Auftragsverarbeitungsvertrag
(AVV)

Präambel

a) Diese Vereinbarung zur Auftragsverarbeitung („Vereinbarung“) wurde durch Bestätigung bei der Account-Registrierung durch den Verantwortlichen wirksam für beide Parteien abgeschlossen.

b) Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien gem. des jeweiligen Auftrags bzw. der AGB (Stand: 1. Februar 2026) (im Folgenden: „Hauptvertrag“). Teil der Durchführung des Hauptvertrages ist die Verarbeitung von personenbezogenen Daten des Verantwortlichen durch den Auftragsverarbeiter im Sinne der Datenschutz-Grundverordnung („DSGVO“).

c) Zur Erfüllung der Anforderungen der DSGVO, insbesondere des Art. 28 Abs. 3 DSGVO, haben die Parteien die nachfolgende Vereinbarung geschlossen.

ABSCHNITT I

Klausel 1: Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG sichergestellt werden.

b) Die in **Anhang I** aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß **Anhang II**.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2: Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3: Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten

Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4: Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 5: Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in **Anhang II** aufgeführt.

Klausel 6: Pflichten der Parteien

6.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

6.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in **Anhang II** genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

6.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in **Anhang II** angegebene Dauer verarbeitet.

6.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

6.6 Einsatz von Künstlicher Intelligenz (KI-Systemen)

a) Der Auftragsverarbeiter setzt zur Erbringung der vertraglich vereinbarten Leistungen Systeme ein, die auf Künstlicher Intelligenz (KI) basieren, insbesondere Sprach- und Embedding-Modelle. Die eingesetzten KI-Systeme und deren Anbieter sind in Anhang IV (Unterauftragsverarbeiter) aufgeführt.

b) Der Auftragsverarbeiter stellt sicher, dass personenbezogene Daten des Verantwortlichen sowie sonstige vom Verantwortlichen übermittelte Inhalte nicht für folgende Zwecke verwendet werden:
   - Training, Feinabstimmung (Fine-Tuning) oder sonstige Weiterentwicklung von KI-Modellen, die nicht ausschließlich dem Verantwortlichen zur Verfügung stehen;
   - Verbesserung allgemein verfügbarer KI-Dienste oder -Produkte des Auftragsverarbeiters oder dessen Unterauftragsverarbeiter;
   - Erstellung von Benchmarks, Analysen oder aggregierten Datensätzen, die Dritten zugänglich gemacht werden.

c) Der Auftragsverarbeiter gewährleistet, dass auch seine Unterauftragsverarbeiter, die KI-Systeme betreiben, vertraglich zur Einhaltung der Vorgaben gemäß Buchstabe b) verpflichtet sind. Der Auftragsverarbeiter wählt ausschließlich solche

KI-Dienste aus, bei denen eine Nutzung der übermittelten Daten zu Trainingszwecken vertraglich ausgeschlossen ist oder vom Auftragsverarbeiter deaktiviert wurde. Ausnahmen sind in **Anhang IV** inkl. Anlage klar gekennzeichnet.

d) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn ein Unterauftragsverarbeiter seine Nutzungsbedingungen dahingehend ändert, dass eine Verwendung übermittelter Daten zu Trainingszwecken nicht mehr ausgeschlossen werden kann. In einem solchen Fall hat der Verantwortliche das Recht, die Nutzung des betreffenden Dienstes zu untersagen, sofern eine technisch gleichwertige Alternative verfügbar ist.

6.7 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

6.8 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste (siehe **Anhang IV**) aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 2 Wochen im Voraus ausdrücklich in schriftlicher Form (E-Mail etc.) über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Zulässig ist nur der Einwand, dass der Einsatz des Unterauftragsnehmers nicht den Vorschriften der DSGVO entspricht. Erhebt der Verantwortliche keine Einwendungen innerhalb der Frist von zwei Wochen, so gilt der Unterauftragnehmer als genehmigt. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des

Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

6.9 Internationale Datenübermittlungen

a) Jede zukünftige Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder nach Benachrichtigung des Verantwortlichen zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

b) Der Verantwortliche erklärt sich vorbehaltlich der generellen Zustimmungspflicht nach Klausel 6.8 damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 6.8 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie (i) die jeweils aktuellen Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind sowie (ii) eine Risikoabschätzung vornehmen, um sicherzustellen, dass sie – ggfs. unter Berücksichtigung weiterer Maßnahmen - keine Zweifel an der Einhaltung europäischer Datenschutzstandards im Land des Datenimporteurs haben.

Klausel 7: Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 7 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

- Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
- Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
- Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
- Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 8: Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

8.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des

Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
   - die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
   - die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
   - die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

8.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in **Anhang III** alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 9:Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
   - der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
   - der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;
   - der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 6.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Klausel 10: Haftung

a) Die Haftung der Parteien im Zusammenhang mit dieser Vereinbarung richtet sich nach den Bestimmungen des Hauptvertrages (AGB für die octopusAI Plattform, Stand: 01.02.2026). Die dortigen Haftungsregelungen gelten entsprechend für Ansprüche aus oder im Zusammenhang mit der Verarbeitung personenbezogener Daten.

b) Ergänzend gilt: Im Innenverhältnis trägt diejenige Partei die Verantwortung für

einen Schaden, die den schadensursächlichen Verstoß gegen datenschutzrechtliche Bestimmungen oder vertragliche Pflichten zu vertreten hat.

Aschau im Chiemgau, 11.02.2026

Stephan Häuslschmid, Geschäftsführer
Tech Advisors GmbH

Ort, Datum

_____

Unterzeichner/in
Firmenname

ANHANG I – LISTE DER PARTEIEN

A. Verantwortlicher (Datenexporteur)

Name:	[Kundenname]
Adresse:	[Kundenadresse]
Ansprechpartner:	[Name, Funktion]
E-Mail:	[E-Mail]
Telefon:	[Telefon]

B. Auftragsverarbeiter (Datenimporteur)

Name:	Tech Advisors GmbH
Adresse:	Sonnwendstr. 1b, 83229 Aschau im Chiemgau
Ansprechpartner:	Stephan Häuslschmid
E-Mail:	datenschutz@tech-advisors.de
Registergericht:	Amtsgericht Traunstein, HRB 33989

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

1.1. Dauer der Vereinbarung

☒ Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages .

☒ Nach Beendigung des Vertrags werden alle Daten zurückgegeben oder gelöscht.

☒ Backups werden innerhalb von 60 Tagen nach Vertragsende gelöscht, sofern keine gesetzlichen oder vertraglichen Aufbewahrungspflichten (z. B. steuerrechtliche Vorgaben, Streitbeilegung) bestehen.

1.2. Art der Daten:

Im Rahmen der Nutzung der octopusAI Plattform können folgende personenbezogene Daten verarbeitet werden:

☒ Stammdaten der Nutzer (z.B. Namen, E-Mail Adressen, Rolle, Verzeichnisdienst-Daten, verschlüsselte Passwort-Hashes)

☒ Inhaltsdaten (insofern datenschutzrechtlich relevant)

☒ Nutzungsdaten & Analysedaten

☒ Konversationsverläufe und sonstige Eingaben (z.B Kommunikationspräferenzen)

☒ Dateien und sonstige Kontextinhalte (z.B. Daten aus Integrationen, Wissensmanagement)

☒ Meta-/Kommunikationsdaten (z.B. Geräte-IDs, IP-Adressen, Standortdaten)

1.3. Verarbeitung besonderer Kategorien von Daten (Art. 9 Abs. 1 DSGVO):

☒ Es werden keine besonderen Kategorien von Daten (z.B. Gesundheitsdaten) verarbeitet.

☐ Es werden grundsätzlich keine besonderen Kategorien von Daten verarbeitet, außer diese werden durch den Auftraggeber/seine Kunden, Nutzer oder Mitarbeiter, etc. der Verarbeitung zugeführt.

☐ Es werden folgende besondere Kategorien von Daten verarbeitet:

☐ Gesundheitsdaten

☐ Daten aus denen die politische Meinung, religiöse oder weltanschauliche Überzeugung oder Gewerkschaftszugehörigkeit hervorgeht

☐ Genetische Daten

☐ biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person

☐ Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

1.4. Kategorien der Betroffenen:

☒ Mitarbeitende des Verantwortlichen

☒ ggf. Dritte, wie zB Kunden und Geschäftspartner (insofern personenbezogene Daten von Nutzenden eingegeben werden oder durch Tool Integrationen angebunden werden)

1.5. Zweck der Verarbeitung:

☒ Betrieb und Bereitstellung der im Hauptvertrag vereinbarten Softwarefunktionen

☒ Weiterentwicklung, technische Optimierung und Fehleranalyse

☒ Einrichtung und Verwaltung des Nutzerkontos

☒ Identifizierung des Nutzers in der Anwendung

☒ Erbringung von Support- und Wartungsleistungen, Support-Kommunikation

☒ Authentifizierung beim Login

☒ Zustellung transaktionaler Nachrichten (z. B. Passwort-Reset)

☒ Anzeige der Konversationsverläufe für den Nutzer

☒ Abrechnungs- und Nachweiszwecke

☒ Speicherung und Analyse hochgeladener Dateien zur Bereitstellung der vom Nutzer angeforderten Funktionen (z. B. Wissensmanagement, Dokumenten- und Bildanalyse)

☒ Missbrauchserkennung und Sicherheitsüberwachung

☒ Beratungsleistungen

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

ERLÄUTERUNG:
Die technischen und organisatorischen Maßnahmen müssen konkret beschrieben werden; eine allgemeine Beschreibung ist nicht ausreichend.

Technische und Organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogenen und mindestens halbjährlich evaluiert wird.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.

- Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
- Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.

Zutrittskontrolle	Da keine eigenen Geschäftsräume betrieben werden (Remote-First), wird die Zutrittskontrolle über Homeoffice-Regelungen und die physische Sicherung von Arbeitsmitteln umgesetzt. Mitarbeitende verarbeiten personenbezogene Daten ausschließlich auf verwalteten Unternehmensgeräten. Arbeitsmittel und ggf. Papierunterlagen sind vor Zugriff Dritter zu schützen (abschließbare Aufbewahrung, Clean-Desk/Clean-Screen, keine Einsicht durch Haushaltsmitglieder/Besuch, keine Verarbeitung in öffentlichen Bereichen). Papierverarbeitung ist zu minimieren; erforderliche Ausdrucke werden sicher aufbewahrt und nach definiertem Prozess (DIN 66399) vernichtet oder zentral zurückgeführt. Ausgabe und Rücknahme von Geräten werden dokumentiert (Asset-Register).
Zugangskontrolle / Zugriffskontrolle	☒ Firewalls (Hardware/Software) ☒ Stets aktueller Virenschutz ☒ Stets aktuelle Softwareversionen (Arbeitsstationen und Server) ☒ Berechtigungs-/ Authentifizierungskonzepte mit auf Nötigste beschränkten Zugriffsregulierungen ☒ Mindestpasswortlängen und Passwortmanager ☒ Einsatz von VPN-Technologie ☒ Verschlüsselung von mobilen Datenträgern und Geräten
Weitergabekontrolle	☒ Festlegung und Dokumentation der Empfänger ☒ Pseudonymisierung bzw. Löschung von sensiblen Daten vor Weitergabe ☒ Verschlüsselung von Datenträgern und Verbindungen
Eingabekontrolle	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten
Auftragskontrolle	☒ Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten ☒ Kontrolle der Einhaltung bei Auftragnehmern ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
Verfügbarkeitskontrolle/ Integrität	☒ Notfallkonzept ☒ Backup- und Recoverykonzept
Gewährleistung des Zweckbindungs-/Trennungsgebotes	☒ Logische Mandantentrennung (softwareseitig) ☒ Trennung von Produktiv-, Entwicklungs- und Testsystemen

ANHANG IV - UNTERAUFTRAGSVERARBEITER

Name	**Amazon Web Services EMEA SARL**
Anschrift	38 Avenue John F. Kennedy, L-1855 Luxemburg, Luxemburg
Gegenstand der Verarbeitung	Betrieb von Sprach- und Embedding- und anderen KI-Modellen.
Art der Verarbeitung	Verarbeitung und Analyse von Profilinformationen, Konversationsverläufen und hochgeladenen Dokumenten und Tabellen zur Bereitstellung der Anwendung.
Serverstandort	EU
AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung.
Name	**Google Cloud EMEA Limited**
Anschrift	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Irland
Gegenstand der Verarbeitung	Betrieb von Sprach- und Embedding- und anderen KI-Modellen.
Art der Verarbeitung	Verarbeitung und Analyse von Profilinformationen, Konversationsverläufen und hochgeladenen Dokumenten und Tabellen zur Bereitstellung der Anwendung.
Serverstandort	EU
AVV liegt vor	Ja

Dauer der Verarbeitung	Dauer der Vertragsbeziehung.
Name	**Microsoft Ireland Operations Limited**
Anschrift	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
Gegenstand der Verarbeitung	Betrieb von Sprach- und Embedding- und anderen KI-Modellen.
Art der Verarbeitung	Verarbeitung und Analyse von Profilinformationen, Konversationsverläufen und hochgeladenen Dokumenten und Tabellen zur Bereitstellung der Anwendung.
Serverstandort	EU
AVV liegt vor	ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung.
Name	**Nebius B.V.**
Anschrift	Schiphol Boulevard 165, 1118 BG Schiphol, Niederlande
Gegenstand der Verarbeitung	Betrieb von Sprach- und Embedding- und anderen KI-Modellen.
Art der Verarbeitung	Verarbeitung und Analyse von Profilinformationen, Konversationsverläufen und hochgeladenen Dokumenten und Tabellen zur Bereitstellung der Anwendung.
Serverstandort	EU
AVV liegt vor	Ja

Dauer der Verarbeitung	Dauer der Vertragsbeziehung.
Name	**OpenAI Ireland Ltd,**
Anschrift	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43
Gegenstand der Verarbeitung	Betrieb von Sprach- und Embedding- und anderen KI-Modellen.
Art der Verarbeitung	Verarbeitung und Analyse von Profilinformationen, Konversationsverläufen und hochgeladenen Dokumenten und Tabellen zur Bereitstellung der Anwendung.
Serverstandort	EU
AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung
Name	**OpenAI, L.L.C.**
Anschrift	3180 18th Street, San Francisco, CA 94110, USA
Gegenstand der Verarbeitung	Betrieb von Sprach- und Embedding- und anderen KI-Modellen – global gehostete und entsprechend gekennzeichnete Modelle.
Art der Verarbeitung	Verarbeitung und Analyse von Profilinformationen, Konversationsverläufen und hochgeladenen Dokumenten und Tabellen zur Bereitstellung der Anwendung.
Serverstandort	USA, Datenübermittlung ist durch Standardvertragsklauseln (SCCs) gemäß Art. 46 DSGVO abgesichert.

AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung
Name	**Hetzner Online GmbH**
Anschrift	Industriestr. 25, 91710 Gunzenhausen, Deutschland
Gegenstand der Verarbeitung	Betrieb von Sprach- und Embedding- und anderen KI-Modellen und Speicherung persistenter Daten.
Art der Verarbeitung	Speicherung, Verarbeitung und Analyse von Profilinformationen, Konversationsverläufen und hochgeladenen Dokumenten und Tabellen zur Bereitstellung der Anwendung.
Serverstandort	EU
AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung**.**
Name	**Stripe Payments Europe, Limited**
Anschrift	3 Dublin Landings, North Wall Quay, Dublin 1, D01 C4E0, Ireland
Gegenstand der Verarbeitung	Abwicklung von Online-Zahlungen (Kreditkarte, Lastschrift etc.), Rechnungsstellung, Betrugsprävention und zugehörige Finanzdienstleistungen.
Art der Verarbeitung	Abwicklung von Online-Zahlungen und zugehörigen Finanzdienstleistungen. Dies umfasst insbesondere: • Prozessierung von Transaktionen • Tokenisierung von Zahlungsdaten

	• Betrugsprävention • Rechnungsstellung und Abonnement-Management • Kunden- und Zahlungsverwaltung • Reporting und Buchhaltung
Serverstandort	EU
AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung
Name	**Brave Software, Inc.**
Anschrift	580 California St., Suite 500, San Francisco, CA 94104, USA
Gegenstand der Verarbeitung	Websuche.
Art der Verarbeitung	Bereitstellung einer technischen Schnittstelle (API) zur Durchführung von Websuchen zur Anreicherung von KI-generierten Antworten
Serverstandort	USA - Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus: Abschluss eines Auftragsverarbeitungsvertrags (AVV) gemäß Art. 28 DSGVO inkl. EU-Standardvertragsklauseln (SCCs).
AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung
Name	**HubSpot, Inc. (als Hauptvertragspartner)** **HubSpot Germany GmbH (Support EU**)
Anschrift	HubSpot, Inc. Two Canal Park

	Cambridge, MA 02141 USA *sowie* HubSpot Germany GmbH Am Postbahnhof 17 10243 Berlin Deutschland
Gegenstand der Verarbeitung	Bereitstellung und Betrieb der CRM-Plattform "HubSpot" zur Verwaltung von Kundenkontakten sowie zum Versand von Marketing-E-Mails
Art der Verarbeitung	• Erhebung, Speicherung und Verwaltung von Kontakt- und Kundendaten • Hosting und Bereitstellung der CRM-Datenbank • Versand, Zustellung und Tracking von E-Mail-Kampagnen (Newsletter) • Protokollierung von Nutzerinteraktionen (Öffnungen, Klicks) • Bereitstellung von Analyse- und Reportingfunktionen • Technischer Support und Wartung der Plattform
Serverstandort	EU
AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung
Name	**Cloudflare Inc.**
Anschrift	101 Townsend Street, San Francisco, California 94107 United States
Gegenstand der Verarbeitung	Erbringung von Sicherheitsdienstleistungen (Web Application Firewall, DDoS-Schutz) und Content-Delivery-Network-Services (CDN) zur

	Gewährleistung der Sicherheit, Verfügbarkeit und Performance der Plattform.
Art der Verarbeitung	Verarbeitung von IP Adressen
Serverstandort	USA, Datenübermittlung ist durch Standardvertragsklauseln (SCCs) gemäß Art. 46 DSGVO abgesichert.
AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung
Name	**Atlassian Pty Ltd**
Anschrift	Level 6, 341 George Street Sydney NSW 2000 Australien
Gegenstand der Verarbeitung	Bereitstellung und Hosting der Cloud-Software "Jira Software" und "Jira Service Management" für internes Projektmanagement sowie Bearbeitung von Kunden-Support-Tickets
Art der Verarbeitung	Bearbeitung von Kunden-Support-Tickets
Serverstandort	EU
AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung
Name	**Requesty Ltd**
Anschrift	71-75 Shelton Street, Covent Garden London WC2H 9JQ

	Vereinigtes Königreich
Gegenstand der Verarbeitung	Betrieb von Sprach- und Embedding- und anderen KI-Modellen
Art der Verarbeitung	Verarbeitung und Analyse von Profilinformationen, Konversationsverläufen und hochgeladenen Dokumenten und Tabellen zur Bereitstellung der Anwendung.
Serverstandort	EU
AVV liegt vor	Ja
Dauer der Verarbeitung	Dauer der Vertragsbeziehung

Anlage zu Anhang IV: Detailinformationen zur Datenverarbeitung durch KI-Anbieter

Die nachfolgenden Informationen konkretisieren die Datenverarbeitung durch diejenigen Unterauftragsverarbeiter, die im Rahmen der octopusAI Plattform Systeme der Künstlichen Intelligenz (insbesondere Sprach- und Embedding-Modelle) betreiben.

