Vereinbarung zur Auftragsdatenverarbeitung

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen dem Kunden (im Folgenden als "**Kunde**") und CA Customer Alliance GmbH, Hausvogteipl. 12, 10117 Berlin, Deutschland (im Folgenden als "**Auftragnehmer**").

Bei Fragen oder Anmerkungen zu dieser Vereinbarung zur Auftragsdatenverarbeitung oder zum Datenschutz im Allgemeinen wenden Sie sich bitte an folgende E-Mail-Adresse: dataprotection@customer-alliance.com

1. **Gegenstand der Vereinbarung**

Im Rahmen der Erbringung von Dienstleistungen gemäß dem Dienstleistungsvertrag (im Folgenden als "**Hauptvertrag**") ist es erforderlich, dass der Auftragnehmer personenbezogene Daten verarbeitet, für die der Kunde im Sinne des Datenschutzrechts als Verantwortlicher fungiert (im Folgenden als "**Kundendaten**"). Diese Vereinbarung spezifiziert die datenschutzrechtlichen Pflichten und Rechte der Parteien im Zusammenhang mit der Nutzung der Kundendaten durch den Auftragnehmer zur Erbringung der Dienstleistungen gemäß dem Hauptvertrag.

2. **Umfang der Beauftragung**

    1. Der Auftragnehmer verarbeitet die Kundendaten im Auftrag und nach den Weisungen des Kunden im Sinne des Art. 28 DSGVO (Auftragsverarbeitung). Der Kunde bleibt datenschutzrechtlich Verantwortlicher.

    2. Die Verarbeitung der Kundendaten durch den Auftragnehmer erfolgt in der Art und dem Umfang und zu dem Zweck, wie in Anlage 1 zu dieser Vereinbarung festgelegt; die Verarbeitung bezieht sich auf die dort angegebenen Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags.

    3. Die Verarbeitung von Kundendaten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder eines anderen Vertragsstaates des Europäischen Wirtschaftsraums (EWR) statt. Dem Auftragnehmer ist es dennoch gestattet, Kundendaten gemäß den Bestimmungen dieser Vereinbarung außerhalb des EWR zu verarbeiten, wenn er den Kunden vorab über den Ort der Datenverarbeitung informiert und die Anforderungen der Art. 44 bis 48 DSGVO erfüllt sind oder eine Ausnahme gemäß Art. 49 DSGVO gilt.

3. **Weisungsrecht des Kunden**

    1. Der Auftragnehmer verarbeitet die Kundendaten gemäß den Weisungen des Kunden, es sei denn, der Auftragnehmer ist gesetzlich zu einer anderen Verarbeitung verpflichtet. In letzterem Fall teilt der Auftragnehmer dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht aufgrund eines wichtigen öffentlichen Interesses verbietet.

    2. Die Weisungen des Kunden sind grundsätzlich abschließend in den Bestimmungen dieser Vereinbarung festgelegt und dokumentiert. Einzelne Weisungen, die von den Festlegungen dieser Vereinbarung abweichen oder zusätzliche Anforderungen stellen, bedürfen der gegenseitigen Vereinbarung und sind schriftlich zu erteilen.

    3. Der Auftragnehmer stellt sicher, dass die Kundendaten gemäß den vom Kunden erteilten Weisungen verarbeitet werden. Ist der Auftragnehmer der Ansicht, dass eine vom Kunden erteilte Weisung gegen diese Vereinbarung oder geltendes Datenschutzrecht verstößt, ist er

nach entsprechender Information des Kunden berechtigt, die Ausführung der Weisung auszusetzen, bis der Kunde die Weisung bestätigt.

4. **Rechtliche Verantwortlichkeit des Kunden**

    1. Der Kunde ist im Verhältnis zwischen den Parteien allein verantwortlich für die Zulässigkeit der Verarbeitung der Kundendaten und für die Wahrung der Rechte der betroffenen Personen.

    2. Der Kunde ist verantwortlich, dem Auftragnehmer die Kundendaten rechtzeitig für die Erbringung der Dienstleistungen gemäß dem Hauptvertrag zur Verfügung zu stellen, und er ist verantwortlich für die Qualität der Kundendaten. Der Kunde informiert den Auftragnehmer unverzüglich und vollständig, wenn er bei der Prüfung der Ergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen oder seine Weisungen feststellt.

