

Vereinbarung

--KUNDE --

- nachfolgend Auftraggeber genannt -

und

kantiko GmbH

Am Kiebitzberg 15

14532 Kleinmachnow

- nachfolgend Auftragnehmer genannt –

- gemeinsam auch „Parteien“ -

über

die Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

Präambel

Zwischen den Parteien besteht ein Auftragsverhältnis. Der Auftraggeber hat die Leistungen des Produktes kontool vom Auftragnehmer am **xx.xx.xxxx** beauftragt.

Diese Vereinbarung und ihre Anlagen konkretisieren die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus einer Auftragsdatenverarbeitung des Auftragnehmers für den Auftraggeber ergeben. Des Weiteren regelt sie die Mindestanforderungen zum Datenschutz und zur IT-Sicherheit, die durch den Auftragnehmer anzuwenden sind. Sie findet Anwendung auf alle Tätigkeiten, die mit einer Auftragsdatenverarbeitung in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen oder sonstigen Daten des Auftraggebers in Berührung kommen können.

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Auftragsverhältnisses, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

§ 1 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Finanzdaten des Kunden, die auf die Server von kontool übertragen und für ein webbasiertes Berichts- und Planungswesen gespeichert und aufbereitet werden. Hierbei werden lediglich Summen- und Salden aus der Buchhaltungssoftware übertragen.

Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (verantwortliche Stelle im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber jederzeit auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Herausgabe oder Löschung der Daten verlangen.

(3) Der Auftragnehmer erhält keine Zugriffsrechte zu den elektronischen Systemen und den Daten des Auftraggebers. Gleichwohl ist dem Auftragnehmer die Überprüfung der IT-Systeme des Auftraggebers für Kontroll- und Wartungszwecke in Notfällen sowie für beauftragte Aufgaben möglich.

§ 2 Leistungsgegenstand, Art, Zweck, Umfang, Art der Daten, Betroffene

(1) Die einzelnen Tätigkeiten und die Dauer des Auftrages sind im o.g. Vertrag konkretisiert.
Gegenstand der Vereinbarung:

- a) Verarbeitung von Geschäftszahlen, Finanz- und Buchhaltungsdaten zur Aufbereitung statistischer Auswertungen auf der Onlineplattform des Auftraggebers.

- (2) Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:
 - a) Der Auftragnehmer erhält keine Zugriffsrechte auf die Daten, die auf der untergebrachten Hardware des Auftraggebers liegen. Eine Verarbeitung von Metadaten für ausschließlich administrative Zwecke ist möglich.
- (3) Art der Daten:
 - a) Elektronisch gespeicherte Daten des Auftraggebers.
Bei der Art und Kategorien der gespeicherten Daten handelt es sich im Wesentlichen um Geschäftszahlen, Finanz- und Buchhaltungsdaten.
- (4) Kreis der Betroffenen:
 - a) Der Kreis der Betroffenen sind die Kunden des Auftraggebers sowie die in den Finanzdaten und buchhalterischen Informationen bzw. Auswertungen enthaltenen Kreditoren und Debitoren.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für ihn einschlägigen Datenschutzgesetze verantwortlich. Er darf die zur Auftragsdurchführung erforderlichen Daten ausschließlich nach der Weisung des Auftraggebers erheben, verarbeiten oder nutzen, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Weisungen des Auftraggebers bedürfen der Schriftform. Mündlich erteilte Weisungen sind zumindest per E-Mail zu bestätigen/dokumentieren. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Für die dadurch entstehenden Aufwände wird die Vergütungsregelung nach §10 angewendet.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. 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.

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

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Für alle nicht im Vertrag vereinbarten Aufwände und Einzelbeauftragungen wird die Vergütungsregelung nach §10 angewendet.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart. (Anmerkung: Im Vertrag können die Parteien hierzu eine Vergütungsregelung treffen.)

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Für die dadurch entstehenden Aufwände wird die Vergütungsregelung nach §10 angewendet.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

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

§ 5 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.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) 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.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung gemäß §10 verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine

Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Datenlöschung

(1) Überlassene Dokumente und Datenträger sowie Kopien derselben sind grundsätzlich nach Beendigung des Auftrags zurückzugeben. Der Auftraggeber kann auch vorher jederzeit die Herausgabe verlangen. Der Auftraggeber kann auch die Löschung bzw. Vernichtung von Dokumenten und Datenträgern sowie Kopien derselben verlangen.

(2) Soweit Daten vom Auftragnehmer berichtet, gelöscht oder gesperrt werden sollen, erfolgt dies ausschließlich auf Weisung des Auftraggebers. Die Vorgänge sind mit Angabe von Datum und durchführender Person zu protokollieren. Die Protokolle sind dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(3) Erfolgt eine Datenlöschung beim Auftragnehmer hat der Auftragnehmer sämtliche löschbaren elektronischen Datenträger, die Daten des Auftraggebers enthalten, datenschutzgerecht und nicht wieder herstellbar zu löschen.

§ 8 Kontrollrecht

(1) Der Auftraggeber kann sich nach rechtzeitiger Anmeldung zu Prüfzwecken in den Betriebsstätten - zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs - von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind.

§ 9 Unterauftragnehmer

1) Der Auftraggeber stimmt hiermit zu, dass der Auftragnehmer Unterauftragnehmer hinzuziehen darf, die in der Liste der zugelassene Unterauftragnehmer (siehe Anlage 2) aufgeführt sind.

(2) Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

§10 Vergütungsregelung

(1) Entstehen dem Auftragnehmer bei der Unterstützung des Auftraggebers im Hinblick auf Datenschutzfragen Aufwände, sind diese dem Auftraggeber in Rechnung zu stellen. Dazu wird ein Stundensatz von 150,00 Euro zzgl. MwSt. festgelegt.

§11 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) Es gilt deutsches Recht.

(5) Gerichtsstand ist Potsdam.

§12 Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Es wird darüber hinaus eine Haftungshöchstgrenze von 30.000,00 Euro vereinbart.

Auftraggeber

Auftragnehmer

Ort, Datum

Ort, Datum Kleinmachnow, 11. Februar 2026

Unterschrift

Unterschrift

KANTIKO

Am Kleinfeld 15
D - 14532 Kleinmachnow
Tel: +49 30 832 123 60
Fax: +49 30 809 292 10

Anlagen:

Anlage 1: Technische und organisatorische Maßnahmen (TOM)

Anlage 2: Verantwortliche Ansprechpartner

Anlage 3: Zugelassene Unterauftragnehmer

Anlage 1 Technische und organisatorische Maßnahmen

1. Technische und organisatorische Maßnahmen Hetzner Online GmbH

gemäß Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d) für den oben genannten Auftragnehmer.

Die nachstehenden Angaben beziehen sich auf die:

kantiko GmbH

Am Kiebitzberg 15
14532 Kleinmachnow
- Auftragnehmer -

Die Firma kantiko GmbH betreibt keine eigenen Server sondern hat die Datenhaltung- und -verarbeitung an ein externes TÜV-zertifiziertes Rechenzentrum mit Datenhaltung in Deutschland ausgelagert.

Bei dem Rechenzentrum handelt es sich um:

Hetzner Online GmbH
Industriestraße 25
91710 Gunzenhausen
- Rechenzentrum -

Der Auftragnehmer hat mit dem Rechenzentrum eine separate Vereinbarung zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO geschlossen.
Darin werden folgende Maßnahmen aufgeführt:

Kontrollziele gemäß Anlage zu Art. 28 DS-GVO: bezüglich Umgang mit personenbezogenen Daten	Beschreibung der technischen und organisatorischen Sicherungsmaßnahmen
Zutritt (Räume und Gebäude) <i>Zielbeschreibung:</i> Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.	• elektronisches Zutrittskontrollsystem mit Protokollierung • Hochsicherheitszaun um den gesamten Datacenter-Park • dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack) • Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude • 24/7 personelle Besetzung der Rechenzentren • Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen • Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
Zugang (IT-Systeme, Anwendungen)	für Dedicated Server, Colocation Server, Cloud Server und Storage Box • Server-Passwörter, welche nur vom Auftraggeber nach

<i>Zielbeschreibung:</i> Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind • Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.
Zugriffe (auf Daten) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, 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.	bei internen Verwaltungssystemen des Auftragnehmers • Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden. • Revisions-sicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers für Dedicated Server, Colocation Server, Cloud Server und Storage Box • Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
Eingabe (in Datenverarbeitungssysteme) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.	bei internen Verwaltungssystemen des Auftragnehmers • Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst. • Änderungen der Daten werden protokolliert. für Dedicated Server, Colocation Server, Cloud Server und Storage Box • Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
Weitergabe (von Daten) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	• Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen. • Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung. • Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt. • Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt. • Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).
Verfügbarkeit (von Daten) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	bei internen Verwaltungssystemen des Auftragnehmers • Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten. • Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter). • Einsatz von Festplattenspiegelung bei allen relevanten Servern. • Monitoring aller relevanten Server. • Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage. • Dauerhaft aktiver DDoS-Schutz. für Dedicated Server, Colocation Server, Cloud Server und Storage Box • Datensicherung obliegt dem Auftraggeber.

	• Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage. • Dauerhaft aktiver DDoS-Schutz. Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.
Datentrennung (zweckbezogen) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	bei internen Verwaltungssystemen des Auftragnehmers • Daten werden physisch oder logisch von anderen Daten getrennt gespeichert. • Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen. für Dedicated Server, Colocation Server, Cloud Server und Storage Box • Die Trennungskontrolle obliegt dem Auftraggeber.
Auftragsdatenverarbeitung (beim Einsatz von Subunternehmern) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass beim Einsatz von Subunternehmern durch den Auftragnehmer die Vorgaben des Auftraggebers umgesetzt werden.	Abschluss eines Vertrags zur Auftragsdatenverarbeitung (ADV) Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint. • Incident-Response-Management ist vorhanden. • Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO) • Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers. • Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers. • Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

2. Technische und organisatorische Maßnahmen Microsoft Ireland Operations, Ltd. (nur bei Nutzung des KI-Moduls / KI-Funktionalitäten in kontool)

gemäß Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d) für den oben genannten Auftragnehmer.

Die nachstehenden Angaben beziehen sich auf die:

kantiko GmbH

Am Kiebitzberg 15
14532 Kleinmachnow
- Auftragnehmer -

Die Firma kantiko GmbH betreibt keine eigenen Server für die KI - Funktionalitäten sondern hat die Datenhaltung- und -verarbeitung an ein externes TÜV-zertifiziertes Rechenzentrum mit Datenhaltung in der EU ausgelagert.

Bei dem Rechenzentrum handelt es sich um:

Microsoft Ireland Operations, Ltd.
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland
- Rechenzentrum -

Der Auftragnehmer hat mit dem Rechenzentrum eine separate Vereinbarung zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO geschlossen.

Die Nutzung von KI Sprachmodellen erfolgt als Teil des Services von Microsoft Azure. Mit dem Dienstleister wurden sämtliche verfügbaren zusätzlichen Abkommen und Einstellungsmöglichkeiten getroffen, um das Mitlesen und den Missbrauch der verarbeiteten Daten zu verhindern. Die betroffenen Daten werden außerdem ausdrücklich nicht zum Anlernen von KI des Unterauftragnehmers verwendet.

Darin werden folgende Maßnahmen aufgeführt:

Kontrollziele gemäß Anlage zu Art. 28 DS-GVO: bezüglich Umgang mit personenbezogenen Daten	Beschreibung der technischen und organisatorischen Sicherungsmaßnahmen
Zutritt (Räume und Gebäude) <i>Zielbeschreibung:</i> Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.	Die eingesetzte IT Infrastruktur wird vollständig auf ISO 27001-zertifizierten in Europa befindlichen Microsoft Azure Servern gehostet und betrieben. Microsoft beschränkt den Zugang zu Einrichtungen, in denen sich Informationssysteme befinden, die Kundendaten oder Professional Services-Daten verarbeiten, auf identifizierte, autorisierte Personen. Folgende Quellen bieten Ihnen umfangreiche weitere Informationen zu den implementierten Maßnahmen seitens Microsoft:

	https://learn.microsoft.com/de-de/azure/security/fundamentals/physical-security https://azure.microsoft.com/de-de/explore/trusted-cloud/ https://docs.microsoft.com/de-de/azure/compliance/
Zugang und Zugriffe (IT-Systeme, Anwendungen) <i>Zielbeschreibung:</i> Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Der Zugriff auf die in Microsoft Azure betriebene Infrastruktur ist nur über gesicherte Wege sowie Multi-Faktor-Authentifizierung und von bestimmten IP Adressen aus möglich. Des Weiteren führt Microsoft Aufzeichnungen über die ein- und ausgehenden Medien, die Kundendaten oder Professional Services-Daten enthalten, einschließlich der Art der Medien, des zugelassenen Absenders/Empfängers, des Datums und der Uhrzeit, der Anzahl der Medien und der darin enthaltenen Arten von solchen Daten. Folgende Quellen bieten Ihnen umfangreiche weitere Informationen zu den implementierten Maßnahmen seitens Microsoft: https://www.microsoft.com/de-de/trust-center https://azure.microsoft.com/de-de/explore/trusted-cloud/ https://docs.microsoft.com/de-de/azure/compliance/
Eingabe (in Datenverarbeitungssysteme) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.	Es sind Protokollierungen der Aktivitäten des IT-Systems selbst (Protokolle der Aktivitäten des Anti-Viren-Systems und/oder der Firewall) eingerichtet. Darüber hinaus sind Protokollierungsmaßnahmen bezüglich der Aktivitäten der IT-Administratoren und der Benutzer selbst eingerichtet.
Weitergabe (von Daten) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen. Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung. Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
Datentrennung (zweckbezogen) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Daten, die verschiedene Kunden/Auftraggeber betreffen und Daten die zu verschiedenen Zwecken verarbeitet werden, sind in geeigneter Weise durch kundenspezifische Ordner sowie Accounts und durch geeignete kundenspezifische Verschlüsselungs-Maßnahmen auf Anwendungsebene voneinander getrennt. Die Auftragnehmerin entwickelt überdies in einer lokalen Umgebung und testet im Anschluss auf dedizierten Development- und Staging-Umgebungen. Erst im Anschluss und nach dem Bestehen aller Qualitäts- und Sicherheitschecks wird an das separate Produktiv-System ausgeliefert.
Auftragsdatenverarbeitung (beim Einsatz von Subunternehmern) <i>Zielbeschreibung:</i> Es ist zu gewährleisten, dass beim Einsatz von Subunternehmern durch den Auftragnehmer die Vorgaben des Auftraggebers umgesetzt werden.	Die Nutzung von KI Sprachmodellen erfolgt als Teil des Services von Microsoft Azure. Wir verfügen über eine eigene Azure OpenAI-Instanz, die u.a. das ChatGPT-Modell beinhaltet, welche nicht der öffentlich verfügbaren Ressource von OpenAI entspricht. Mit dem Dienstleister wurden sämtliche verfügbaren zusätzlichen Abkommen

	und datenschutzfreundlichen Einstellungsmöglichkeiten getroffen, um unter anderem auch das Mitlesen und den Missbrauch der verarbeiteten Daten zu verhindern. Die betroffenen Daten werden außerdem ausdrücklich nicht zum Anlernen von KI des Unterauftragnehmers verwendet. Zur bestmöglichen Vorbeugung gegen eine mögliche Halluzination wurden entsprechende Einstellungen hinsichtlich der Kreativität gewählt. Folgende Quellen bieten Ihnen umfangreiche weitere Informationen zu den implementierten Maßnahmen bezüglich Microsoft als (Unter-)Auftragsverarbeiter und Azure OpenAI: https://learn.microsoft.com/de-de/legal/cognitive-services/openai/data-privacy https://learn.microsoft.com/de-de/legal/cognitive-services/openai/limited-access AVV Microsoft: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
--	---

3. Technische und organisatorische Maßnahmen Amazon Web Services EMEA SARL (nur bei Nutzung des KI-Moduls / KI-Funktionalitäten in kontool)

gemäß Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d) für den oben genannten Auftragnehmer.

Die nachstehenden Angaben beziehen sich auf die:

kantiko GmbH

Am Kiebitzberg 15
14532 Kleinmachnow
- Auftragnehmer -

Die Firma kantiko GmbH betreibt keine eigenen Server für die KI - Funktionalitäten sondern hat die Datenhaltung- und -verarbeitung an ein externes TÜV-zertifiziertes Rechenzentrum mit Datenhaltung in der EU ausgelagert.

Bei dem Rechenzentrum handelt es sich um:

Amazon Web Services EMEA SARL
38 avenue John F. Kennedy,
L-1855, Luxemburg
- Rechenzentrum -

Der Auftragnehmer hat mit dem Rechenzentrum eine separate Vereinbarung zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO geschlossen.

Die Nutzung von KI Sprachmodellen erfolgt als Teil des Services von Amazon AWS Bedrock. Mit dem Dienstleister wurden sämtliche verfügbaren zusätzlichen Abkommen und Einstellungsmöglichkeiten getroffen, um das Mitlesen und den Missbrauch der verarbeiteten Daten zu verhindern. Die betroffenen Daten werden außerdem ausdrücklich nicht zum Anlernen von KI des Unterauftragnehmers verwendet.

Darin werden folgende Maßnahmen aufgeführt:

Kontrollziele gemäß Anlage zu Art. 28 DS-GVO: bezüglich Umgang mit personenbezogenen Daten	Beschreibung der technischen und organisatorischen Sicherungsmaßnahmen
Zutritt	Die eingesetzte IT Infrastruktur wird vollständig auf ISO 27001-zertifizierten in Europa befindlichen Amazon AWS Servern gehostet und betrieben. Amazon beschränkt den Zugang zu Einrichtungen, in denen sich Informationssysteme befinden, die Kundendaten oder Professional Services-Daten verarbeiten, auf identifizierte, autorisierte Personen. Die Rechenzentren sind durch mehrstufige physische Sicherheitsmaßnahmen geschützt (z. B. Sicherheitszonen, Zutrittskarten, biometrische Verfahren). Der Zutritt nur für autorisiertes Personal nach dem Need-to-know-Prinzip.

	Es erfolgt eine permanente Überwachung (Videoüberwachung, Sicherheitspersonal, Protokollierung).
Zugang und Zugriffe	Der Zugriff auf die in Amazon AWS betriebene Infrastruktur ist nur über gesicherte Wege sowie Multi-Faktor-Authentifizierung und von bestimmten IP Adressen aus möglich. • Zugriff auf Systeme ausschließlich über individuelle Benutzerkonten. • Starke Passwort-Richtlinien und regelmäßige Überprüfung von Berechtigungen. • Zentrale Identitäts- und Zugriffsverwaltung (IAM). • Rollenbasierte Zugriffskonzepte (Role-Based Access Control). • Mandantentrennung (logische Isolation) zwischen Kunden. • Protokollierung und Überwachung von Zugriffen auf Daten und Systeme.
Eingabe	• Protokollierung von Änderungen an Daten und Systemkonfigurationen. • Nachvollziehbarkeit, wer Daten eingegeben, geändert oder gelöscht hat. • Einsatz von Monitoring- und Logging-Systemen.
Weitergabe	• Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung. • Verschlüsselung von Daten bei der Übertragung (z. B. TLS/HTTPS). • Kontrolle und Protokollierung von Datenexporten. • Einsatz sicherer Schnittstellen (APIs) mit Authentifizierung.
Datentrennung	• Logische Trennung der Daten verschiedener Kunden. • Mandantenfähige Systeme mit strikter Datenisolierung. • Trennung von Produktiv-, Test- und Entwicklungssystemen.
Verfügbarkeit und Belastbarkeit	Verfügbarkeitskontrolle • Hochverfügbare Infrastruktur mit redundanten Systemen. • Einsatz mehrerer Rechenzentren (Availability Zones). • Regelmäßige Backups und Notfallwiederherstellungspläne (Disaster Recovery). Schutz vor Verlust • Automatisierte Backup-Mechanismen. • Regelmäßige Tests von Wiederherstellungsverfahren. • Schutz vor DDoS-Angriffen und anderen Bedrohungen. Belastbarkeit • Skalierbare Infrastruktur zur Lastverteilung. • Kontinuierliche Überwachung der Systemleistung. • Automatische Fehlererkennung und -behebung.
Verschlüsselung und Pseudonymisierung	• Verschlüsselung von Daten im Ruhezustand (at rest). • Schlüsselmanagement über zentrale Key-Management-Systeme.

	• Unterstützung von kundenseitig verwalteten Schlüsseln.
Verfahren zur regelmäßigen Überprüfung	• Regelmäßige interne und externe Sicherheitsprüfungen. • Zertifizierungen und Prüfberichte (z. B. ISO/IEC 27001). • Kontinuierliche Verbesserung der Sicherheitsmaßnahmen.
Auftragskontrolle	• Verarbeitung personenbezogener Daten ausschließlich gemäß dokumentierter Weisung des Auftraggebers. • Verpflichtung der Mitarbeitenden auf Vertraulichkeit. • Einsatz von Unterauftragnehmern nur unter Einhaltung der DSGVO-Vorgaben.

Datenschutzmanagement	• Etabliertes Informationssicherheits- und Datenschutzmanagementsystem. • Benennung eines Datenschutzbeauftragten. • Schulungen und Sensibilisierungsmaßnahmen für Mitarbeitende.
Auftragsdatenverarbeitung	• Die Nutzung von KI Sprachmodellen erfolgt als Teil des Services von Amazon AWS Bedrock. Mit dem Dienstleister wurden sämtliche verfügbaren zusätzlichen Abkommen und datenschutzfreundlichen Einstellungsmöglichkeiten getroffen, um unter anderem auch das Mitlesen und den Missbrauch der verarbeiteten Daten zu verhindern. Die betroffenen Daten werden außerdem ausdrücklich nicht zum Anlernen von KI des Unterauftragnehmers verwendet. Zur bestmöglichen Vorbeugung gegen eine mögliche Halluzination wurden entsprechende Einstellungen hinsichtlich der Kreativität gewählt.

4. Technische und organisatorische Maßnahmen Google Ireland Limited (nur bei Nutzung des KI-Moduls / KI-Funktionalitäten in kontool)

gemäß Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d) für den oben genannten Auftragnehmer.

Die nachstehenden Angaben beziehen sich auf die:

kantiko GmbH

Am Kiebitzberg 15
14532 Kleinmachnow
- Auftragnehmer -

Die Firma kantiko GmbH betreibt keine eigenen Server für die KI - Funktionalitäten sondern hat die Datenhaltung- und -verarbeitung an ein externes TÜV-zertifiziertes Rechenzentrum mit Datenhaltung in der EU ausgelagert.

Bei dem Rechenzentrum handelt es sich um:

Google Ireland Limited
Gordon House
Barrow Street
Dublin 4
Irland
- Rechenzentrum -

Der Auftragnehmer hat mit dem Rechenzentrum eine separate Vereinbarung zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO geschlossen.

Die Nutzung von KI Sprachmodellen erfolgt als Teil des Services von Google Gemini. Mit dem Dienstleister wurden sämtliche verfügbaren zusätzlichen Abkommen und Einstellungsmöglichkeiten getroffen, um das Mitlesen und den Missbrauch der verarbeiteten Daten zu verhindern. Die betroffenen Daten werden außerdem ausdrücklich nicht zum Anlernen von KI des Unterauftragnehmers verwendet.

Darin werden folgende Maßnahmen aufgeführt:

Kontrollziele gemäß Anlage zu Art. 28 DS-GVO: bezüglich Umgang mit personenbezogenen Daten	Beschreibung der technischen und organisatorischen Sicherungsmaßnahmen
Zutritt	• Betrieb der Infrastruktur in gesicherten Rechenzentren mit mehrstufigen physischen Sicherheitsmaßnahmen. • Zutritt nur für autorisierte Personen. • Einsatz von Sicherheitspersonal, Zutrittsprotokollierung und Videoüberwachung.
Zugang und Zugriffe	Zugangskontrolle • Zugriff auf Systeme nur über personalisierte Benutzerkonten. • Einsatz starker Authentifizierungsverfahren (z. B. Mehrfaktor-Authentifizierung).

	- Regelmäßige Überprüfung und Einschränkung von Zugriffsrechten nach dem Need-to-know-Prinzip. Zugriffskontrolle - Rollen- und berechtigungsbasierte Zugriffskonzepte. - Logische Mandantentrennung zwischen Kunden. - Protokollierung und Überwachung von Zugriffen auf Systeme und Daten.
Eingabe	- Protokollierung von Änderungen an Systemen und Konfigurationen. - Nachvollziehbarkeit von Datenverarbeitungsvorgängen. - Einsatz von Monitoring- und Logging-Mechanismen.
Weitergabe	- Verschlüsselung personenbezogener Daten bei der Übertragung (z. B. TLS). - Zugriff auf Schnittstellen (APIs) nur nach Authentifizierung und Autorisierung. - Kontrolle und Protokollierung von Datenübertragungen.
Datentrennung	- Logische Trennung von Kundendaten. - Mandantenfähige Systemarchitektur. - Trennung von Produktiv-, Test- und Entwicklungssystemen.
Verfügbarkeit und Belastbarkeit	Verfügbarkeitskontrolle - Einsatz redundanter Infrastrukturkomponenten. - Nutzung verteilter Rechenzentren. - Notfallkonzepte zur Sicherstellung der Verfügbarkeit. Schutz vor Verlust - Regelmäßige Datensicherungen. - Maßnahmen zur Wiederherstellung bei Störungen oder Ausfällen. - Schutzmechanismen gegen Angriffe (z. B. DDoS). Belastbarkeit der Systeme - Skalierbare Infrastruktur zur Bewältigung von Lastspitzen. - Permanente Systemüberwachung. - Automatisierte Fehlererkennung und -behebung.
Verschlüsselung und Pseudonymisierung	- Verschlüsselung personenbezogener Daten im Ruhezustand (at rest). - Zentrales Schlüsselmanagement. - Unterstützung von Pseudonymisierungsmaßnahmen durch den Verantwortlichen.
Verfahren zur regelmäßigen Überprüfung	- Regelmäßige Sicherheitsüberprüfungen und Audits. - Einsatz standardisierter Sicherheits- und Datenschutzprozesse. - Kontinuierliche Weiterentwicklung der Sicherheitsmaßnahmen.
Auftragskontrolle	- Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. - Verpflichtung der Mitarbeitenden auf Vertraulichkeit. - Einsatz von Unterauftragnehmern nur unter Einhaltung datenschutzrechtlicher Vorgaben.
Datenschutzorganisation	Implementiertes Datenschutz- und Informationssicherheitsmanagement.

	• Benennung eines Datenschutzbeauftragten. • Regelmäßige Schulungen der Mitarbeitenden zu Datenschutz und Informationssicherheit.
Auftragsdatenverarbeitung	• Die Nutzung von KI Sprachmodellen erfolgt als Teil des Services Google Cloud gcp. Mit dem Dienstleister wurden sämtliche verfügbaren zusätzlichen Abkommen und datenschutzfreundlichen Einstellungsmöglichkeiten getroffen, um unter anderem auch das Mitlesen und den Missbrauch der verarbeiteten Daten zu verhindern. Die betroffenen Daten werden außerdem ausdrücklich nicht zum Anlernen von KI des Unterauftragnehmers verwendet. Zur bestmöglichen Vorbeugung gegen eine mögliche Halluzination wurden entsprechende Einstellungen hinsichtlich der Kreativität gewählt.

Anlage 2 zur Vereinbarung nach Art. 4 Nr. 7 DS-GVO

Liste der Ansprechpartner/Verantwortlichen

Verantwortliche und weisungsberechtigte Personen des Auftraggebers und Auftragnehmers.

Auftraggeber

Weisungsberechtigte Funktionen	Name	E-Mail	Tel.

Sonstige Funktionen	Name	E-Mail	Tel.

Auftragnehmer

Weisungsempfänger	Name	E-Mail	Tel.
Geschäftsführer	Stefan Jürgens	juergens@kantiko.com	+49 (0) 30 83212 360
Geschäftsführer	Benjamin Panke	panke@kantiko.com	+49 (0) 30 83212 360
Geschäftsführer	Mirko Behnken	behnken@kantiko.com	+49 (0) 30 83212 360

Sonstige Funktionen	Name	E-Mail	Tel.
Datenschutzbeauftragter	Mirko Behnken	behnken@kantiko.com	+49 (0) 30 83212 360
Leiter Entwicklung	Lukas Possegger	possegger@kantiko.com	+49 (0) 30 83212 360

Anlage 3 zur Vereinbarung nach Art. 28 Abs. 2-4 DS-GVO

Liste der zugelassenen Unterauftragnehmer

Nachstehend aufgeführte Unterauftragnehmer übernehmen für den Auftragnehmer Teilaufgaben des Auftrags.

Nr.	Firma, Adresse	Aufgabe	Ansprechpartner, Weisungsempfänger, Datenschutzbeauftragter	Kontaktdaten
1	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen	Hosting Dienstleister, eine separate ADV i.S. Art. 28 DS-GVO liegt vor und kann auf Anforderung nachgewiesen werden.	Geschäftsführer: Martin Hetzner, Stephan Konvickova, Günther Müller	Tel.: +49 9831 505-0 Fax: +49 9831 505-3 info@hetzner.com www.hetzner.com
2	Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	Nur bei Nutzung des KI-Moduls / KI-Funktionalitäten in kontool: Der Dienstleister stellt die Cloud-Lösung „Microsoft Azure“ mit OpenAI in dem Modul Foundry bereit, eine separate ADV i.S. Art. 28 DS-GVO liegt vor und kann auf Anforderung nachgewiesen werden.	Catherine Doyle	Tel. (Datenschutz): +353 1 706 3117. Adresse: 70 Sir John Rogerson's Quay, IRL-D02 Dublin, Ireland.
3	Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855, Luxemburg	Nur bei Nutzung des KI-Moduls / KI-Funktionalitäten in kontool: Der Dienstleister stellt die Cloud-Lösung „Amazon	aws-EU-privacy@amazon.com	Zentrale (Luxemburg): +352 26 73 30 00

		AWS“ bereit, eine separate ADV i.S. Art. 28 DS-GVO liegt vor und kann auf Anforderung nachgewiesen werden.		
4	Google Ireland Limited Gordon House Barrow Street Dublin 4 Irland	Nur bei Nutzung des KI-Moduls / KI-Funktionalitäten in kontool: Der Dienstleister stellt die Cloud-Lösung „Gemini“ bereit, eine separate ADV i.S. Art. 28 DS-GVO liegt vor und kann auf Anforderung nachgewiesen werden.	Kristie Chon Flynn	Tel: +353 1 543 1000 Data Protection Officer Google Ireland Limited Gordon House, Barrow Street Dublin 4 Irland

Vor Aufnahme der Tätigkeit ist die schriftliche Zustimmung durch den Auftraggeber einzuholen.