Auftragsverarbeitungsvertrag

zwischen

MEISTERWERK APP GmbH
Oranienburger Straße 84
10178 Berlin

als Auftragsverarbeiter

(nachfolgend: Auftragnehmer)

und

dem Auftraggeber

I. Allgemeines

1. Der Auftragnehmer erbringt auf der Grundlage eines Hauptvertrages über eine von ihm entwickelte Software gegenüber Auftraggebern Dienstleistungen zur Verwaltung, Planung, Durchführung und Abrechnung insbesondere von Handwerkerleistungen. Teil der Erfüllung der Dienstleistungen ist die Verarbeitung personenbezogener Daten, die dem Auftragnehmer vom Auftraggeber zur Verfügung gestellt werden. Dahingehend sind insbesondere die Vorgaben in Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (nachfolgend: DSGVO) zu beachten. Zur Wahrung dieser Anforderungen schließen die Parteien diesen Vertrag.

2. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 DSGVO (Auftragsverarbeitung). Der Auftragsverarbeitungsvertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Auftragsverarbeitung von personenbezogenen Daten.

3. Sofern in diesem Vertrag die Begriffe „Datenverarbeitung“ und/oder „Verarbeitung“ (von Daten) benutzt werden, wird die Definition des Begriffs „Verarbeitung“ nach Art. 4 Nr. 2 DSGVO zugrunde gelegt.

II. Gegenstand des Auftrags

1. Zur Erfüllung der Verpflichtung aus dem Hauptvertrag mit dem Auftraggeber erhalten der Auftragnehmer und seine Beschäftigten durch den Auftraggeber Zugriff auf vom Auftraggeber erhobene personenbezogene Daten und verarbeiten diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Der Hauptvertrag und die allgemeinen Geschäftsbedingungen sind Anlagen zu dem Auftragverarbeitungsvertrag.

2. Der Auftragsverarbeitungsvertrag regelt ausschließlich den Umgang mit diesen personenbezogenen Daten. Der Abschluss des Auftragsverarbeitungsvertrages ist zwingend für den Abschluss des Hauptvertrages.

III. Dauer des Auftragsverarbeitungsvertrags

1. Der Auftragsverarbeitungsvertrag ist grundsätzlich rechtlich unselbstständig und teilt das rechtliche Schicksal des Hauptvertrags zwischen Auftraggeber und Auftragnehmer. Die Laufzeit des Auftragsverarbeitungsvertrages entspricht daher der des Hauptvertrages. Jede Kündigung oder sonstige Beendigung des Hauptvertrages gilt für diesen Vertrag entsprechend.

2. Der Auftragsverarbeitungsvertrag gilt jedoch dann über die Laufzeit des Hauptvertrages hinaus und solange, wie der Auftragnehmer noch personenbezogene Daten, die ihm zur Erfüllung der Dienstleistungen übermittelt wurden, speichert. Für die Rückgabe oder Löschung der Daten gilt Ziff. XIV.

3. Das Recht zur ordentlichen Kündigung des Auftragsverarbeitungsvertrages ist ausgeschlossen. Der Auftraggeber kann diesen Vertrag jederzeit aus wichtigem Grund ohne Einhaltung einer Frist kündigen. Ein wichtiger Grund liegt u.a. vor, wenn der Auftragnehmer in besonders schwerem Maße gegen die Bestimmung des Auftragsverarbeitungsvertrages und insbesondere gegen die aus Art. 28 DSGVO abgeleiteten Pflichten verstößt, der Auftragnehmer beharrlich eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers zu Kontrollzwecken nachdrücklich vertragswidrig verweigert. Für die bereits übermittelten Daten gilt vorstehende Ziff. 2.

IV. Gegenstand, Dauer und Zweck der vorgesehenen Datenverarbeitung; Übermittlung in Drittländer

1. Der Gegenstand, die Dauer und der Zweck der Datenverarbeitung durch den Auftragnehmer im Auftrag des Auftraggebers ergeben sich aus dem Hauptvertrag (einschließlich der dazugehörigen Leistungsbeschreibung).