    3. Ist der Auftragnehmer verpflichtet, einer staatlichen Stelle oder Person Informationen über die Verarbeitung von Kundendaten zu geben oder in anderer Weise mit diesen Stellen zusammenzuarbeiten, so ist der Kunde auf erste Anforderung verpflichtet, den Auftragnehmer bei der Bereitstellung solcher Informationen und bei der Erfüllung anderer Kooperationspflichten zu unterstützen.

5. **Anforderungen an das Personal**

Der Auftragnehmer verpflichtet alle Personen, die mit der Verarbeitung von Kundendaten befasst sind, zur Vertraulichkeit in Bezug auf die Verarbeitung von Kundendaten.

6. **Sicherheit der Verarbeitung**

    1. Der Auftragnehmer ergreift gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Kundendaten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen, um ein dem Risiko angemessenes Schutzniveau für Kundendaten zu gewährleisten. Die aktuellen Maßnahmen sind in **Anlage 2** aufgeführt.

    2. Der Auftragnehmer hat das Recht, technische und organisatorische Maßnahmen während der Laufzeit der Vereinbarung zu ändern, solange sie weiterhin den gesetzlichen Anforderungen entsprechen.

7. **Beauftragung weiterer Auftragsverarbeiter**

    1. Der Kunde erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter in Bezug auf die Verarbeitung von Kundendaten zu beauftragen. Weitere zum Zeitpunkt des Vertragsabschlusses konsultierte Auftragsverarbeiter ergeben sich aus **Anlage 3**. Generell ist keine Genehmigung für vertragliche Beziehungen mit Dienstleistern erforderlich, die mit der Prüfung oder Wartung von Datenverarbeitungsverfahren oder -systemen durch Dritte befasst sind oder die sonstige Zusatzleistungen umfassen, auch wenn dabei ein Zugriff auf Kundendaten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Schritte zum Schutz der Vertraulichkeit der Kundendaten unternimmt.

    2. Der Auftragnehmer informiert den Kunden über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder den Ersatz weiterer Auftragsverarbeiter. Im Einzelfall hat der Kunde das

Recht, gegen den Einsatz eines potenziellen weiteren Auftragsverarbeiters Einspruch zu erheben. Ein Einspruch darf vom Kunden nur aus wichtigen Gründen erhoben werden, die dem Auftragnehmer nachzuweisen sind. Sofern der Kunde nicht innerhalb von 14 Tagen nach Erhalt der Mitteilung Einspruch erhebt, verfällt sein Recht, gegen den entsprechenden Einsatz Einspruch zu erheben. Erhebt der Kunde Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diese Vereinbarung mit einer Frist von drei (3) Monaten zu kündigen.

3. Die Vereinbarung zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem die gleichen Pflichten auferlegen, die dem Auftragnehmer aus dieser Vereinbarung obliegen. Die Parteien vereinbaren, dass diese Anforderung erfüllt ist, wenn der Vertrag ein Schutzniveau aufweist, das dieser Vereinbarung entspricht, bzw. wenn dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt werden.

8. **Rechte der betroffenen Personen**

1. Der Auftragnehmer unterstützt den Kunden im Rahmen des Zumutbaren durch technische und organisatorische Maßnahmen bei der Erfüllung von dessen Pflicht, auf Anfragen zur Ausübung der Rechte betroffener Personen zu reagieren.

2. Soweit eine betroffene Person einen Antrag auf Ausübung ihrer Rechte direkt an den Auftragnehmer stellt, leitet der Auftragnehmer diesen Antrag rechtzeitig an den Kunden weiter.

3. Der Auftragnehmer informiert den Kunden über alle Informationen bezüglich der gespeicherten Kundendaten, über die Empfänger von Kundendaten, an die der Auftragnehmer sie gemäß der Weisung weitergeben soll, und über den Zweck der Speicherung, soweit der Kunde nicht über diese Informationen verfügt und soweit er nicht in der Lage ist, sie selbst zu erheben.

