VERTRAG ZUR AUFTRAGSVERARBEITUNG

Vertragliche Rahmenparameter zur Auftragsverarbeitung der

kloud klickers GmbH

Edisonallee 11

89231 Neu-Ulm

Version: 1.0 | 2024

Inhalt

A) Präambel

1. Der Verantwortliche beauftragt den Auftragnehmer mit der Verarbeitung personenbezogener Daten unter Beachtung nachfolgender Regelungen.
2. Im Rahmen der Leistungserbringung nach dem Hauptvertrag ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten des Verantwortlichen umgeht. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Daten des Verantwortlichen zur Durchführung des Hauptvertrags.

B) Gegenstand und Dauer des Auftrags

1. Im Rahmen der Leistungserbringung nach dem **Hauptvertrag** ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten des Verantwortlichen umgeht. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Daten des Verantwortlichen zur Durchführung des Hauptvertrags.
   Der Auftrag umfasst ausschließlich die in Anhang 1 beschriebene Dienstleistung (= Gegenstand der Auftragstätigkeit). Art und Zweck der vorgesehenen Verarbeitung personenbezogener Daten sowie die Art der Daten und die Kategorien betroffener Personen ergeben sich aus Anhang 1 dieser Vereinbarung.

2. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Eine – auch nur teilweise - Verlagerung der Dienstleistung oder eine Auftragserfüllung außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums bedarf ebenfalls der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der Art 44 ff. DSGVO erfüllt sind.
3. Die Laufzeit bestimmt sich nach F).

C) Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Beurteilung der datenschutzrechtlichen Zulässigkeit der Auftragsverarbeitung gemäß Art. 6 Abs. 1 DSGVO, der Einhaltung von gesetzlichen Bestimmungen des Datenschutzes sowie für die Wahrung der Rechte der Betroffenen gemäß Art. 12 bis 22 DSGVO verantwortlich. Der Auftragnehmer ist verpflichtet, alle Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.

2. Der Verantwortliche erteilt alle Weisungen schriftlich oder in Textform. Er hat das Recht, dem Auftragnehmer Weisungen über Art, Umfang und Verfahren der Datenverarbeitung oder diesbezügliche Änderungen zu erteilen.
3. Der Verantwortliche informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
4. Der Verantwortliche ist verpflichtet, die für die Leistungserbringung erforderlichen Angaben, Daten und Datenbestände dem Auftragnehmer rechtzeitig in der im Einzelnen vereinbarten Form zur Verfügung zu stellen.
5. Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertrages bestehen.

D) Datengeheimnis, Vertraulichkeit der Daten

1. Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen sowie Datensicherheitsmaßnahmen des Verantwortlichen vertraulich zu behandeln. Diese Verpflichtung besteht auch nach Beendigung dieses Vertrages fort.
2. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor der Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und diese sich schriftlich zur Wahrung des Datengeheimnisses - auch nach der Beendigung ihres Beschäftigungsverhältnisses - verpflichtet haben. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften. Die Vertraulichkeitspflichten gelten auch nach Beendigung dieser Vereinbarung fort. Des Weiteren sichert der Auftragnehmer zu, seine Mitarbeiter auf die Folgen der Verletzung von Betriebs- und Geschäftsgeheimnissen hinzuweisen.
3. Der Auftragnehmer verwendet die zur automatisierten Datenverarbeitung überlassenen bzw. zur Verfügung gestellten personenbezogenen Daten für keine anderen, insbesondere keine eigenen Zwecke.

Datenträger, die vom Verantwortlichen stammen bzw. für diesen genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert. Ferner wird der Auftragnehmer die Daten des Verantwortlichen strikt von sonstigen Datenbeständen trennen.

4. Kopien oder Duplikate von personenbezogenen Daten (unabhängig in welcher Form diese vorliegen) werden nicht ohne Wissen und Genehmigung des Verantwortlichen erstellt. Unberührt bleibt die Herstellung von Backups, wenn die Anfertigung dieser erforderlich ist, um ordnungsgemäß die Daten zu verarbeiten oder gesetzliche Aufbewahrungspflichten zu erfüllen.