2. Die Verarbeitung und Nutzung der Daten findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, in einem sonstigen Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum statt. Jede weitere Verlagerung in ein Drittland und jeder Zugriff aus einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers oder muss der Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland durch den Auftraggnehmer dienen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

V. Art der Datenverarbeitung und der personenbezogenen Daten

1. Die durch den Auftragnehmer verarbeiteten personenbezogenen Daten gehören insbesondere zu folgenden Datenkategorien:

    - Namen und Adressdaten
    - Kontaktdaten
    - Vertragsdaten
    - Mitarbeiterdaten
    - Standortdaten
    - Arbeitszeiten, Urlaubsanspruch- sowie Zeiten und Termininformationen
    - Bild-, Video- und Audiodaten

2. Die Art der Datenverarbeitung betrifft das Erheben und die Speicherung in einer Software der vom Auftraggeber über ein Interface eingegebenen personenbezogenen Daten im Rahmen einer Unternehmens- und Auftragsanlage, -bearbeitung oder Abrechnung von Dienstleistungen sowie die Übermittlung von personenbezogenen Daten zwischen dem Auftraggebern und seinen Mitarbeitern bzw. sonstigen Beauftragten.

3. Für eine umfassende Aufstellung verweisen wir auf Anlage 1 dieser Vereinbarung.

VI. Kategorien betroffener Personen

1. Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags betroffenen Personen umfasst:

    - Mitarbeiter des Auftraggebers oder sonstige von ihm Beauftragte
    - Kunden des Auftraggebers
    - Geschäftspartner des Auftraggebers

- Sonstige am Auftragsort anwesende Personen (z.B: Mieter, Angestellte des Kunden)

Für eine umfassende Aufstellung verweisen wir auf Anlage 1 dieser Vereinbarung

VII. Technische und organisatorische Maßnahmen/Sicherheit der Datenverarbeitung

1. Nach Art. 28 Abs. 3 S. 2 lit. c) DSGVO ist der Auftragnehmer verpflichtet, alle gem. Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (Datenschutzkonzept) zu ergreifen, um den Schutz der personenbezogene Daten sicherzustellen. Auf Art. 82 DSGVO wird hingewiesen.

2. Der Auftragnehmer wird daher mindestens die in Anlage 2 genannten technischen und organisatorischen Maßnahmen ergreifen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Etwaige weitergehende Pflichten, die nach Art. 32 DSGVO in seiner jeweiligen Fassung für den Auftragnehmer gelten, bleiben unberührt.

3. Der Auftragnehmer stellt sicher, dass die technischen und organisatorischen Maßnahmen dem jeweiligen Stand der Technik entsprechen. Insoweit ist es dem Auftragnehmer gestattet, alternative aber gleichwohl adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen im Hinblick auf die technischen und organisatorischen Maßnahmen sind vom Auftragnehmer zu dokumentieren.

4. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert ferner zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

5. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden nach Möglichkeit besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

VIII. Berichtigung, Löschung und Sperrung von Daten

1. Der Auftragnehmer darf die Daten, die Gegenstand der Auftragsverarbeitung sind, nur nach Weisung des Auftraggebers berichtigen, löschen oder sperren. Sollte sich ein Betroffener unmittelbar an den Auftragnehmer wenden, und um eine Berichtigung oder Löschung seiner Daten ersuchen, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

2. Eine Weisung kann sich insbesondere aus entsprechenden Eingaben des Auftragnehmers in der Software gemäß dem Hauptvertrag ergeben.

IX. Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen

1. Der Auftragnehmer verpflichtet sich, dass die geeigneten technischen und organisatorische Maßnahmen nach Ziff. VII. so durchgeführt werden, dass die Verarbeitung der Daten im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

2. Der Auftragnehmer stellt sicher, dass bei ihm – sofern gesetzlich erforderlich – ein betrieblicher Datenschutzbeauftragter, der die erforderliche Fachkunde und Zuverlässigkeit besitzt, bestellt ist. Derzeit ist dies nicht der Fall.

3. Der Auftragnehmer stellt zudem sicher, dass sich alle zur Verarbeitung der personenbezogenen Daten befugten Personen ihm gegenüber zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b) DSGVO).

4. Der Auftragnehmer wird angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit dabei unterstützen, damit dieser seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III. der DSGVO genannten Rechte der betroffenen Personen nachkommen kann (Art. 28 Abs. 3 lit. e) DSGVO).