4. Der Auftragnehmer ermöglicht dem Kunden im Rahmen des Zumutbaren und Erforderlichen, Kundendaten zu berichtigen, zu löschen oder die weitere Verarbeitung einzuschränken, oder berichtigt, sperrt oder schränkt auf Weisung des Kunden selbst die weitere Verarbeitung ein, wenn und soweit dies für den Kunden unmöglich ist.

9. **Mitteilungs- und Unterstützungspflichten des Auftragnehmers**

1. Soweit der Kunde aufgrund einer Verletzung der Sicherheit von Kundendaten einer gesetzlichen Meldepflicht unterliegt (insbesondere gemäß Art. 33, 34 DSGVO), informiert der Auftragnehmer den Kunden rechtzeitig über alle meldepflichtigen Ereignisse in seinem Verantwortungsbereich. Der Auftragnehmer unterstützt den Kunden auf dessen Anfrage im Rahmen des Zumutbaren und Erforderlichen bei der Erfüllung der Meldepflichten.

2. Der Auftragnehmer unterstützt den Kunden im Rahmen des Zumutbaren und Erforderlichen bei den vom Kunden durchzuführenden Datenschutz-Folgenabschätzungen und gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörde gemäß Art. 35, 36 DSGVO.

10. **Löschung von Kundendaten**

1. Der Auftragnehmer löscht die Kundendaten nach Beendigung dieser Vereinbarung, sofern der Auftragnehmer nicht gesetzlich zur weiteren Speicherung der Kundendaten verpflichtet ist.

2. Der Auftragnehmer kann Dokumentationen, die als Nachweis für die ordnungsgemäße und korrekte Verarbeitung von Kundendaten dienen, auch nach Beendigung der Vereinbarung aufbewahren.

11. **Nachweise und Audits**

    1. Der Auftragnehmer stellt dem Kunden auf dessen Anfrage alle dem Auftragnehmer zur Verfügung stehenden und erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten aus dieser Vereinbarung zur Verfügung.

    2. Der Kunde ist berechtigt, den Auftragnehmer hinsichtlich der Einhaltung der Bestimmungen dieser Vereinbarung zu überprüfen, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen; einschließlich Inspektionen.

    3. Zur Durchführung von Inspektionen gemäß Ziffer 11.2 ist der Kunde berechtigt, die Geschäftsräume des Auftragnehmers, in denen Kundendaten verarbeitet werden, zu den üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5. auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strenger Geheimhaltung der Geschäfts- und Betriebsgeheimnisse des Auftragnehmers zu betreten.

    4. Der Auftragnehmer ist berechtigt, nach eigenem Ermessen und unter Berücksichtigung der gesetzlichen Verpflichtungen des Kunden, Informationen nicht offenzulegen, die im Hinblick auf das Geschäft des Auftragnehmers sensibel sind oder wenn der Auftragnehmer infolge ihrer Offenlegung gegen gesetzliche oder andere vertragliche Bestimmungen verstoßen würde. Der Kunde ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, Kosteninformationen, Qualitätskontroll- und Vertragsmanagementberichte oder andere vertrauliche Daten des Auftragnehmers zu erhalten, die für die vereinbarten Prüfungszwecke nicht direkt relevant sind.

    5. Der Kunde informiert den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen im Voraus) über alle Umstände im Zusammenhang mit der Durchführung des Audits. Der Kunde kann ein Audit pro Kalenderjahr durchführen. Weitere Audits werden gegen Kostenerstattung und nach Rücksprache mit dem Auftragnehmer durchgeführt.

    6. Beauftragt der Kunde einen Dritten mit der Durchführung des Audits, so hat der Kunde den Dritten schriftlich ebenso zu verpflichten, wie der Kunde gegenüber dem Auftragnehmer gemäß dieser Ziffer 11 der Vereinbarung verpflichtet ist. Darüber hinaus hat der Kunde den Dritten zur Geheimhaltung und Vertraulichkeit zu verpflichten, es sei denn, der Dritte unterliegt einer beruflichen Geheimhaltungspflicht.

