Clanwilliam Place Dublin 2 Ireland	Websitenanwendung
SevDesk GmbH	sevDesk GmbH Hauptstraße 115 77652 Offenburg	Rechnungsversand
Techflow.ai GmbH	Techflow.ai GmbH. Ingelheimer Str. 23 64295 Darmstadt	Automatisierung
Gocardless SAS	GoCardless Ltd. Sutton Yard, Goswell Rd., London EC1V 7EN, Vereinigtes Königreich	Zahlungsverkehr
Auth0 by Okta	Okta Headquarters North America 100 First Street San Francisco, CA 94105, USA	Autentifizierung