5. Der Auftragnehmer wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten unterstützen (Art. 28 Abs. 3 lit. f) DSGVO).

6. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Er wird die vom Auftraggeber oder einem von diesem beauftragten Prüfer durchzuführenden Überprüfungen – einschließlich Inspektionen – ermöglichen und dazu beitragen (Art. 28 Abs. 3 lit. h) DSGVO).

X. Berechtigung zur Begründung von Unterauftragsverhältnissen mit weiteren Auftragnehmern (Art. 28 Abs. 2 DSGVO)

1. Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung für die Beauftragung von Unterauftragsverarbeitern. Der Auftragnehmer wird alle bereits bei Abschluss des Auftragsverarbeitungsvertrages bestehenden Unterauftragsverhältnisse

in der Anlage 3 zu diesem Vertrag angeben. Der Auftragnehmer unterrichtet den Auftraggeber mit ausreichendem Vorlauf (mindestens 14 Tage) in Textform über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Auftraggeber damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können.

2. Der Auftragnehmer wird Unterauftragnehmer sorgfältig auswählen. Er wird die in Art. 28 Abs. 2 und 4 DSGVO genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragnehmers einhalten.

3. Der Vertrag des Auftragnehmers mit dem Unterauftragnehmer muss den gesetzlichen Anforderungen des Art. 28 DSGVO entsprechen und dabei ein diesem Auftragsverarbeitungsvertrag im Wesentlichen entsprechendes Niveau gegenüber dem Unterauftragnehmer umsetzen. Der Auftragnehmer ist verpflichtet, die für den Datenschutz relevanten vertraglichen Vereinbarungen mit dem Unterauftragnehmer dem Auftraggeber auf Verlangen offenzulegen.

4. Bei einer Unterbeauftragung werden dem Auftraggeber gegenüber dem Unterauftragnehmer durch den Auftragnehmer Kontroll- und Weisungsrechte entsprechend den Vorgaben dieses Vertrags und im Einklang mit den Vorgaben in Art. 28 Abs. 3 DSGVO eingeräumt. Dies umfasst auch das Recht des Auftraggebers, von dem Unterauftragnehmer auf schriftliche Anforderung hin Auskunft über den datenschutzrelevanten Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis zu erhalten, auf Verlangen durch Übermittlung von Kopien der betreffenden Vertragsunterlagen.

5. Die Weiterleitung von Daten an einen Unterauftragnehmer ist erst zulässig, wenn dieser geeignete technischen und organisatorischen Maßnahmen zur Datensicherheit umgesetzt hat. Dies umfasst die Einhaltung der Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten. Der Auftragnehmer hat sich für die Einhaltung der Pflichten des Unterauftragnehmers vor der ersten Übermittlung personenbezogener Daten hinreichende Garantien geben zu lassen.

XI. Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers (Art. 28 Abs. 3 lit. h) DSGVO)

1. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und die Einhaltung der

vertraglichen Pflichten zu kontrollieren. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

2. Sofern nicht ein wichtiger Grund für eine sofortige Kontrollmaßnahme vorliegt, ist die Kontrollmaßnahme durch den Auftraggeber mit einer angemessenen Frist anzukündigen. Ein wichtiger Grund für eine unverzügliche Kontrollmaßnahme liegt u.a. in den Fällen der Art. 33 und 34 DSGVO vor.

3. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses und insbesondere bei der Durchführung von Kontrollmaßnahmen erlangten Kenntnisse von und Datensicherheitsmaßnahmen und Geschäftsgeheimnissen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Auftragsverarbeitungsvertrages bestehen.

XII. Mitwirkungspflichten des Auftragnehmers; mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen (Art. 28 Abs. 3 lit. f) DSGVO)

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten und stellt alle für den Auftraggeber zur Erstellung des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO relevanten Informationen, die seine Tätigkeit betreffen, zur Verfügung. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber zu übersenden.

