Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO zwischen dem Kunden (nachfolgend „**Auftraggeber**“ genannt) und CA Customer Alliance GmbH, Ullsteinstr. 130, 12109 Berlin, Deutschland (nachfolgend „**Auftragnehmer**“ genannt).

1. Vertragsgegenstand

Im Rahmen der Leistungserbringung aus dem Servicevertrag (nachfolgend „**Hauptvertrag**“ genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Auftraggeber-Daten**“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Umfang der Beauftragung

2.1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

2.2. Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in **Anlage 1** zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.3. Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3. Weisungsbefugnisse des Auftraggebers

3.1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer

gemeinsamen Abstimmung und müssen dokumentiert werden.

3.3. Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

4. Verantwortlichkeit des Auftraggebers

4.1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich.

4.2. Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.3. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. Anforderungen an das Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

6. Sicherheit der Verarbeitung

6.1. Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten. Die aktuellen Maßnahmen können der **Anlage 2** entnommen werden.

6.2. Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1. Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus **Anlage 3**. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

7.2. Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potenziellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von drei (3) Monaten zu kündigen.

7.3. Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

8. Rechte der betroffenen Personen

8.1. Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

8.2. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

8.3. Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

8.4. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren

und Erforderlichen Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1. Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen unterstützen.

9.2. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

10. Datenlöschung

10.1. Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

10.2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11. Nachweise und Überprüfungen

11.1. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

11.2. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

11.3. Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der 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 strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.

11.4. Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die

sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

11.5. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

11.6. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt.

11.7. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. Vertragsdauer und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

13. Haftung

13.1. Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsbegrenzungen gemäß des Hauptvertrages. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

13.2. Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern

freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. Schlussbestimmungen

14.1. Für Streitigkeiten aus diesem Vertrag gilt deutsches Recht. Erfüllungsort und ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers. Im Falle von Widersprüchen in den beiden Sprachfassungen hat die deutsche Fassung Vorrang.

14.2. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

14.3. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Anlagen:

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Weitere Auftragsverarbeiter

Anlage 1 - Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

1. Zweck, Art und Umfang der Datenverarbeitung

Der Auftragnehmer versendet im Auftrag des Auftraggebers vor und während dessen Leistungserbringung Nachrichten an dessen Endkunden, um Feedback zu erhalten, die Kommunikation zu verbessern, zu standardisieren und zu automatisieren. Die Ergebnisse werden im Auftrag des Kunden aufbereitet und ausgewertet. Hinzutreten Auswertungen aus indirektem und abgeleitetem Feedback, wie Informationen aus internen und/oder öffentlichen Quellen, um die Stimme des Endkunden vollständig abzubilden. Der Auftragnehmer aggregiert und anonymisiert die über die Plattform gesammelten Daten des Auftraggebers, um dem Auftraggeber zusätzliche Dienste wie Reporting, Benchmarking und KPI-Monitoring-Funktionen im Zusammenhang mit dem Feedback der Endkunden des Auftraggebers anzubieten.

2. Art der Daten

a) Stammdaten (z.B. Name, Geschlecht, Sprache);
b) Kontaktdaten (z.B. E-Mail-Adresse, Anschrift, Telefon-Nr.);
c) Kommunikationsdaten (z.B. E-Mail-Korrespondenz);
d) Vertragsdaten (z.B. Vertragsdauer, Informationen zur Leistungserbringung wie Umsatz od. Kosten);
e) Ggfs. vorhandene individuelle Segmentierungsdaten des Auftraggebers für dessen Kunden wie Weg des Vertragsschlusses (Internet, Telefon, etc.), Herkunftsland, Leistungskategorie oder Altersgruppe;
f) Feedback des Auftraggebers durch dessen Kunden (z.B. Kundenbewertung);
g) Zufriedenheitsanalysen (z.B. Text-, Themen-und Ausdrucksauswertungen).

3. Kategorien betroffener Personen

a) Personal des Kunden;
b) Endkunden des Kunden;
c) Supplier des Auftraggebers.

Anlage 2 - Technische und organisatorische Maßnahmen

Zum Schutz der personenbezogenen Daten sind nachfolgende technische und organisatorische Maßnahmen getroffen worden:

1. Zutrittskontrolle

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

Gewährleistet durch:

a) Festlegung von Sicherheitsbereichen und befugten Personen
b) Raumsicherung (Schlüssel, Rollo, etc.)
c) Anwesenheitsaufzeichnung
d) Außensicherung des Gebäudes (Zaunanlage, Sicherheitstüren/-fenster)
e) Sorgfalt bei Auswahl des Wachpersonals
f) Sorgfalt bei Auswahl der Reinigungsdienste
g) Videoüberwachung der Eingänge
h) Schlüsselverwaltung / Dokumentation der Schlüsselvergabe
i) Automatisches Zugangskontrollsystem
j) Chipkarten / Transpondersysteme
k) Manuelles Schließsystem
l) Sicherheitsschlösser
m) Türen mit Knauf (Außenseite)

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Gewährleistet durch:

a) Abschließbarkeit der Datenstation
b) Login mit Benutzername & Passwort u. Festlegungen zu deren Wechsel
c) Verschlüsselung der Passwörter
d) Anti-Virus-Software Server
e) Anti-Virus-Software Clients
f) Firewall
g) Mobile Device Management
h) Einsatz von VPN-Tunnel bei Remote-Zugriffen
i) Sperre externer Schnittstellen (USB)
j) Verschlüsselung von Notebooks / Tablets
k) Verwalten von Benutzerberechtigungen
l) Erstellen von Benutzerprofilen
m) Zentrale Passwortvergabe
n) Richtlinie ‘Sicheres Passwort’
o) Richtlinie ‘Löschen/ Vernichten’

p) Richtlinie ‘Datenschutz und Sicherheit’

3. Zugriffskontrolle

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.

Gewährleistet durch:

a) Benutzerspezifisch abgestufte Rechteverwaltung
b) Verwaltung von Benutzerrechte durch Administratoren
c) Minimale Anzahl an Administratoren
d) Dokumentation der Rechteverwaltung
e) Bildschirmverdunklung bei Arbeitsunterbrechung
f) Regelmäßige Sicherheitsupdates
g) Aktenschredder (mind. Stufe 3, cross cut)
h) Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten

4. Trennungskontrolle

Es ist dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

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

Gewährleistet durch:

a) Festlegung der Befugnisse für die Verarbeitung von Daten
b) Festlegung der zugelassenen Übermittlungsberechtigten, Übermittlungsempfänger und Übermittlungswege
c) Transportsicherung von Datenträgern
d) Gesichertes W-LAN

e) Regelungen zur Datenträgervernichtung
f) Verschlüsselung

6. Eingabekontrolle

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

Gewährleistet durch:
a) Verwaltung von Lese- / Schreibzugriff
b) Protokollierung der Lese- / Schreibzugriffe u. Programmaufrufe
c) Kennzeichnung von Erfassungsunterlagen mit Namen u. Datum nach Eingabe
d) Bestimmungen zur Veränderung von Zugriffsrechten u. zur Datenverantwortlichkeit
e) Klare Zuständigkeiten für Löschungen

7. Verfügbarkeitskontrolle

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

Gewährleistet durch:
a) Anlage von periodischen Sicherungskopien
b) USV-Schutz bei Stromausfall
c) Virenschutz/Firewall
d) Notfallplan
e) Ausfall- und Wiederherstellungspläne
f) Dauerhaft aktiver DDoS-Schutz

8. Auftragskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Gewährleistet durch:
a) Festlegung von Rechten u. Pflichten des Auftragnehmers
b) Vertrag zur Auftragsdatenverarbeitung
c) Schulung aller zugriffsberechtigten Mitarbeiter
d) Regelmäßige Datenschutzaudits
e) Vereinbarung von Kontroll- und Auditrechten