    7. Nach Ermessen des Auftragnehmers kann der Nachweis der Einhaltung der Verpflichtungen aus dieser Vereinbarung anstelle einer Inspektion auch durch Vorlage eines geeigneten, aktuellen Gutachtens oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Prüfungsabteilung, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzprüfer oder Qualitätsprüfer) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit - z.B. gemäß "BSI-Grundschutz" - ("Auditbericht") erbracht werden, wenn der Auditbericht es dem Kunden in angemessener Weise ermöglicht, sich von der Einhaltung der vertraglichen Verpflichtungen zu überzeugen.

12. **Vertragslaufzeit und Kündigung**

Die Laufzeit und Kündigung dieser Vereinbarung richtet sich nach den Laufzeit- und Kündigungsbestimmungen des Hauptvertrags. Eine Kündigung des Hauptvertrags führt automatisch zu einer Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

13. **Haftung**

1. Die Haftung des Auftragnehmers aus dieser Vereinbarung richtet sich nach den im Hauptvertrag vorgesehenen Haftungsbeschränkungen. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die durch eine schuldhafte Verletzung dieser Vereinbarung oder einer seiner datenschutzrechtlichen Pflichten als Verantwortlicher durch den Kunden verursacht wurden, stellt der Kunde den Auftragnehmer auf erstes Anfordern von diesen Ansprüchen frei.

2. Der Kunde verpflichtet sich, den Auftragnehmer auf erstes Anfordern von allen möglichen Bußgeldern freizustellen, die dem Auftragnehmer entsprechend dem Verantwortungsanteil des Kunden für den mit dem Bußgeld sanktionierten Verstoß auferlegt werden.

14. **Schlussbestimmungen**

    1. Für Streitigkeiten aus diesem Vertrag gilt deutsches Recht. Erfüllungsort und Gerichtsstand ist der Sitz des Auftragnehmers. Bei Widersprüchen in den beiden Sprachfassungen ist die deutsche Fassung maßgebend.

    2. Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine rechtlich zulässige Bestimmung zu ersetzen, die dem Zweck der unwirksamen Bestimmung am nächsten kommt und die Anforderungen des Art. 28 DSGVO erfüllt.

    3. Im Falle von Konflikten zwischen dieser Vereinbarung und anderen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, haben die Bestimmungen dieser Vereinbarung Vorrang.

Anlage:

Anlage 1: Zweck, Art und Umfang der Verarbeitung von Kundendaten, Arten personenbezogener Daten und Kategorien betroffener Personen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Weitere Auftragsverarbeiter

Anlage 1 - Zweck, Art und Umfang der Verarbeitung von Kundendaten, Arten personenbezogener Daten und Kategorien betroffener Personen

1. **Zweck der Datenverarbeitung**

Der Auftragnehmer sendet Nachrichten an Endkunden von und im Auftrag des Kunden vor und während der Erbringung seiner Dienstleistung, um Feedback zu erhalten, die Kommunikation zwischen dem Kunden und seinen Endkunden zu verbessern, zu standardisieren und zu automatisieren. Die Ergebnisse werden im Auftrag des Kunden verarbeitet und ausgewertet. Darüber hinaus werden Auswertungen aus indirektem und abgeleitetem Feedback, wie Informationen aus internen und/oder öffentlichen Quellen, genutzt, um die Stimme des Endkunden vollständig darzustellen. Der Auftragnehmer aggregiert und anonymisiert dadurch die über die Plattform gesammelten Kundendaten, um dem Kunden zusätzliche Dienstleistungen wie Berichterstattung, Benchmarking und KPI-Überwachungsfunktionen im Zusammenhang mit dem Feedback der Endkunden des Kunden anzubieten.

2. **Arten personenbezogener Daten**

    a. Stammdaten (z.B. Name, Geschlecht, Sprache);

b. Kontaktdaten (z.B. E-Mail-Adresse, Anschrift, Telefonnummer);

c. Kommunikationsdaten (z.B. E-Mail-Korrespondenz);

d. Vertragsdaten (z.B. Vertragsdauer, Informationen zur Leistungserbringung wie Umsatz oder Kosten);

e. Gegebenenfalls vorhandene individuelle Segmentierungsdaten des Kunden für seine Endkunden wie Art des Vertragsabschlusses (Internet, Telefon, etc.), Herkunftsland, Dienstleistungskategorie oder Altersgruppe;

f. Bewertung des Kunden durch den Endkunden (Kundenbewertung);

g. Zufriedenheitsanalysen (z.B. Text-, Themen- und Ausdrucksauswertungen).

3. **Kategorien betroffener Personen**

a. Personal des Kunden;

b. Endkunden des Kunden;

c. Lieferanten des Kunden.

Anlage 2 -- Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen wurden zum Schutz personenbezogener Daten getroffen:

- **1. Zutrittskontrolle**

Unbefugten Personen ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Sichergestellt durch:

a. Definition von Sicherheitsbereichen und berechtigten Personen

b. Raumsicherung (Schlüssel, Rollladen, etc.)

c. Anwesenheitsaufzeichnung

d. Außensicherung des Gebäudes (Einzäunung, Sicherheitstüren/-fenster)

e. Sorgfalt bei der Auswahl von Sicherheitspersonal

f. Sorgfalt bei der Auswahl von Reinigungsdiensten

g. Videoüberwachung der Eingänge

h. Schlüsselmanagement / Regelung (Auf- und Zuschließen) / Dokumentation der Schlüsselverteilung

i. Automatisches Zutrittskontrollsystem

j. Chipkarten / Transpondersysteme

k. Manuelles Schließsystem

l. Sicherheitsschlösser

m. Türen mit Knauf (außen)

n. Stark eingeschränkte Zugriffsrechte zum Serverraum

o. Server in abschließbaren Serverschränken, Schlüssel bei der IT-Abteilung

2. **Zugangskontrolle (extern)**

Es muss verhindert werden, dass Datenverarbeitungssysteme von unbefugten Personen genutzt werden können.

Sichergestellt durch:

a. Abschließbarkeit der Datenstation

b. Anmeldung mit Benutzername & Passwort und Vorgaben für deren Änderung (Gültigkeitsdauer max. 1 Jahr)

c. Verschlüsselung von Passwörtern

d. Anti-Virus-Software Server

e. Anti-Virus-Software Clients

f. Firewall

g. Mobile Device Management

h. Verwendung von VPN-Tunneln für Fernzugriff

i. Sperrung externer Schnittstellen (USB)

j. Verschlüsselung von Notebooks / Tablets

k. Verwaltung von Benutzerberechtigungen

l. Erstellung von Benutzerprofilen

m. Zentrale Passwortvergabe

n. Sichere Passwortrichtlinie

o. Lösch-/Vernichtungsrichtlinie

p. Datenschutz- und Sicherheitsrichtlinie

3. **Zugriffskontrolle (intern)**

Es ist dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Sichergestellt durch:

a. Authentifizierung mit Benutzern + Passwörtern

b. Benutzerspezifisches abgestuftes Rechtemanagement /Rollendefinition

c. Verwaltung der Benutzerrechte durch Administratoren

d. Minimale Anzahl von Administratoren

e. Dokumentation des Rechtemanagements

f. Bildschirmverdunklung bei Arbeitsunterbrechung

g. Regelmäßige Sicherheitsupdates

h. Aktenvernichter (min. Stufe 3, Kreuzschnitt)

i. Protokollierung des Zugriffs auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

j. Sichere Passwortrichtlinie

k. Lösch-/Vernichtungsrichtlinie

l. Datenschutz- und Sicherheitsrichtlinie

4. **Trennungskontrolle**

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Sichergestellt durch:

a. Getrennte Softwaresysteme

b. Getrennte Datenbanken und Speicherung

c. Steuerung über Berechtigungskonzept

d. Trennung durch Zugriffsregelungen

e. Festlegung von Datenbankrechten

5. **Weitergabekontrolle**

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Sichergestellt durch:

a. Festlegung von Befugnissen für die Verarbeitung von Daten

b. Festlegung der berechtigten übermittelnden Parteien, übermittelnden Empfänger und Übermittlungswege

c. Transportsicherheit von Datenträgern

d. Gesichertes W-LAN

e. Regelungen zur Vernichtung von Datenträgern

f. E-Mail-Verschlüsselung (S/MIME, PGP, REDDCRYPT)

g. IT-Sicherheitsrichtlinie

6. **Eingabekontrolle**

Es ist dafür Sorge zu tragen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Sichergestellt durch:

a. Lese-/Schreibzugriffsverwaltung

b. Protokollierung von Lese-/Schreibzugriffen und Programmaufrufen

c. Kennzeichnung von Dateneingabedokumenten mit Namen und Datum nach Eingabe

d. Bestimmungen zur Änderung von Zugriffsrechten und Datenverantwortlichkeit

e. Strenge Verantwortlichkeiten für Löschungen

7. **Verfügbarkeitskontrolle**

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Sichergestellt durch:

a. Erstellung periodischer Sicherungskopien

b. USV-Schutz bei Stromausfall

c. Virenschutz/Firewall

d. Notfallplan

e. Wiederherstellungsplan

f. Permanent aktiver DDoS-Schutz

8. **Auftragskontrolle**

Es muss gewährleistet sein, dass personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, nur entsprechend den Weisungen des Kunden verarbeitet werden können.

Sichergestellt durch:

a. Festlegung von Rechten und Pflichten des Auftragnehmers

b. Vertrag für die Auftragsdatenverarbeitung

c. Schulung aller Mitarbeiter mit Zugriffsrechten

d. Regelmäßige Datenschutzaudits

e. Vereinbarung über Kontroll- und Prüfrechte

f. Auftragnehmer benennt Datenschutzbeauftragten oder verantwortliche Person

Anlage 3 -- Weitere Auftragsverarbeiter			
Firma, Adresse	**Dienstleistung / Art der Verarbeitung**	**Rechtsschutz**	**Maßnahmen für ein vergleichbares Schutzniveau (nur in Drittstaaten)**
ALL-INKL.COM - Neue Medien München, Hauptstraße 68, 02742 Friedersdorf Deutschland	Webhosting	Datenverarbeitungsvereinbarung	/
Apollo 415 Mission St, Etage 37, San Francisco, Kalifornien 94105, USA	Datenanreicherung	Standardvertragsklausel und individuelle Beurteilung auf ein mit dem EU-Standard vergleichbares Schutzniveau.	ISO-Zertifikat (27001) und SOC-2-Konformität zertifiziert durch A-LIGN.
char desarrollo de sistemas s.l.u. Parque Empresarial Arboretum – Avda. de la Fama, 16-20, 3ª planta 08940 Cornellà de Llobregat – Barcelona – Spanien	Anbieter von Immobilienverwaltungssystemen	Datenverarbeitungsvereinbarung	Datenverschlüsselung im Ruhezustand und für Daten während der Übertragung – HTTPS für alle Dienste mit TLS (SSL) und vollständig DSGVO-konform
CHARGEBEE INC., 340 S. Lemon Avenue, Suite Nr. 1537, Walnuss, CA 91789 USA	Abrechnung	Standardvertragsklausel und individuelle Beurteilung auf ein mit dem EU-Standard vergleichbares Schutzniveau.	Zertifizierungen und Audits durch Dritte; ISO 27001-Zertifikat; SOC 1/SOC 2- und MFA-Standards; Sicherheitsrichtlinien auf Netzwerk-, Anwendungs- und Betriebsebene; AWS-Sicherheitseinrichtung – mehrere Zertifizierungen für Rechenzentren, einschließlich ISO 27001-Konformität, PCI-Zertifizierung und SOC-Berichte.
Google LLC, 1600 Amphitheatre Parkway, Bergblick, CA 94043 USA	Google Workspace Google Analytics	Standardvertragsklausel und individuelle Beurteilung auf ein mit dem EU-Standard vergleichbares Schutzniveau.	ISO-Zertifikate (ISO 27001, 27017, 27018); Datenschutzrichtlinie; Compliance Center und Berichte.
HelpScout PBC 177 Huntington Ave, Boston, MA 02115, USA	Support-Helpdesk	Standardvertragsklausel und individuelle Beurteilung auf ein mit dem EU-Standard vergleichbares Schutzniveau.	Help Scout ist SOC2 Typ 2 für Sicherheit und Verfügbarkeit zertifiziert. EU-Datenschutzgesetze, einschließlich der EU-Datenschutz-Grundverordnung

			(„EU-DSGVO“) AWS-Sicherheit eingerichtet
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Deutschland	Hosting	Datenverarbeitungsver einbarung	/
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 USA	Inbound-Marketin g, Vertrieb, Kundenerfolg und Kundenbeziehung smanagement	Standardvertragsklause l und individuelle Beurteilung auf ein mit dem EU-Standard vergleichbares Schutzniveau.	Verbindliche Unternehmensregeln; Rechenzentrum (ISO 27001-Zertifikat / SOC 2-Audit); HTTPs-Verschlüsselung.
Luzmo NV Tiensevest 102 Box 201, B-3000 Leuven, Belgien	Konversationsanal yse	#VALUE!	AICPA SOC 2 Typ II-konform
Mailgun Technologies, Inc., 548 Market Street, Suite 43099, San Francisco, CA 94101 USA	E-Mail-Anbieter (E-Mail-API)	Standardvertragsklause l und individuelle Beurteilung auf ein mit dem EU-Standard vergleichbares Schutzniveau.	Externer Netzwerkscan und Penetrationstest; Datenverschlüsselung; Einbrucherkennung; Lieferantenverwaltungsverfahren – Kontrolle und regelmäßige Prüfung aller Unterauftragsverarbeiter.
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Büro 365	Standardvertragsklause l und individuelle Beurteilung auf ein mit dem EU-Standard vergleichbares Schutzniveau.	Externe Vertrauens- und Prüfberichte; ISO 27001, 27017, 27018, 22301, 277701 Zertifikate; Richtlinie zur Verhinderung von Datenverlust; Konform mit SSAE 18 SOC 1 Typ II und SSAE 18 SOC 2 Typ II.
Nonius Rua Eng.º Frederico Ulrich, 2650 4470-605 Moreira da Maia Portugal	Anbieter von Immobilienverwalt ungssystemen	Datenverarbeitungsver einbarung	Datenverschlüsselung im Ruhezustand und für Daten während der Übertragung – HTTPS für alle Dienste mit TLS (SSL) und vollständig DSGVO-konform
OpenAI OpCo, LLC 3180 18th Street, San Francisco, CA 94110	Erkenntnisse, Berichterstattung, Analytik	Datenverarbeitungsver einbarung	/
OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken Deutschland	Hosting	Datenverarbeitungsver einbarung	/
Scaling Technologies GmbH, Pfarrer-Hillmann-Weg 1, 51069 Köln Deutschland	Web-Operationen	Datenverarbeitungsver einbarung	/
Stripe, Inc. 510 Townsend Street San	Zahlungslösung	Standardvertragsklause l und individuelle	Datenverschlüsselung im Ruhezustand und für Daten während

Francisco, CA 94103 USA		Beurteilung auf ein mit dem EU-Standard vergleichbares Schutzniveau.	der Übertragung – HTTPS für alle Dienste, die TLS (SSL) verwenden; alle Kartennummern werden im Ruhezustand mit AES-256 verschlüsselt; Audit-Protokolle; Zugriffsverwaltungsrichtlinie; PCI Service Provider Level 1-Zertifikat.
Twilio, Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105 USA	Anbieter für Kurznachrichten (SMS)	Standardvertragsklausel und individuelle Beurteilung auf ein mit dem EU-Standard vergleichbares Schutzniveau.	Verbindliche Unternehmensregeln; Sicherheitsrahmen basierend auf ISO 27001; ISO/IEC 27001, ISO/IEC 27017 & 27018, SOC 2 Typ II, PCI DSS Level 1 Zertifikate; AWS-Sicherheitseinrichtung – mehrere Zertifizierungen für Rechenzentren, einschließlich ISO 27001-Konformität, PCI-Zertifizierung und SOC-Bericht; Datenbanken (Kundendaten) werden mit dem Advanced Encryption Standard verschlüsselt und Kundendaten werden bei der Übertragung zwischen der Softwareanwendung des Kunden und den Diensten mit TLS v1.2 verschlüsselt; Penetrationstests; Richtlinien und Verfahren für das Management von Sicherheitsvorfällen gemäß NIST SP 800-61.