2. Der Auftragnehmer informiert den Auftraggeber unverzüglich nach Kenntniserlangung, wenn er oder eine bei ihm beschäftigte Person gegen Vorschriften zum Schutz personenbezogener Daten, gegen Bestimmungen nach diesem Vertrag zur Auftragsverarbeitung oder gegen eine vom Auftraggeber erteilte sonstige Weisung verstoßen hat. Dies gilt insbesondere, wenn Anhaltspunkte dafür bestehen, dass ein Dritter – unerheblich aus welchem Grund – unrechtmäßig Kenntnis von Auftraggeberdaten erlangt haben könnte oder wenn in sonstiger Weise eine Gefährdung für die Integrität oder Vertraulichkeit der Auftraggeberdaten eingetreten ist. Der Auftragnehmer ist verpflichtet, den Auftraggeber auf dessen Wunsch unverzüglich im Rahmen des Zumutbaren zu unterstützen, um etwaige nachteilige Folgen für den Auftraggeber oder Betroffene zu verhindern.

3. Dies gilt insbesondere in den Fällen, in denen gemäß Art. 33 oder 34 DSGVO eine Meldepflicht gegenüber der Aufsichtsbehörde oder eine Benachrichtigungspflicht gegenüber der betroffenen Person bestehen könnte.

4. In Fälle des Art. 33 oder 34 DSGVO übermittelt der Auftragnehmer unverzüglich die für die Erfüllung von Melde- und Nachweispflichten des Auftraggebers notwendigen Informationen einschließlich der Informationen nach Art. 33 Abs. 3 DSGVO.

XIII. Umfang der Weisungsbefugnisse des Auftraggebers

1. Der Auftragnehmer verarbeitet personenbezogene Daten – auch in Bezug auf die etwaige Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – ausschließlich nach Weisung des Auftraggebers, sofern nicht ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a) DSGVO vorliegt. Der Auftraggeber hat das Recht, die im Rahmen der oben genannten Aufgabenbeschreibung erfolgende Datenverarbeitung in Bezug auf Art, Umfang und Verfahren im Einzelfall zu konkretisieren. Auskünfte an Dritte oder die betroffenen Personen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen, sofern der dazu nicht rechtlich verpflichtet ist.

2. Weisungen sollen grundsätzlich schriftlich oder in Textform (z.B. per E-Mail) erteilt werden. Mündliche Weisungen wird der Auftraggeber nachfolgend schriftlich oder per E-Mail (in Textform) bestätigen. Die Bestätigung ist keine Voraussetzung für die Verbindlichkeit der Weisung. Der Auftraggeber ist verpflichtet, die Weisungen zu dokumentieren und die Dokumentation dem Auftragnehmer auf Anfrage zur Verfügung zu stellen.

   Weisungsberechtigte Person(en) des Auftraggebers ist der Vertragspartner des Hauptvertrages.

   Weisungen an den Auftragnehmer sind an dpa@meisterwerk.app zu richten.

3. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

4. Das Weisungsrecht erstreckt sich nicht auf die von Auftragnehmer zu ergreifenden technischen und organisatorischen Maßnahmen und findet im Allgemeinen seine Grenzen in den Vorgaben und Zielen des Auftragsverarbeitungsvertrages sowie des Hauptvertrages.

5. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke als zur Erfüllung seiner Verpflichtungen aus dem Hauptvertrag. Er ist insbesondere nicht berechtigt, sie an Dritte im eigenen Interesse weiterzugeben. Kopien und Duplikate der Daten werden

ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Erfüllung gesetzlicher Aufbewahrungspflichten erforderlich sind.

6. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist in diesen Fällen berechtigt, die Durchführung der Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

XIV. Rückgabe überlassener Datenträger, Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags (Art. 28 Abs. 3 lit. g) DSGVO)

1. Nach Beendigung des Hauptvertrages, gleich aus welchem Grund, hat der Auftragnehmer sämtliche im Auftrag des Auftraggebers verarbeiteten personenbezogene Daten dem Auftraggeber auf dessen Aufforderung hin auszuhändigen bzw. in sonstiger Weise verfügbar zu machen oder nach Wahl des Auftraggebers löschen.

2. Hat der Auftraggeber keine Wahl nach Ziff. 1 getroffen, wird der Auftragnehmer die im Auftrag des Auftraggebers verarbeiteten personenbezogene Daten sechs Monate nach Beendigung des Hauptvertrages löschen

3. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

4. Eine etwaige Rückgabe ist vom Auftraggeber in entsprechender Anwendung des Hauptvertrags zu vergüten.

5. Der Auftragnehmer ist berechtigt, sowohl eine solche Löschung bzw. Vernichtung als auch eine Rückgabe ausnahmsweise zu unterlassen, sofern und soweit rechtliche Anforderungen an den Auftragnehmer entgegenstehen. Der Auftragnehmer wird solche rechtlichen Anforderungen dem Auftraggeber mitteilen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

XV. Haftungsbegrenzung

1. Der Auftragnehmer haftet bei Verstößen gegen seine Verpflichtungen aus dem Auftragverarbeitungsvertrag gegenüber dem Auftraggeber nach den nachfolgenden Bestimmungen:
    a. Bei Vorsatz, grober Fahrlässigkeit sowie bei schuldhafter Verletzung von Leben, Körper oder Gesundheit nach den gesetzlichen Bestimmungen;
    b. Bei fahrlässig verursachten Sach- und Vermögensschäden nur bei Verletzung wesentlicher Vertragspflichten, also Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht oder deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung die andere Partei regelmäßig vertrauen darf (sog. Kardinalspflichten), jedoch der Höhe nach beschränkt auf die bei Vertragsschluss vorhersehbaren und vertragstypischen Schäden, maximal jedoch EUR 125.000,-. Insbesondere Folgeschäden stellen keine vorhersehbaren und vertragstypischen Schäden dar.
2. Die vorstehenden Haftungsbeschränkungen gelten auch zugunsten von gesetzlichen Vertretern, Mitarbeitern und Erfüllungsgehilfen des Auftragnehmers.

XVI. Inkrafttreten, salvatorische Klausel, Gerichtsstand, anwendbares Recht

1. Der Vertrag tritt mit Zustimmung durch den Auftraggeber in Kraft. Die Übermittlung bzw. Bereitstellung des Auftragsverarbeitungsvertrages durch den Auftragnehmer gilt als Angebot zum Abschluss des Vertrages.

2. Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

3. Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Berlin.

XVII. Umfang des Auftragsverarbeitungsvertrags

1. Als Bestandteile dieses Vertrags gelten die nachfolgend aufgeführten folgenden Anlagen, auch soweit diese nicht fest mit dem vorliegenden Vertrag verbunden sind.

    - Anlage 1: Aufstellung betroffener Personen/Betroffenengruppen sowie betroffener Daten/Datenkategorien
    - Anlage 2: Datensicherheitskonzept (technische und organisatorische Maßnahmen nach Art. 32 DSGVO)

- Anlage 3: Unterauftragnehmer

2. Das in Anlage 2 beschriebene Datensicherheitskonzept ist im Falle von Fortschreibungen in der jeweils beim Auftragnehmer vorhandenen aktuellen Fassung Bestandteil des Auftragsverarbeitungsvertrages.

Anlage 1

Betroffene Personen/-gruppen	Betroffene Daten/-kategorien
Mitarbeiter des Auftraggebers oder sonstige von ihm Beauftragte	● Name und Adressdaten ● Kontaktdaten ○ Telefonnummer ○ E-Mail ● Arbeits.- und Pausenzeiten ● Krankheits- und Ferientage ● Tätigkeit ○ Chat-Nachrichten ○ Kommentare ○ Termine ○ Terminverfügbarkeit ● Bild-, Audio-, Video Dateien und Dokumente
Kunden des Auftraggebers	● Name und Adressdaten ● Kontaktdaten ○ Telefonnummer ○ E-Mail ● Bild-, Audio-, Video Dateien und Dokumente ● Tätigkeit ○ Chat-Nachrichten ○ Kommentare ○ Termine ○ Terminverfügbarkeit ● Vertragsabrechnungs- und Zahlungsdaten
Geschäftspartner des Auftraggebers	● Name und Adressdaten ● Kontaktdaten ○ Telefonnummer

	○ E-Mail ● Bild-, Audio-, Video Dateien und Dokumente ● Tätigkeit ○ Chat-Nachrichten ○ Kommentare ○ Termine ○ Terminverfügbarkeit ● Vertragsabrechnungs- und Zahlungsdaten
Sonstige am Auftragsort anwesende Personen (z.B: Mieter, Angestellte des Kunden)	● Name und Adressdaten ● Kontaktdaten ○ Telefonnummer ○ E-Mail ● Bild-, Audio-, Video Dateien und Dokumente ● Tätigkeit ○ Chat-Nachrichten ○ Kommentare ○ Termine ○ Terminverfügbarkeit ● Vertragsabrechnungs- und Zahlungsdaten

Anlagen 2

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.v. Art. 32 DSGVO.

1. Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 Hs. 2 lit. a) DSGVO)
    - [Datenbankverschlüsselung, eingeschränkter Zugriff auf Produktionsdaten]
        - Der Zugriff auf die Datenbank wird über eine verschlüsselte SSH-Verbindung hergestellt und zusätzlich durch VPN-Verschlüsselung gesichert. Die Verschlüsselung wird auch für Daten im Ruhezustand verwendet.

    - Der Zugriff auf die Server-Infrastruktur ist durch VPN-Verschlüsselung und ein Passwort mit 2fa-Authentifizierung geschützt, und die Berechtigungen werden je nach Bedarf mit einer fein abgestuften Zugriffskontrolle pro Benutzer eingeschränkt.
    - Personenbezogene Daten werden anonymisiert, bevor sie für andere Zwecke als für die Erfüllung der Funktionen der Hauptanwendung verarbeitet werden.

2. Vertraulichkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Zutrittskontrollen

- Schlüsselregelung/Schlüsselbuch
    - Eine begrenzte Anzahl von Mitarbeitern erhält Schlüssel für den Zugang zum Büro. Die Mitarbeiter erhalten je nach Bedarf Zugang zu den Schlüsseln und müssen mindestens ein Jahr oder länger im Unternehmen gearbeitet haben.
- Manuelles Schließsystem
    - Das Büro ist mit mehreren manuellen Schließsystemen an der Bürotür und einem einzigen manuellen Schließsystem an der Gebäudetür gesichert.

2.2. Zugangskontrollen

- W-LAN ist gesichert
    - W-LAN ist mit WPA3 gesichert.
- Passwortvergabe/Passwortregeln
    - Passwortrichtlinien: mindestens 8 Zeichen einschließlich Sonderzeichen. Empfohlen werden Zufallspasswörter, die von einem Tool zur Verwaltung von Passwörtern unterstützt werden.
    - Die 2-Faktor-Authentifizierung ist für den Zugang zur Server-Infrastruktur und zu den Finanzdiensten erforderlich. Sie wird für alle anderen Systeme empfohlen, in denen sie verfügbar ist.
- Regelung für den Umgang mit Passwörtern
    - Die Mitarbeiter erhalten Zugang zu einem vom Unternehmen verwalteten Passwort-Manager und sind verpflichtet, alle Unternehmensdaten mit diesem Tool zu speichern.
    - Den Mitarbeitern ist es nicht gestattet, Passwörter auf einem lokalen Speicher zu speichern.

- Einsatz von Anti-Viren-Software

    - Die Arbeitsgeräte werden durch die Verwendung eines aktuellen Betriebssystems (iOS, MacOS, Android, Windows) mit der neuesten Version, Firewall und Virenscans geschützt.
- Einsatz verschlüsselter Cloud-Technologie
    - Die Mitarbeiter erhalten für verschiedene Funktionen Zugang zu Cloud-Anwendungen. Die Konten sind mit ihrer Arbeits-E-Mail und ihren Anmeldedaten verknüpft.

2.3. Zugriffskontrollen

- Anzahl der Administratoren auf das Mindeste begrenzt
    - Administratoren werden auf der Grundlage ihrer Rolle im Unternehmen und ihres Bedarfs an erweiterten Rechten für die Erfüllung ihrer Aufgaben ernannt. Es wird ein Minimum an Administratoren ernannt, und alle anderen Benutzer erhalten je nach Bedarf fein abgestufte Zugriffsberechtigungen.
- Physische Löschung von Datenträgern vor deren Wiederverwendung
    - Der Speicher der physischen Geräte wird nach der Ausmusterung und vor der Wiederverwendung der Geräte gelöscht und neu formatiert.
- Datenaufbewahrung auf verschlüsselten Cloud-Servern
    - Virtuelle Datenspeicher in der Cloud-Infrastruktur sind verschlüsselt.

2.4. Trennung

- Physikalisch getrennte Speicherung auf gesonderten Systemen und Datenträgern.
    - Den einzelnen Serveranwendungen werden getrennte Datenbankressourcen für die Persistenz der Daten zugewiesen. Die Serveranwendungen werden mit gemeinsamen Rechen- und Speicherressourcen ausgeführt. Die Anwendungsgrenzen werden mit Hilfe von Industriestandard-Containertechnologie aufrechterhalten.

3. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

- Angemessene Verschlüsselungstechniken
    - Alle Verschlüsselungen von Daten bei der Übertragung und im Ruhezustand werden von vertrauenswürdigen Drittanbietern durchgeführt, die den Anweisungen in den von ihnen bereitgestellten Unterlagen folgen. Wenn möglich, werden die von unseren Infrastrukturanbietern bereitgestellten Verschlüsselungsdienste der manuellen Anwendung dieser Technologien vorgezogen.
- E-Mail-Verschlüsselung
    - E-Mails werden bei den besten E-Mail-Anbietern in der Cloud gehostet und der E-Mail-Verkehr wird während der Übertragung verschlüsselt.
- Regelungen bei Ausscheiden von Mitarbeitern

    - Mitarbeiter, die das Unternehmen verlassen, sind verpflichtet, vor ihrem Ausscheiden alles Material, das sich in ihrem Besitz befindet UND mit ihrer Arbeit zusammenhäng Die Geräte werden zurückgegeben, gelöscht und neu formatiert, bevor sie im Unternehmen wiederverwendet werden.
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
    - Die Mitarbeiter sind im Rahmen ihres Arbeitsvertrags an eine Vertraulichkeitsvereinbarung gebunden.
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO):
    - Die Standardeinstellungen für die Datenerfassung beschränken sich auf die Daten, deren Erfassung erforderlich ist.
    - Die Zugriffsrechte der Mitarbeiter auf Benutzerdaten werden standardmäßig verweigert und nur bei Bedarf und nachgewiesener Vertrauenswürdigkeit erteilt.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)
    - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
        - Datensicherungen werden verschlüsselt und redundant in der Cloud in mehreren Rechenzentren gespeichert.
    - Erstellen eines Recoverykonzepts
        - Es wird ein Notfallwiederherstellungsplan geführt und die Ausführung routinemäßig geübt. Der Notfallwiederherstellungsplan wird regelmäßig überprüft.
    - Backup-Strategie (offline, online z.B. Cloud)
        - Für die Datensicherung werden mehrere Strategien eingesetzt, darunter Point-in-Time, automatische Datenbank-Snapshots, manuelle Datenbank-Snapshots und Sicherungsdienste von Drittanbietern.
    - Rasche Wiederherstellbarkeit Verfügbarkeit und Zugang zu personenbezogenen Daten (Art. 32 Abs. 1 lit. c) DSGVO):
        - Datensicherungs- und Wiederherstellungsprozesse, redundante Speichersysteme, Notfallpläne und Verfahren zur Reaktion auf Vorfälle werden wie zuvor beschrieben beibehalten, um die schnelle Wiederherstellbarkeit und Verfügbarkeit personenbezogener Daten zu gewährleisten.
5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Datenschutz-Management)
    - Incident-Response-Management
        - Es werden etablierte Verfahren zur Erkennung von, Reaktion auf und Abschwächung von Vorfällen, die die Vertraulichkeit, Integrität oder Verfügbarkeit

personenbezogener Daten beeinträchtigen könnten, beibehalten und regelmäßig überprüft.