Anlage 3 – Weitere Auftragsverarbeiter			
Unternehmen, Adresse	**Service / Art der Verarbeitung**	**Rechtliche Abdeckung**	**Maßnahmen zur Gewährleistung eines vergleichbaren Schutzniveaus (nur in Drittländern)**
ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf Germany	Web-Hosting	Data Processing Agreement	/
CHARGEBEE INC., 340 S. Lemon Avenue, Suite #1537, Walnut, CA 91789 USA	Billing	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	3rd-party-certifications & audits; ISO 27001 certificate; SOC 1/SOC 2 and MFA standards; network, application and operational level security policies; AWS security setup - multiple certifications for data centers, including ISO 27001 compliance, PCI certification and SOC reports.
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA	Google Workspace Google Analytics	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	ISO-certificates (ISO 27001, 27017, 27018); Data Protection Guideline; Compliance Center & Reports.
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Germany	Hosting	Data Processing Agreement	/
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 USA	Inbound-Marketing and Sales	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	Binding Corporate Rules; Data Center (ISO 27001 certificate / SOC 2 audit); HTTPs encryption.

Intercom, Inc., 55 2nd Street, 4th Fl., San Francisco, CA 94105 USA	Live-Chat	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	External audits, pentests and bug bounties; SOC 2 audit; ISO 27001 certificate; HIPAA audit; AWS security setup; API and application endpoints are TLS/SSL only; security policy; security and awareness training.
Impala Travel Technology Ltd., 70 White Lion Street, London, N1 9PP UK	PMS-data-extraction (API)	Data Processing Agreement	Adequate protection of personal data in UK - EU Commission Implementing Decision as of June 28, 2021 - C(2021) 4800.
Mailgun Technologies, Inc., 548 Market Street, Suite 43099, San Francisco, CA 94101 USA	Email-provider (e-mail-API)	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	External network scan and penetration test; data encryption; intrusion detection; vendor management procedure - control and frequent auditing of all sub-processors.
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Office 365	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	External trust & audit reports; ISO 27001, 27017, 27018, 22301, 277701 certificates; data loss prevention policy; SSAE 18 SOC 1 Type II & SSAE 18 SOC 2 Type II compliant.
OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken Germany	Hosting	Data Processing Agreement	/
Scaling Technologies GmbH, Pfarrer-Hillmann-Weg 1, 51069 Köln Germany	Web Operations	Data Processing Agreement	/

Stripe, Inc. 510 Townsend Street San Francisco, CA 94103 USA	Payment Solution	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	Data encryption at rest and for data in transit - HTTPS for all services using TLS (SSL); all card numbers are encrypted at rest with AES-256; audit logs; access management policy; PCI Service Provider Level 1 certificate.
SugarCRM, Inc., 10050 N Wolfe Road, SW2-130 Cupertino, CA 95014 USA	Customer-Relation ship-Management	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	SOC II certificate; encryption for all passwords, key data and backups; all production and customer data is encrypted in transit and at rest; multifactor authentication; data loss prevention tools; hosted in Ireland (EU); AWS security setup - multiple certifications for data centers, including ISO 27001 compliance, PCI certification and SOC reports.
Twilio, Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105 USA	Provider for Short-Messages (SMS)	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	Binding Corporate Rules; security framework based on ISO 27001; ISO/IEC 27001, ISO/IEC 27017 & 27018, SOC 2 Type II, PCI DSS Level 1 certificates; AWS security setup - multiple certifications for data centers, including ISO 27001 compliance, PCI certification and SOC report; databases (customer data) are encrypted using the Advanced Encryption Standard and customer data is encrypted when in transit between customer's software application and the services using TLS v1.2; penetration testing; security incident management policies and procedures in accordance with NIST SP 800-61.