E) Pflichten des Auftragnehmers

1. Allgemeine Pflichten

   a) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

   b) Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer einen Datenschutzbeauftragten sowie wenn nötig einen Vertreter im Sinne des Art. 27 DSGVO. Als Datenschutzbeauftragter wird eine Person bestellt, die die gesetzlich vorgeschriebenen Voraussetzungen erfüllt. Die Kontaktdaten des Datenschutzbeauftragten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.

   c) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

   d) Auskünfte an Dritte oder an Betroffene darf der Auftragsnehmer nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen. Gleiches gilt für die Herausgabe von Datensätzen.

   e) Der Auftragnehmer ist verpflichtet, dem Verantwortlichen Kontrollen oder Ermittlungen durch Aufsichtsbehörden oder durch Revisoren/Prüfer unverzüglich mitzuteilen, sofern dies personenbezogene Daten des Auftraggebers betrifft.

   f) Soweit ein Betroffener seine Rechte nach der DSGVO oder anderer datenschutzrechtlicher Bestimmungen unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer

dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Er unterlässt es, eigenverantwortlich Auskünfte zu erteilen, es sei denn, der Verantwortliche hat ihn zuvor dazu aufgefordert.

g) Der Auftragnehmer unterstützt den Verantwortlichen bei einer anstehenden Datenschutzfolgenabschätzung sowie der Führung des Verzeichnisses von Verarbeitungstätigkeiten im notwendigen Umfang, sofern dies personenbezogene Daten des Verantwortlichen betrifft. Die hierzu notwendigen Angaben stellt er dem Verantwortlichen zur Verfügung.

h) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis unverzüglich zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

i) Der Auftragnehmer hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten des Verantwortlichen mitzuwirken. Er hat dem Verantwortlichen die erforderlichen Angaben und Dokumente auf Anfrage offen zu legen.

j) Der Auftragnehmer führt selbst ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung und beachtet hierbei die Vorgaben des Art. 30 Abs. 2 DSGVO.

2. Weitere Auftragnehmer

a) Die Beauftragung von weiteren Auftragnehmern zur Verarbeitung von Daten des Verantwortlichen ist dem Auftragnehmer nur mit Genehmigung des Verantwortlichen gestattet, Art. 28 Abs. 2 DSGVO, welche in Textform zu erfolgen hat.

b) Die Zustimmung kann nur dann erteilt werden, wenn der Auftragnehmer dem Verantwortlichen Namen und Anschrift sowie die vorgesehene Tätigkeit des weiteren Auftragnehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den weiteren Auftragnehmer unter Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die Dokumentation dazu ist dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.

c) Eine Beauftragung weiterer Auftragnehmer durch den Auftragnehmer in Drittstaaten darf nur dann erfolgen, wenn die besonderen Voraussetzungen des Art 44 ff. DSGVO erfüllt sind (bspw. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

d) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Verantwortlichem und Auftragnehmer auch gegenüber dessen weiteren Auftragnehmern gelten.

e) Der Vertrag mit dem weiteren Auftragnehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

f) Die Weiterleitung von Daten an den weiteren Auftragnehmer ist erst zulässig, wenn dieser die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat und der Auftragnehmer die Einhaltung dieser Pflichten durch den weiteren Auftragnehmer regelmäßig überprüft.

g) Der Auftragnehmer haftet gegenüber dem Verantwortlichen dafür, dass der weitere Auftragnehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

h) Der Auftragnehmer informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger nachgelagerter Auftragnehmer, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 Satz 2 DSGVO).

i) Nicht als weitere Auftragnehmer im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen i.d.R. z.B. Telekommunikationsleistungen oder Reinigungskräfte. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

j) Die vom Auftragnehmer bereits eingesetzten weiteren Auftragnehmer sind im Anhang 2 zu diesem Vertrag aufgeführt. Mit dem Einsatz dieser weiteren Auftragnehmer erklärt sich der Verantwortliche einverstanden.

k) Der Auftragnehmer hat die Einhaltung der Pflichten des jeweiligen weiteren Auftragnehmers zu überprüfen. Das Ergebnis der Überprüfung ist zu dokumentieren und dem Verantwortlichen auf Verlangen zugänglich zu machen.

3. Technische und organisatorische Maßnahmen

a) Der Auftragnehmer sichert dem Verantwortlichen zu, die für die beauftragte Tätigkeit erforderlichen technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes ergriffen zu haben und einzuhalten. Insbesondere wird zugesichert, dass der Auftragnehmer ein für die konkrete Auftragnehmer ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitung derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

b) Die beim Auftragnehmer hinsichtlich der beauftragten Tätigkeit relevanten technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO sind im Anhang 3 zu dieser Vereinbarung,

passend zum ermittelten Risiko unter der Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse aufgeführt.

c) Der Auftragnehmer stellt sicher, dass die eingeräumten Zugriffsrechte auf Systeme des Verantwortlichen nicht durch Unbefugte verwendet werden können sowie, dass Daten des Verantwortlichen nicht durch Unbefugte eingesehen werden können.

d) Der Auftragnehmer verpflichtet sich zu einer ausreichenden Datensicherung, soweit Daten des Verantwortlichen beim Auftragnehmer gespeichert werden. Insbesondere sichert der Auftragnehmer ausreichende Vorkehrungen gegen Datenverlust, Nichtverfügbarkeit und Verbreitung von Malware zu.

e) Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt: Zunächst wird der Schutzbedarf der personenbezogenen Daten, die verarbeitet werden, ermittelt (normal, hoch, sehr hoch). Die technischen und organisatorischen Maßnahmen werden anschließend unter Berücksichtigung des Risikos, das mit der Datenverarbeitung für die Rechte und Freiheiten der betroffenen Personen verbunden ist, ausgewählt. Das Risiko bestimmt sich nach der Schwere des möglichen physischen, materiellen oder immateriellen Schadens für die betroffene Person (vernachlässigbar, begrenzt, wesentlich, maximal) sowie der Wahrscheinlichkeit, dass ein solcher Schaden eintritt (vernachlässigbar, begrenzt, wesentlich, maximal).

f) Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer in dokumentierter Form abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

4. Pflichten des Auftragnehmers bei Verstößen gegen Vorgaben zum Datenschutz

a) Der Auftragnehmer unterrichtet den Verantwortlichen unverzüglich bei Störungen des Betriebsablaufs, bei Eintritt von oder Verdacht auf Verletzung datenschutzrechtlicher Vorschriften bzw. den in dieser Vereinbarung getroffenen Festlegungen sowie bei anderen Fehlern bzw. Unregelmäßigkeiten im Rahmen der Auftragsarbeiten für den Verantwortlichen. Gleiches gilt, wenn der Auftragnehmer feststellt, dass die bei ihm getroffenen technischen und organisatorischen Maßnahmen den gesetzlichen Anforderungen nicht genügen.

b) Die entsprechende Meldung des Auftragnehmers hat die Vorgaben aus Art. 33 Abs. 3 DSGVO zu berücksichtigen; er sichert ferner zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 oder 34 DSGVO angemessen zu unterstützen.

c) Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragnehmer nur nach vorheriger schriftlicher Weisung durchführen. Der Auftragnehmer wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen nach Überprüfung bestätigt oder geändert wird.

d) Bei Konsultationen der Aufsichtsbehörde wird der Verantwortliche seitens des Auftragnehmers unterstützt.

5. Kontrollpflichten

a) Der Auftragnehmer erklärt sich damit einverstanden, dass der Verantwortliche bzw. ein von ihm beauftragter Dritter während der üblichen Betriebs- und Geschäftszeiten und ohne Störung des Betriebsablaufs berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz, die Datensicherheit bzw. der vertraglichen Vereinbarungen sowie die Angemessenheit der zugesicherten technischen und organisatorischen Maßnahmen in den Geschäftsräumen des Auftragnehmer zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

b) Der Auftragnehmer sichert zu, dass er bei Erforderlichkeit bei diesen Kontrollen unterstützend mitwirkt.

c) Der Auftragnehmer verpflichtet sich, auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, Nachweise zu erbringen und Einsichtnahmen zu gewähren, die zur Durchführung einer Auftragskontrolle, bei der die Wirksamkeit technischer und organisatorischer Maßnahmen überprüft wird, erforderlich sind.