- Regelmäßige Datenschutzschulungen
    - Alle Mitarbeiter, die mit personenbezogenen Daten umgehen, erhalten regelmäßig Schulungen zu Datenschutzgesetzen, -richtlinien und bewährten Verfahren, um das Bewusstsein und die Kompetenz aufrechtzuerhalten.
- Hard- und Softwareprodukte aus seriösen Quellen
    - Hardware- und Softwareprodukte werden von seriösen Anbietern beschafft und bieten angemessene Sicherheitsvorkehrungen.
- Datenschutzbeauftragter
    - Momentan besteht keine gesetzliche Verpflichtung für uns zur Beauftragung eines Datenschutzbeauftragten. [Falls gewünscht:] Es ist geplant, zukünftig einen qualifizierten Datenschutzbeauftragten zu ernennen, um unsere Datenschutzbemühungen zu überwachen und die Einhaltung der DSGVO sicherzustellen.
- Ausreichende Ressourcen für Datenschutzmanagementsystem
    - Es werden ausreichende personelle, finanzielle und technische Ressourcen bereitgestellt, um ein wirksames Datenschutzmanagementsystem einzuführen und aufrechtzuerhalten.
- Schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 DSGVO
    - Bei der Beauftragung von Datenverarbeitern werden schriftliche Anweisungen durch Datenverarbeitungsverträge erteilt, die den Anforderungen von Artikel 28 DSGVO entsprechen.
- Datenschutzmanagement-Audits und Maßnahmenplan
    - Interne Audits unserer Datenschutzpraktiken werden regelmäßig durchgeführt, und es wird ein Aktionsplan zur Behebung festgestellter Lücken oder verbesserungswürdiger Bereiche erstellt.

Anlagen 3

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen Dritter in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

Unterauftragnehmer	Art der Datenverarbeitung
AWS Amazon Web Services AWS (Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg	Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung,
Uploadcare Uploadcare Inc, 2711 Centerville Road, Suite 400 City of Wilmington, County of New Castle, 19808, USA, registered under the laws of USA 82-1639831	Erfassen, Empfangen, Speicherung (temporär), Anpassung oder Veränderung, Auslesen
Sendgrid Twilio Ireland Limited. (25 – 28 North Wall Quay, North Wall, Dublin 1, D01 H104, Ireland	Erheben, Erfassen, Empfangen, Ordnen, Auslesen
Twilio Twilio Ireland Limited. (25 – 28 North Wall Quay, North Wall, Dublin 1, D01 H104, Ireland	Erheben, Erfassen, Empfangen, Ordnen, Auslesen
Rollout Cloudbees Faubourg de l'Hôpital 18, CH-2000 Neuchâtel, Switzerland	Erfassen, Empfangen, Ordnen, Auslesen, Abfragen, Verwendung,
Pusher Pusher Ltd, located at Eighth Floor 6 New Street Square, New Fetter Lane, London, England EC4A 3AQ	Erheben, Erfassen, Empfangen, Ordnen, Anpassung oder Veränderung, Auslesen, Verwendung,
Expo 650 Industries Inc (650 Industries, Inc, 624 University Avenue, 1st Floor, Palo Alto, CA-94301, USA	Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung,
Mixpanel, Inc. One Front Street, 28th Floor, San Francisco, CA 94111, USA)	Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung,
Mapbox, Inc. 1133 15th St NW, Suite 825, Washington DC, 20005	Erfassen, Empfangen, Auslesen, Abfragen
Intercom R&D Unlimited Company mit Hauptsitz in 55 2nd St, 4th Fl., San Francisco, CA 94105 USA	Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung,
Segment Twilio Ireland Limited. (25 – 28 North Wall Quay, North Wall, Dublin 1, D01 H104, Ireland)	Erheben, Erfassen, Empfangen, Ordnen, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung,

Sentry Functional Software, Inc., 132 Hawthorne Street, San Francisco, CA-94107, USA	Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Auslesen, Abfragen, Verwendung,
HubSpot 2 Canal Park, Cambridge, MA 02141, Vereinigte Staaten	Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung,
OpenAI OpenAI Ireland Ltd. (OpenAI Ireland Ltd., 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland)	Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung,
SAS BJT PARTNERS - RINGOVER GROUP 50 bis rue Maurice Arnoux 92120 Montrouge, France	Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung
Ringo 59 Avenue Sainte-Foy, 92200 Neuilly sur Seine	Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung
Retell AI Inc. 1121 Industrial Rd, Ste 500, San Carlos, CA 94070	Erheben, Erfassen, Empfangen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung