Vertrag über die Auftragsverarbeitung

zwischen

cloudmanufaktur GmbH

Seestr. 46

8598 Bottighofen

- im nachfolgenden „Auftragnehmer“ genannt -

und

_____
Firma

_____
Straße Hausnr.

_____ - _____
PLZ – Ort

Kundennummer: _____

- im nachfolgenden „Auftraggeber“ genannt

Die Regelungen zur Auftragsverarbeitung ergänzen die allgemeinen Geschäftsbedingungen der cloudmanufaktur GmbH. Im Falle eines Widerspruchs zwischen diesen Regelungen und den allgemeinen Geschäftsbedingungen der cloudmanufaktur GmbH gehen diese Regelungen zur Auftragsverarbeitung vor.

§ 1 Allgemeines

(1) Der Auftraggeber beauftragt den Auftragnehmer mit der Wartung und Pflege von Software (virtuellen Telefonanlage) und IT-Systemen. Bei der Erbringung von Supportleistungen ist es nicht auszuschließen, dass der Auftragnehmer Zugriff auf personenbezogenen Daten erhält, welche auf dem IT-System gespeichert sind. Der Zugriff auf personenbezogenen Daten ist eine Nebenfolge, nicht
Zweck oder Gegenstand der Leistungserbringung durch den Auftragnehmer. Die Parteien regeln mit dieser Vereinbarung ausschließlich die datenschutzrechtlichen Verpflichtungen, die bei einem Zugriff auf personenbezogene Daten des Auftraggebers zu beachten sind.

(2) cloudmanufaktur verarbeitet personenbezogene Daten im Auftrag des Kunden i.S.d. Art. 4 Nr. 8 und Art. 28 der Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(3) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von personenbezogenen Daten) benutzt wird, gilt die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO. Die Verwendung personenbezogener Daten umfasst insbesondere die Speicherung, Veränderung, Übermittlung, Sperrung, Löschung sowie Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung personenbezogener Daten.

(4) Alle in dieser Vereinbarung enthaltenen Verweise auf die DSGVO gelten in ihrer jeweils aktuellen Fassung.

§ 2 Gegenstand und Dauer des Auftrags

I. Gegenstand

(1) Der Gegenstand des Auftrages ergibt sich über die Bereitstellung einer virtuellen Telefonanlage sowie optionalen Verträge zwischen den Vertragspartnern.

(2) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum bzw. in einem sicheren Drittland erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu 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 (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

II. Dauer:

(1) Der Vertrag beginnt mit der Beauftragung und wird auf unbestimmte Zeit geschlossen.

(2) Dieser Vertrag endet bei Kündigung des Hauptvertrages ohne dass es einer gesonderten Kündigung bedarf.

(3) Etwaige Lösch- und Rückgabepflichten nach Beendigung dieses Vertrages sind in § 12 geregelt.

(4) Der Kunde kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der cloudmanufaktur gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, cloudmanufaktur eine Weisung des Kunden nicht ausführen kann oder will oder cloudmanufaktur den Zutritt des Kunden oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

§ 3 Konkretisierung des Auftragsinhalts

I. Art der Daten

Folgende Datenarten sind Gegenstand der Verarbeitung durch den Auftragnehmer:

a) Bestandsdaten
Für Kundenkonto-Inhaber: Name, Anschrift, Email-Adresse, Telefonnummer, Mobilrufnummer

b) Nutzungsdaten
IP Adresse, Angaben über Beginn und Ende der Gesprächsverbindung, gewählte Rufnummer, angenommene Rufnummer, Rufnummern von Weiterleitungen

c) Inhaltsdaten
Voicemail-Aufzeichnungen und PDF-Dokumente (Faxübertragungen), angelegte Kontakte im Cloud-Anlagen Telefonbuch

II. Kategorien betroffener Personen:

(1) Kreis der von der Datenverarbeitung betroffenen Personen:
Benutzer Ihres Accounts, anrufende und angerufene Teilnehmer bzw. Sender/Empfänger von

SMS/Fax, cloudmanufaktur Mitarbeiter, Vertriebspartner der cloudmanufaktur, Dienstleister des Kunden.

(2) Regelungen für Cloudmanufaktur Vertriebspartner:
Cloudmanufaktur Vertriebspartner haben ausschließlich Zugriff auf Bestands- und Nutzungsdaten ihrer Kunden. Der Datenschutz zwischen Kunde und Vertriebspartner muss durch einen separaten Vertrag vereinbart werden.

(3) Der Auftraggeber verpflichtet sich, die Benutzer des Accounts und - soweit erforderlich - den Betriebsrat oder vergleichbare Vertretungen über die Verarbeitung der in 1. genannten Daten zu informieren.

§ 4 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 Anlage 1].

(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.

§ 5 Berichtigung, 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, 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.

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

§ 6 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

(2) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(3) Je nach Umfang der Maßnahmen kann der Auftragnehmer eine Vergütung verlangen.

(4) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 6 entsprechend.

(5) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 7 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(3) 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.

(4) Die Verarbeitung von Daten im Auftrag des Verantwortlichen findet grundsätzlich in den Betriebsstätten des Auftragsverarbeiters statt.
Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) unter Einhaltung der Maßnahmen nach Art. 32 DSGVO erlauben.
Als Datenverarbeitungsgeräte kommen ausschließlich Firmen-Rechner zum Einsatz, die entsprechend abgesichert sind. Der Transport der Daten erfolgt ausschließlich über verschlüsselte Verbindungen.

(5) 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 Anlage 1].

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

(7) 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.

(8) 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.

(9) 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.

(10) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

§ 8 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten.

(2) Weisungen durch den Auftraggeber haben in schriftlicher Form zu erfolgen.

(3) Der Auftragnehmer ist verpflichtet den Auftraggeber über mögliche Verstöße gegen Datenschutzvorschriften zu informieren.

(4) Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

§ 9 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen 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.

(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.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO bzw. vergleichbarer Schweizer Datenschutzgesetze
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO bzw. vergleichbarer Schweizer Datenschutzgesetze
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(3) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§ 10 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 als Telekommunikationsleistungen, Wartung und Benutzerservice 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 schriftlicher Information des Auftraggebers beauftragen. Der Auftraggeber hat ein Widerspruchsrecht. Der Widerspruch darf nur aus wichtigen Grund erfolgen.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber den Subunternehmern gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(4) Die Verpflichtung des Subunternehmers muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.
Cloudmanufaktur hat alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 2 zu diesem Vertrag angeben.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziffer 7 dieses Vertrages) des Auftragsgebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte vom Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(6) 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.

(7) Der Auftragnehmer nimmt für die Verarbeitung von personenbezogenen Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag personenbezogene Daten verarbeiten.

§ 11 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 Maß- nahmen, 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

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

§ 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 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. Das Protokoll der Löschung ist 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.

§ 13 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Gerichtsstand ist Bottighofen.

Ort, Datum	Unterschrift (Auftraggeber / Kunde)
Bottighofen, 01.01.2023	
Ort, Datum	Unterschrift (Auftragnehmer / cloudmanufaktur)

Anlage 1 – Technisch-organisatorische Maßnahmen des Auftragnehmers

Version 1.0

§ 1. Einleitung:

Beschrieben werden hier die allgemeinen technisch-organisatorische Maßnahmen der cloudmanufaktur GmbH. Dabei werden die Maßnahmen in diesem Dokument generisch aufgeführt. Die detaillierten Beschreibungen der Technologien, Konzepte, Regelungen und sonstiger Maßnahmen sind in gesonderten Dokumentationen aufgeführt.

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

I. Zutrittskontrolle

A Gebäude Seestr. 46, Bottighofen

a) Der Zugang zum Gebäude ist nur mit Chipkarte möglich
b) Besucher werden an der Eingangstür abgeholt und persönlich begleitet
c) Die Chipkarten sind den Mitarbeitern zugeordnet
d) Chipkarten, die verloren gemeldet werden, werden sofort deaktiviert

B Rechenzentrum Frankfurt

a) Der Zugang zum Gebäude ist nur für autorisierte Personen möglich
b) Das Gebäude ist durch Alarmsystem, Videoüberwachung in allen Bereichen und 24/7 Sicherheitspersonal gesichert.
c) Die 19 Zollschränke sind immer verschlossen, die Schlüssel müssen beim Wachdienst abgeholt werden.

C Rechenzentrum Frankfurt

a) Der Zugang zum Gebäude ist nur für autorisierte Personen möglich
b) Das Gebäude ist durch Alarmsystem, Videoüberwachung in allen Bereichen und 24/7 Sicherheitspersonal gesichert.
c) Die 19 Zollschränke sind immer verschlossen, die Schlüssel müssen beim Wachdienst abgeholt werden.

II. Zugangskontrolle

a) Alle Benutzerkonten sind passwortgeschützt.
b) Jeder Mitarbeiter hat sein persönliches Passwort.
c) Wir haben folgende Passwortkonventionen:
mindestens 12 Zeichen, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
d) Bei der Anmeldung sind 5 Fehlversuche erlaubt.
e) Die PC´s und einzelne Anwendungen sperren den Zugang bei Inaktivität.
f) Unsere Mitarbeiter sind angewiesen, bei Verlassen des Arbeitsplatzes den PC zu sperren.
g) Der Zugriff auf die Benutzerkonten ist für die Mitarbeiter auf die Dauer ihres Arbeitsverhältnisses begrenzt. Endet das Arbeitsverhältnis werden die Zugangsberechtigungen gesperrt.
h) Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.
i) Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.
j) Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

III. Zugriffskontrolle

a) Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.
b) Berechtigungen für IT-Systeme und Applikationen werden ausschließlich von Administratoren eingerichtet.
c) Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken für ihren Aufgabenbereich benötigen.
d) Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.
e) Es ist auf Berechtigungsgruppenebene festgelegt wer die Daten löschen, exportieren, bearbeiten und ansehen kann.
f) Datenträgerentsorgung erfolgt nach DIN66399 P-4
g) Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.
h) Alle Server- und Client-Systeme werden regelmäßig unter Einsatz eines zentralen Remotemanagementsystems mit Sicherheits-Updates aktualisiert und fortlaufend überwacht.

IV. Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

V. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

a) aktuell wird keine Pseudonymisierung durchgeführt.

§ 14 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

I. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

a) Eine Weitergabe von personenbezogenen Daten erfolgt nur in dem Umfang, wie dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.
b) Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.
c) Unsere Mitarbeiter werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

II. Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

a) Die Eingabe, Änderung und Löschung von personenbezogenen Daten, wird grundsätzlich protokolliert.
b) Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

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

I. Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

a) Alle Server werden von der cloudmanufaktur GmbH administriert (Sicherungskonzept, Backupstrategie, Notfallplanung etc.).
b) Alle Rechner sind mit Virenschutzprogrammen ausgestattet.
c) Alle Daten werden mehrfach an verschiedene Standorte gesichert.
d) Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage sowie eine CO2-Löschanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.
e) cloudmanufaktur verfügt über Firewall-Cluster in den Rechenzentren.

II. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

a) Die Backup-Strategie erfolgt durch die cloudmanufaktur GmbH.
b) Sicherstellung einer schnellen Beschaffung von Hardware durch entsprechende Serviceverträge mit Lieferanten und Dienstleistern.

§ 16 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

I. Incident-Response-Management (Vorfalls-Reaktions-Management, Notfallpläne)

Wir haben ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit. Und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

a) Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
b) Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

II. Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:

a) Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen.

III. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Bei Online Formularen wird schon bei der Entwicklung Sorge dafür getragen, dass diese datenschutzfreundlich voreingestellt sind.

Anlage 2: Unterauftragsverhältnisse

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

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Newsletter-Versand, Information über anstehende Updates oder Wartungen:

CleverReach GmbH & Co. KG, Mühlenstr. 43, 26180 Rastede, Deutschland

Telefondienst, Chat-Dienst über Webseite

Offinea AG, Zugerstrasse 32, 6341 Baar, Schweiz
MWC – Mobile Word Communications GmbH, Kavalierstr. 9, 13187 Berlin, Deutschland
Günstige-werbeartikel.de GmbH, Hainer Weg 305, 60599 Frankfurt am Main, Deutschland

Webhosting, Mailhosting

LA Webhosting, Inhaber Philipp Lahn, Spielbergtor 12d, 99099 Erfurt, Deutschland

Cloud-Dienstleistungen, Cloudspeicher, Hosting, Hosted Exchange, Office 365, Onlinekalender, Kontaktsynchronisation

Microsoft Enterprise Service Privacy, Microsoft Corporation, Microsoft Ireland Operations, Ltd., South County Business Park Leopardstown, Dublin 18, D18 P521, Irland
Citybites, Hermann-Köhl-Str. 8, 89160 Dornstadt

Cloud- Dienstleistungen, Cloudspeicher, Hosting, Software as a Service (SaaS)

OVH, St. Johanner Str. 41-43, 66111 Saarbrücken, Deutschland, Kanada
Google Ireland Ltd, Gorden House, Barrow Street, Dublin 4, Irland

Auftragsabwicklung Hardwarelieferungen sowie DSL-Leitungsbereitstellung

Citybites, Hermann-Köhl-Str. 8, 89160 Dornstadt
iWay AG, Badenerstrasse 569, 8048 Zürich, Schweiz
Peoplefone GmbH, Erich-Herion-Straße 6, 70736 Fellbach, Deutschland

Fernwartungssoftware

TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen, Deutschland

Anlage 3 - Gegenstand des Auftrags

1. Gegenstand der Vereinbarung

Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Auftrag, Leistungsbeschreibung und AGB (nachfolgend Hauptvertrag), soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

2. Art(en) der personenbezogenen Daten

Die Art der verarbeiteten Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

3. Kategorien betroffener Person

Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

4. Weisungsberechtigte Personen des Auftraggebers:

Inhaber/ Geschäftsführer des Auftraggebers sowie folgende Personen:

5. Weisungsempfangsberechtigte Personen des Auftragnehmers:

Geschäftsführer sowie Support-Mitarbeiter