6. Wartungsarbeiten an IT-Systemen

Soweit der Auftragnehmer für den Verantwortlichen Wartungsarbeiten an IT-Systemen durchführt, gelten zusätzlich die folgenden Vereinbarungen:

a) Der Auftragnehmer darf im Rahmen der Wartung nur auf personenbezogene Daten des Verantwortlichen zugreifen, wenn dies für die Durchführung der Wartung erforderlich ist. Dem Auftragnehmer ist es bei der Wartung untersagt, personenbezogene Daten des Verantwortlichen auf eigenen Systemen oder Datenträgern zu speichern, es sei denn der Verantwortliche weist ihn hierzu an.

b) Fernwartungsarbeiten hat der Auftragnehmer dem Verantwortlichen im Vorfeld anzukündigen. Der Verantwortliche ist berechtigt, die Durchführung der Fernwartung mit zu verfolgen. Auf Anfrage und

soweit erforderlich, wirkt der Auftragnehmer an der Konfiguration technischer Kontrolleinrichtungen mit.

7. Löschung und Rückgabe von Daten

a) Eine Berichtigung, Löschung oder Sperrung von Daten erfolgt ausschließlich im Rahmen der schriftlichen Weisung des Verantwortlichen.

b) Test- und Ausschussmaterial ist durch den Auftragnehmer unverzüglich unter Einhaltung mindestens der Sicherheitsstufe P-4 der DIN 66399 (hinsichtlich etwaiger Schriftstücke) bzw. mindestens gemäß der Sicherheitsstufe H-4 bzw. T-4 der DIN 66399 (hinsichtlich magnetischer Datenträger) zu vernichten. Die Vernichtung der Daten wird nach Aufforderung des Verantwortlichen vom Auftragnehmer durch Zusendung eines geeigneten Nachweises bestätigt.

c) Sofern Daten(-sätze) des Verantwortlichen auf Systemen des Auftragnehmers gespeichert wurden, sind diese Daten(-sätze) nach Abschluss der jeweiligen Auftragstätigkeiten dem Verantwortlichen in einer migrationsfähigen Form auszuhändigen bzw. nach Weisung des Verantwortlichen unverzüglich zu löschen. Das Löschen der Daten(-sätze) hat so zu erfolgen, dass eine Rekonstruktion der Datensätze ausgeschlossen werden kann oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Auf Anfrage des Verantwortlichen hat der Auftragnehmer die Logdatei über den Löschvorgang vorzulegen. Der Verantwortliche bestätigt in Textform die Rückgabe der Daten in einem migrationsfähigen Format.

d) Nach Abschluss der jeweiligen Auftragsarbeiten hat der Auftragnehmer dem Verantwortlichen sämtliche in seinen Besitz gelangten Datensätze, die im unmittelbaren Zusammenhang mit dem Auftragsverhältnis stehen, weisungsgemäß zu löschen und dies im Falle der Löschung unter Angabe des Löschdatums schriftlich zu bestätigen.

e) Dem Auftragnehmer ist es untersagt, im Rahmen der Auftragsarbeiten verarbeitete personenbezogene Daten länger zu speichern, als dies mit dem Verantwortlichen schriftlich vereinbart ist.

f) Unterliegen vom Auftragnehmer zu Zwecken der Dokumentation der Auftragstätigkeiten angefertigte Unterlagen gesetzlichen Aufbewahrungspflichten, sind diese durch den Auftragnehmer bis zum Ablauf der geforderten Frist datenschutzrechtlich zu sperren.

F) Beginn und Ende des Vertrages, Vertragsstrafe

a) Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages.

b) Der Verantwortliche kann das Auftragsverhältnis jederzeit ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer in schwerwiegender Weise gegen die Bestimmungen dieses Vertrages oder gegen gesetzliche Bestimmungen verstößt, der Auftragnehmer eine Weisung des

Verantwortlichen nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schwerwiegenden Verstoß dar.