Diese Informationen ergänzen die vertraglichen Verpflichtungen gemäß Klausel 6.6 dieses Vertrages und dienen der Transparenz gegenüber dem Verantwortlichen.

Alle genannten Zusicherungen basieren auf den zum Zeitpunkt der Vertragsunterzeichnung gültigen Nutzungsbedingungen, Produktbestimmungen und Auftragsverarbeitungsverträgen der jeweiligen Anbieter. Tech Advisors GmbH informiert den Verantwortlichen unverzüglich, sofern sich wesentliche Änderungen an diesen Bedingungen ergeben (vgl. Klausel 6.6d).

1. Microsoft Azure OpenAI Service

Anbieter	Microsoft Ireland Operations Limited
Anschrift	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
Dienst	Azure OpenAI Service (KI Modelle)

Vertragliche Grundlage

Tech Advisors GmbH hat mit Microsoft einen Kundenvertrag über die Nutzung der Azure Services geschlossen. Die Azure Services nutzt Tech Advisors auf Basis dieses Kundenvertrages sowie der *Produktbestimmungen für Azure*, die grundlegende Datenschutz- und Informationssicherheitspflichten von Microsoft enthalten.

Zusätzlich besteht ein *Auftragsverarbeitungsvertrag (Data Protection Addendum, DPA)* gemäß Art. 28 DSGVO, der die Datenverarbeitung durch Microsoft regelt.

Zusicherungen zur Datennutzung

Microsoft hat sich in den vertraglichen Vereinbarungen zu folgenden Punkten verpflichtet:

Datennutzung	Status	Grundlage
Weitergabe an andere Azure-Nutzer	Ausgeschlossen	DPA, Produktbestimmungen
Weitergabe an OpenAI oder andere Modellentwickler	Ausgeschlossen	Azure OpenAI Service Terms
Nutzung zum Training der Foundation Models	Ausgeschlossen	Azure OpenAI Service Terms
Nutzung zur Verbesserung anderer Microsoft-Dienste	Ausgeschlossen	Produktbestimmungen
Offenlegung oder Zugänglichmachung gegenüber Dritten	Ausgeschlossen	DPA

Konkret bedeutet dies: Sämtliche Prompts, Outputs, Embeddings und etwaige kundeneigene Trainingsdaten werden nicht (i) anderen Nutzern zur Verfügung gestellt, (ii) an OpenAI oder andere Modellentwickler weitergegeben, (iii) zum Training der Modelle genutzt oder (iv) zur Verbesserung anderer Microsoft-Services verwendet.

Speicherort und Datenverarbeitung

Aspekt	Details
Rechenzentrumsregion	EU
Ruhende Daten (data-at-rest)	Ausschließlich innerhalb der EU
Datenverarbeitung	EU, sofern nicht ein LLM gewählt wird, das ausschließlich "global" verfügbar und entsprechend gekennzeichnet ist.

Microsoft sichert in den Datenschutz- und Sicherheitsbestimmungen für Azure Core Services zu:

„Wenn der Kunde einen bestimmten Dienst derart konfiguriert, dass er in einem Rechenzentrum innerhalb einer Großregion (jeweils als ‚Geo' bezeichnet) bereitgestellt wird, speichert Microsoft die Kundendaten-at-rest innerhalb dieses bestimmten Geo."

Tech Advisors hat die Region EU konfiguriert.

Drittlandtransfer

Einzelne LLMs werden von Microsoft nur „global" bereitgestellt (siehe Kennzeichnung auf der Plattform, bzw. Möglichkeit, dass Admin dies von vornherein ausschließt). Bei diesen Modellen kann Microsoft Prompts und Vervollständigungen in jeder Azure Region weltweit verarbeiten.

Für solche Fälle gilt:

- *EU-Standardvertragsklauseln (SCCs)* wurden mit Microsoft vereinbart
- Microsoft ist unter dem *EU-US Data Privacy Framework* zertifiziert
- Ruhende Daten werden auch in diesen Fällen in der EU gespeichert

2. Amazon Web Services (AWS Bedrock)

Anbieter	Amazon Web Services EMEA SARL
Anschrift	38 Avenue John F. Kennedy, L-1855 Luxemburg, Luxemburg
Dienst	Amazon Bedrock (KI-Modelle)

Vertragliche Grundlage

Tech Advisors GmbH hat mit AWS einen Kundenvertrag geschlossen. Die AWS Bedrock-Services nutzt Tech Advisors auf Basis der *AWS Service Terms*.

Zusätzlich besteht ein *Auftragsverarbeitungsvertrag (Data Processing Addendum, DPA)* gemäß Art. 28 DSGVO, der die Datenverarbeitung durch AWS regelt.

Zusicherungen zur Datennutzung

AWS hat sich in den AWS Service Terms und dem DPA zu folgenden Punkten verpflichtet:

Datennutzung	Status	Grundlage
Nutzung zum Training der Foundation Models	Ausgeschlossen	AWS Service Terms, DPA
Nutzung zur Verbesserung anderer AWS-Dienste	Ausgeschlossen	AWS Service Terms
Speicherung oder Protokollierung von Prompts/Outputs	Ausgeschlossen	AWS Bedrock User Guide
Weitergabe an Dritte	Ausgeschlossen	DPA
Offenlegung gegenüber Dritten	Ausgeschlossen	DPA

Dies ist im AWS Bedrock User Guide wie folgt zusammengefasst:

„Amazon Bedrock doesn't store or log your prompts and completions. Amazon Bedrock doesn't use your prompts and completions to train any AWS models and doesn't distribute them to third parties."

Speicherort und Datenverarbeitung

Aspekt	Details
Rechenzentrumsregion	EU
Ruhende Daten (data-at-rest)	Ausschließlich innerhalb der Europäischen Union
Datenverarbeitung	EU, sofern nicht ein LLM gewählt wird, das ausschließlich "global" verfügbar und entsprechend gekennzeichnet ist

Drittlandtransfer

Standardfall (EU-Regionen): Sofern ein Foundation Model in der EU-Region verfügbar ist, findet die gesamte Datenverarbeitung innerhalb der EU statt. Ein Drittlandtransfer findet in diesem Fall nicht statt.

Ausnahmefall (Global gehostete Modelle): Einzelne Foundation Models werden von AWS nur in bestimmten Regionen außerhalb der EU bereitgestellt (z.B. ausschließlich in US-Regionen). Wenn der Verantwortliche ein solches Modell aktiv auswählt (siehe Kennzeichnung auf der Plattform, bzw. Möglichkeit, dass Admin dies von vornherein ausschließt) , kann AWS Prompts und Vervollständigungen in der jeweiligen Region weltweit verarbeiten.

Für solche Fälle gilt:

- *EU-Standardvertragsklauseln (SCC)* wurden mit AWS vereinbart
- AWS ist unter dem *EU-US Data Privacy Framework* zertifiziert
- Ruhende Daten werden auch in diesen Fällen in der EU gespeichert

3. Google Cloud (Vertex AI)

Anbieter	Google Cloud EMEA Limited
Anschrift	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Irland
Dienst	Google Cloud Vertex AI (KI-Modelle)

Vertragliche Grundlage

Tech Advisors GmbH hat mit Google Cloud einen Kundenvertrag geschlossen. Die Google Cloud Platform-Services nutzt Tech Advisors auf Basis der *Service Specific Terms*.

Zusätzlich besteht ein *Auftragsverarbeitungsvertrag (Data Processing Addendum)* gemäß Art. 28 DSGVO, der die Datenverarbeitung durch Google Cloud regelt.

Zusicherungen zur Datennutzung

Google hat sich in den Service Specific Terms zu folgenden Punkten verpflichtet:

Datennutzung	Status	Grundlage
Nutzung zum Training der Foundation Models	Ausgeschlossen	Service Specific Terms
Nutzung zur Verbesserung der KI/ML-Modelle	Ausgeschlossen	Service Specific Terms
Nutzung von Prompts/Antworten für Modelltraining	Ausgeschlossen	Google Cloud AI-Leitfaden
Nutzung von Trainingsdaten für Adaptermodelle	Ausgeschlossen	Google Cloud AI-Leitfaden

Google erklärt in seinem Leitfaden zu generativen AI-Produkten sowie in der Erklärung zu Datenschutzverpflichtungen für Cloud-basierte AI-Produkte:

„Kunden können die Foundation Models von Google Cloud verwenden, da sie sicher sein können, dass ihre Prompts, Antworten und alle Trainingsdaten für Adaptermodelle nicht zum Trainieren von Foundation Models verwendet werden."

Tech Advisors hat keiner abweichenden Nutzung zugestimmt.

Speicherort und Datenverarbeitung

Aspekt	Details
Rechenzentrumsregion	EU
Ruhende Daten (data-at-rest)	Ausschließlich in der vom Kunden gewählten Region/Multi-Region
Datenverarbeitung	EU, sofern nicht ein LLM gewählt wird, das ausschließlich "global" verfügbar und entsprechend gekennzeichnet ist

Google Cloud sichert in den Service Terms zu:

„Wenn der Kunde eine bestimmte Region oder Multi-Region als Datenstandort wählt, speichert Google die Kundendaten nur in dieser ausgewählten Region oder Multi-Region."

Tech Advisors hat die Region EU als primäre Region konfiguriert.

Drittlandtransfer

Nicht alle Foundation Models in Vertex AI sind in allen Google Cloud-Regionen verfügbar. Die Verfügbarkeit variiert je nach Modell:

Standardfall (EU-Regionen).

Sofern ein Foundation Model in der EU-Region verfügbar ist, findet die gesamte Datenverarbeitung innerhalb der EU statt. Ein Drittlandtransfer findet in diesem Fall nicht statt.

Ausnahmefall (Global gehostete Modelle):

Einzelne Foundation Models oder bestimmte Funktionen werden von Google Cloud nur in bestimmten Regionen außerhalb der EU bereitgestellt. Wenn der Verantwortliche ein solches Modell oder eine solche Funktion aktiv auswählt (siehe Kennzeichnung auf der Plattform, bzw. Möglichkeit, dass Admin dies von vornherein ausschließt), kann Google Prompts und Outputs in der jeweiligen Region weltweit verarbeiten.

Für solche Fälle gilt:

- *EU-Standardvertragsklauseln (SCC)* wurden mit Google vereinbart
- Google ist unter dem *EU-US Data Privacy Framework* zertifiziert
- Ruhende Daten werden auch in diesen Fällen in der EU gespeichert

4. Nebius B.V.

Anbieter	Nebius B.V.
Anschrift	Schiphol Boulevard 165, 1118 BG Schiphol, Niederlande
Dienst	KI-Modelle

Vertragliche Grundlage

Tech Advisors GmbH hat mit Nebius einen Kundenvertrag sowie einen *Auftragsverarbeitungsvertrag (DPA)* gemäß Art. 28 DSGVO geschlossen.

Zusicherungen zur Datennutzung

Datennutzung	Status	Grundlage
Nutzung zum Training der Modelle	Ausgeschlossen	Nutzungsbedingungen, DPA
Weitergabe an Dritte	Ausgeschlossen	DPA

Speicherort und Datenverarbeitung

Aspekt	Details
Rechenzentrumsregion	EU
Ruhende Daten (data-at-rest)	Ausschließlich innerhalb der EU
Datenverarbeitung	Ausschließlich innerhalb der EU

Drittlandtransfer

Ein Drittlandtransfer findet nicht statt.

5. OpenAI (API-Dienste) – EU Verarbeitung

Anbieter	OpenAI Ireland Ltd
Anschrift	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43
Dienst	OpenAI API (KI-Modelle)

Vertragliche Grundlage

Tech Advisors GmbH hat mit OpenAI Ireland Ltd einen *Kundenvertrag (Services Agreement)* geschlossen sowie einen *Auftragsverarbeitungsvertrag (Data Processing Addendum, DPA)* gemäß Art. 28 DSGVO vereinbart.

Für Kunden im EWR erbringt OpenAI die Services über die irische Niederlassung OpenAI Ireland Ltd. Die Datenverarbeitung für die als „EU“ gekennzeichneten Modelle für Tech Advisors erfolgt ausschließlich in der Europäischen Union.

Zusicherungen zur Datennutzung

OpenAI verarbeitet Kundendaten ausschließlich weisungsgebunden zu den vertraglich vereinbarten Zwecken:

Datennutzung	Status	Grundlage
Nutzung zum Training der Modelle	Ausgeschlossen	Services Agreement
Nutzung zur Verbesserung der Services	Ausgeschlossen (ohne explizite Zustimmung)	Services Agreement
Weitergabe an Dritte	Ausgeschlossen	DPA

Das OpenAI Services Agreement stellt hierzu klar:

„OpenAI will not use Customer Content to develop or improve the Services, unless Customer explicitly agrees to such use."

Tech Advisors hat keiner abweichenden Nutzung zugestimmt.

Zero Data Retention

Für Tech Advisors ist *Zero Data Retention* mit OpenAI gesondert vereinbart und aktiviert. Dadurch werden Kundendaten, die über die OpenAI-API übermittelt werden:

- nicht protokolliert
- nicht gespeichert
- nicht aufbewahrt

Die ansonsten üblichen 30-Tage-Aufbewahrungsfristen für API-Daten finden bei Tech Advisors keine Anwendung.

Speicherort und Datenverarbeitung

Aspekt	**Details**
Rechenzentrumsregion	EU
Ruhende Daten (data-at-rest)	Ausschließlich innerhalb der EU
Datenverarbeitung	Ausschließlich innerhalb der EU

Drittlandtransfer

Ein Drittlandtransfer findet nicht statt. Die gesamte Datenverarbeitung erfolgt innerhalb der EU durch OpenAI Ireland Ltd.

6. OpenAI (API-Dienste) – USA-Verarbeitung

Anbieter	OpenAI, L.L.C.
Anschrift	3180 18th Street, San Francisco, CA 94110, USA
Dienst	OpenAI API (KI-Modelle)

Vertragliche Grundlage

Tech Advisors GmbH hat mit OpenAI, L.L.C. einen Vertrag zur Nutzung der API-Dienste geschlossen sowie einen *Auftragsverarbeitungsvertrag (Data Processing Addendum, DPA)* gemäß Art. 28 DSGVO vereinbart.

Zusicherungen zur Datennutzung

Gemäß den von OpenAI veröffentlichten *Datenschutzgrundsätzen für Geschäftskunden und die API-Nutzung* verpflichtet sich OpenAI explizit zu folgenden Punkten:

Datennutzung	**Status**	**Grundlage**
Nutzung von API-Daten zum Training der Modelle	Ausgeschlossen (Standard)	OpenAI API Data Privacy

Nutzung zur Verbesserung der Modelle	Ausgeschlossen (Standard)	OpenAI API Data Privacy
Weitergabe an Dritte	Ausgeschlossen	DPA

Diese Zusagen gelten standardmäßig für alle API-Kunden. Tech Advisors hat keiner abweichenden Nutzung zugestimmt.

Datenaufbewahrung zur Missbrauchserkennung

Zur Erkennung und Verhinderung von Missbrauch können Daten für einen Zeitraum von maximal 30 Tagen aufbewahrt und danach automatisch gelöscht werden. Diese Aufbewahrung dient ausschließlich der Sicherheit und Integrität des Dienstes und nicht dem Modelltraining.

Speicherort und Datenverarbeitung

Aspekt	**Details**
Vertragspartner	OpenAI, L.L.C. (USA)
Unternehmenssitz	San Francisco, USA
Datenverarbeitung	USA

Drittlandtransfer

Da OpenAI, L.L.C. seinen Sitz in den USA hat, findet ein Drittlandtransfer statt. Dieser ist wie folgt abgesichert:

Schutzmaßnahme	**Status**
EU-Standardvertragsklauseln (SCCs)	Vereinbart (Bestandteil des DPA)
EU-US Data Privacy Framework	OpenAI ist zertifiziert

Die SCCs gewährleisten ein angemessenes Datenschutzniveau gemäß Art. 46 DSGVO.

6. Hetzner Online GmbH

Anbieter	Hetzner Online GmbH
Anschrift	Industriestr. 25, 91710 Gunzenhausen, Deutschland
Dienst	Hosting, Speicherung persistenter Daten, Betrieb von Sprach- und Embedding-Modellen

Vertragliche Grundlage

Tech Advisors GmbH hat mit Hetzner einen Kundenvertrag sowie einen *Auftragsverarbeitungsvertrag (AVV)* gemäß Art. 28 DSGVO geschlossen.

Zusicherungen zur Datennutzung

Hetzner stellt Infrastruktur (Server, Speicher) bereit und verarbeitet keine Inhalte der Kundendaten zu eigenen Zwecken.

Datennutzung	Status	Grundlage
Nutzung zu eigenen Zwecken	Ausgeschlossen	AVV
Weitergabe an Dritte	Ausgeschlossen	AVV

Speicherort und Datenverarbeitung

Aspekt	Details
Rechenzentrumsstandort	Deutschland (EU)
Datenverarbeitung	Ausschließlich innerhalb der EU

Drittlandtransfer

Ein Drittlandtransfer findet nicht statt. Hetzner betreibt alle relevanten Rechenzentren in Deutschland und Finnland (EU).

7. Brave Software, Inc. (Brave Search API)

Anbieter	Brave Software, Inc.
Anschrift	580 California St., Suite 500, San Francisco, CA 94104, USA
Dienst	Websuche (Brave Search API) zur Anreicherung von KI-generierten Antworten

Vertragliche Grundlage

Tech Advisors GmbH nutzt die Brave Search API auf Basis der Nutzungsbedingungen von Brave. Ein *Auftragsverarbeitungsvertrag (AVV)* gemäß Art. 28 DSGVO inkl. *EU-Standardvertragsklauseln (SCCs)* wurde abgeschlossen.

Art der Datenverarbeitung

Die Brave Search API wird verwendet, um Websuchen durchzuführen und Suchergebnisse in KI-generierte Antworten einzubinden. Dabei werden Suchanfragen (Queries) an Brave übermittelt. Diese können je nach Kontext personenbezogene Daten enthalten.

Zusicherungen zur Datennutzung

Datennutzung	Status	Grundlage
Speicherung von Suchanfragen zu Trainingszwecken	Nicht vorgesehen	Brave Privacy Policy

Weitergabe an Dritte	Ausgeschlossen	AVV

Speicherort und Datenverarbeitung

Aspekt	Details
Unternehmenssitz	USA
Datenverarbeitung	USA

Drittlandtransfer

Da Brave seinen Sitz in den USA hat, findet ein Drittlandtransfer statt. Dieser ist wie folgt abgesichert:

- *EU-Standardvertragsklauseln (SCCs)* gemäß Art. 46 DSGVO wurden vereinbart