G) Schlussbestimmungen

a) Sofern der Verantwortliche besonderen oben nicht genannten Geheimnisschutzregeln unterliegt und er dies dem Auftragnehmer zu Vertragsbeginn schriftlich mitteilt, ist auch dieser verpflichtet, die Geheimnisschutzregelungen zu beachten.

b) Sollte das Eigentum des Verantwortlichen beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf die Datenträger und die Datenbestände des Verantwortlichen ausgeschlossen.

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

d) Sollten einzelne Teile des Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

e) Ergänzungen oder Änderungen zu diesem Vertrag unterliegen der Schriftform.

Ergänzende Regelungen zu dieser Vereinbarung

- **Anhang 1:** Auflistung der beauftragten Dienstleistungen (Art und Zweck der Verarbeitung, Art der Daten und Kategorien betroffener Personen)
- **Anhang 2:** Liste der vom Auftragnehmer beauftragten weiteren Auftragnehmer
- **Anhang 3:** Übersicht der beim Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

_____

Manuel Staiger, Geschäftsführer kloud klickers GmbH

Anhang 1: Auflistung der beauftragten Dienstleistungen (Art und Zweck der Verarbeitung, Art der Daten und Kategorien betroffener Personen)

Dienstleistung	Cloud Services mit Microsoft Azure
Art der personenbezogenen Daten	unternehmensbezogene Informationen (Zugehörigkeit zur Abteilung bzw. Position etc.)
Kategorien betroffener Personen	Mitarbeiter- und Unternehmensinformationen
Art und Zweck der Verarbeitung von Daten	Angebotserstellung, Deployment und Abwicklung von Managed Cloud Services, Abrechnung

Anhang 2: Liste der vom Auftragnehmer beauftragten weiteren Auftragnehmer

Weitere Auftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Art der Dienstleistung**
Zoho Corporation GmbH Trinkausstraße 7 40213 Düsseldorf	CRM-Lösung
Kajabi, LLC (HQ) 17100 Laguna Canyon Rd, #100, Irvine, California 92603	Softwarehersteller, Videoproduktion und Online-Kursen
Microsoft Ireland Operations Limited One Microsoft Place South County Business Park, Leopardstown, Dublin 18 D18 P521	Microsoft 365 inkl. Security-Lösungen, Microsoft Azure
mibeca GmbH Schillerstraße 1 29525 Uelzen	Vertriebsdienstleistung
IT sure GmbH Edisonallee 11 89231 Neu-Ulm	Marketing, Finanz- und Personaldienstleistung

Anhang 3: Übersicht der beim Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen

1. Vertraulichkeit

1.1 Zutrittskontrolle

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ verschlossener Empfang / Rezeption / Pförtner
☒ Chipkarten / Transpondersysteme	☒ Besucherbuch / Protokoll der Besucher
☒ Manuelles Schließsystem	☒ Abholung der Besucher und Begleitung durch Mitarbeiter
☒ Sicherheitsschlösser	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Schließsystem mit Codesperre	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Absicherung der Gebäudeschächte	☒ Anmeldung der Besucher bei der Aufsichtsperson
☒ Türen mit Knauf Außenseite	☒ Betretung des Betriebsgebäudes von Mitarbeitern und Reinigungspersonal nur durch Verwendung der Schlüssel
☒ Klingelanlage mit Kamera	☒ Zentrale Vergabe und Verwaltung der Schlüssel in einem Schlüsselausgabesystem
☒ Videoüberwachung der Eingänge	☒ Identifizierung jedes Schlüssels und seines Inhabers
	☒ Unverzügliche Entziehung der Schlüssel bei Entzug der Berechtigung

1.2 Zugangskontrolle

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Login mit biometrischen Daten	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Zentrale Passwortvergabe
☒ Anti-Virus-Software Clients	☒ Richtlinie „Sicheres Passwort“
☒ Verschlüsselung von Datenträgern	☒ Richtlinie „Löschen / Vernichten“
☒ Intrusion Detection Systeme (Defender)	☒ Hinweis an Mitarbeiter, dass bei Abwesenheit vom Arbeitsplatz, der jeweilige Bildschirm durch Eingabe einer Tastenkombination zu sperren ist
☒ Automatische Desktopsperre mit Passwortschutz	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Verschlüsselung von Notebooks / Tablet	☒ Nutzung von mobilen privaten Datenverarbeitungssystemen (z.B. Notebook, Tablet, Smartphone) unter Zugriff auf das Netzwerk des DSV (LAN oder WLAN) ist grundsätzlich nicht gestattet und nur mit vorheriger, schriftlicher Zustimmung der EDV-Abteilung zulässig.

☒ tägliche Vollsicherung (z. B. Zoho)	☒ Vergabe von Zugangsberechtigungen unter strenger Einhaltung der Funktionstrennung, um zu verhindern, dass sich eine Person selbst Rechte genehmigen und zuweisen kann

1.3 Zugriffskontrolle

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Bereichsspezifische Einschränkung der Zugriffe auf Datenbestände und Funktionen (Teilzugriffsmöglichkeit)	☒ Einsatz von Berechtigungskonzepten/ Festlegung der Befugnisse für Verarbeitung von Daten
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Erfordernis einer Zustimmung des Abteilungsleiters bei Änderungen von Zugriffsberechtigungen
	☒ Verwaltung Benutzerrechte durch Administratoren
	☒ Minimale Anzahl an Administratoren

1.4 Trennungskontrolle

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
	☒ Festlegung von Datenbankrechten

1.5 Pseudonymisierung

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
	☒ Alle mit der Verarbeitung personenbezogener Daten beauftragten Personen werden regelmäßig auf die Einhaltung der vorhandenen Regelungen geschult, um ihre Kenntnisse auf dem neuesten Stand zu halten.

2. Integrität

2.1 Weitergabekontrolle

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ E-Mail-Verschlüsselung	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Protokollierung der Zugriffe und Abrufe	
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
☒ Nutzung von Signaturverfahren	
☒ Sicherung der Datenverarbeitungssysteme mit Firewalls gegen Angriffe Dritter	

2.2 Eingangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung sowie aller Zugriffe auf Daten	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☒ Manuelle Kontrolle der Protokolle (bei Bedarf)	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☒ internes Dokumentationssystem (EDV-Dokuwiki)	☒ Klare Zuständigkeiten für Löschungen

2.3 Integritätsschutz

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Betriebssysteme auf allen Datenverarbeitungsgeräten auf dem aktuellen Stand	
☒ Regelmäßige Software-Updates (Sobald verfügbar)	
☒ Spam-Filter und Antivirenschutz im Mailserver	

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)/ Emergency-Response-Handbuch
☒ Recovery-Konzepte und Recovery-Routinen	☒ Kontrolle des Sicherungsvorgangs
☒ Regelmäßige Durchführung von Datensicherungen und Backup-Prozeduren (täglich, wöchentlich)	☒ Festlegungen zu Brandschutzbereichen und Kontrollen von Brandschutzmaßnahmen von der Feuerwehr

3.2 Belastbarkeitskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Backup & Recovery-Konzept
	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums (Azure)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Software-Lösungen für Datenschutz-Management im Einsatz	☒ Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☒ Die gesamte Kommunikation über die Internetseite nur über eine Transportverschlüsselung (z.B. HTTPS) verschlüsselt übertragen.	☒ Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
☒ Alle extern nutzbaren Internetseiten (z.B. Wiki, Cloud, WEbmailer) ausschließlich über HTTPS-gesicherte Verbindungen nutzbar machen.	☒ Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt (Arbeitsgruppe, keine explizit benannte interne Person)
☒ Einführung von Abteilungslaufwerken sowie Nutzung verschlüsselter Verbindungen	☒ Die Datenschutz-Folgenabschätzung (DSFA wird bei Bedarf durchgeführt)
☒ Transportverschlüsselte Verbindung der Clients zum Mailserver	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
☒ Externe Mailnutzung erfolgt nur über HTTPS-verschlüsselte Verbindungen, über den Webmailer oder TLS-Verschlüsselt über IMAPS bzw. ActiveSync	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
	☒ Beratung durch eine fachlich spezialisierte Rechtsanwaltskanzlei im Datenschutzrecht

4.2 Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Intrusion Prevention System (IPS) (Defender)	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ Intrusion Detection System (IDS) (Defender)	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
	☒ Schriftliche Weisungen an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Subunternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus