

Anhang:

Vertrag über Auftragsverarbeitung gemäß Art. 28 DSGVO

§ 1 Geltung und Definitionen

- 1) Dieser Vertrag über eine Auftragsverarbeitung („**Vertrag**“) gilt ausschließlich im Geschäftsverhältnis der GO TO KI GmbH zu ihren Geschäftskunden („**Auftraggeber**“) und ergänzt den jeweils abgeschlossenen Projektvertrag und die Allgemeinen Geschäftsbedingungen der GO TO KI GmbH.
- 2) Im Falle eines Widerspruchs dieses Vertrags mit dem Projektvertrag oder den Allgemeinen Geschäftsbedingungen gilt dieser Vertrag vorrangig.
- 3) In diesem Vertrag verwendete Begriffe und Abwandlungen entsprechen denen, die in den Allgemeinen Geschäftsbedingungen der GO TO KI GmbH verwendet wurden, sofern nachstehend nicht abweichend oder ergänzend geregelt. Abweichend oder ergänzend kommen die folgenden Begriffe zur Anwendung:
 - „**Auftraggeber**“: Bezeichnet den Geschäftskunden, d. h. eine natürliche oder juristische Person, die die Dienstleistungen der GO TO KI GmbH in Anspruch nehmen möchte.
 - „**Auftragnehmer**“: Bezeichnet die GO TO KI GmbH, Schumannstraße 17, 10117 Berlin.
 - „**Projektvertrag**“: Bezeichnet den zwischen dem Auftraggeber und dem Auftragnehmer geschlossenen Vertrag über die Nutzung der Dienstleistungen der GO TO KI GmbH. Der Inhalt des Projektvertrags ergibt sich aus dem Rahmenvertrag und den hierzu vereinbarten Einzelaufträgen, ergänzt durch die Allgemeinen Geschäftsbedingungen.
 - „**Parteien**“: Gemeinsame Bezeichnung für den Auftraggeber und den Auftragnehmer.
 - „**Vertrag**“: Bezeichnet diesen Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DSGVO nebst seinen Anlagen.

§ 2 Gegenstand und Dauer des Auftrags

- 1) Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der Auftragsverarbeitung ergeben, die zum Zwecke der Erbringung der Leistungen aus dem Projektvertrag seitens des Auftragnehmers für den Auftraggeber durchzuführen ist. Der Gegenstand des Auftrags ergibt sich somit aus dem Projektvertrag, auf den hier verwiesen wird.

- 2) Darüber hinaus findet dieser Vertrag Anwendung auf alle Tätigkeiten, die mit den Tätigkeiten gemäß dem Projektvertrag im Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.
- 3) Dieser Vertrag tritt mit dem Zustandekommen des Projektvertrags in Kraft. Die Dauer dieses Vertrages entspricht der Laufzeit des Projektvertrags. Die Verpflichtungen aus diesem Vertrag gelten aber auch nach Beendigung des Projektvertrags weiter, solange der Auftragnehmer nicht sämtliche personenbezogenen Daten des Auftraggebers nach Maßgabe dieses Vertrages herausgegeben, gelöscht oder sonst vernichtet hat.

§ 3 Konkretisierung des Auftragsinhalts

- 1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im Projektvertrag. Änderungen der Verarbeitungsgegenstände und Verfahrensänderungen sind gemeinsam zwischen den Parteien abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
- 2) Der Auftragnehmer stellt in seinem Verantwortungsbereich die Einhaltung sämtlicher gesetzlicher Bestimmungen zum Datenschutz sicher.
- 3) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet primär in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Soweit der Auftragnehmer Unterauftragnehmer mit Sitz in einem Drittland einsetzt, die die im Auftrag verarbeiteten Daten des Auftraggebers (auch) in einem Drittland verarbeiten, trägt der Auftragnehmer dafür Sorge, dass in dem Drittland durch die dafür erforderlichen Maßnahmen im Sinne der Art. 44 ff. DSGVO ein angemessenes Datenschutzniveau sichergestellt ist.
- 4) Der Auftraggeber stimmt bereits jetzt einer Verlagerung einzelner Verarbeitungsprozesse in die in **Anlage 1** (Unterauftragnehmer) aufgeführten Drittländer zu. Für eine Übersicht, auf welche Weise in dem jeweiligen Drittland ein angemessenes Datenschutzniveau sichergestellt wird, wird auf **Anlage 1** (Unterauftragnehmer) verwiesen.
- 5) Gegenstand der vorliegenden Auftragsverarbeitung sind folgende Arten personenbezogener Daten:
 - Personenstammdaten (z. B. Name, Geburtsdatum, Adresse, Staatsangehörigkeit)
 - Kommunikationsdaten (z. B. Telefonnummer, E-Mail)
 - Audioeingaben von Nutzern, daraus generierte Texttranskriptionen und KI-generierte Antworten; diese können u.a. enthalten:

- Vertragsstammdaten (z. B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Mitarbeiterhistorie
- Terminwünsche/Terminabsprachen
- Vertragsabrechnungs- und Zahlungsdaten
- Interne Vermerke (z. B. Notizen in Bezug auf Anrufer)
- Gesundheitsdaten (z. B. Schwerbehinderung), Familienstand und/oder ethnische Herkunft, sofern diese Informationen aus der Kommunikation hervorgehen
- Metadaten (z. B. Zeitstempel, technische Logs)
- Berufliche Angaben (z. B. Titel, Fachrichtung, Arbeitgeber oder Praxis, berufliche Registernummer), auch aus öffentlich zugänglichen Quellen und Registern mit Fundstelle
- Antworten auf Befragungen (z. B. per E-Mail, Formular oder Telefon)
- Segmentzuordnungen (z. B. Segment, Konfidenz, zugrunde liegender Beleg)
- Werbeeinwilligungen und Widersprüche (z. B. Sperrvermerke)
- Nutzerkonten (z. B. Rolle, Mandantenzuordnung, Anmeldedaten)
- Inhalte, die Nutzer in Campaign OS einstellen oder dort erzeugen (z. B. Wissensbasis, Briefings, Kampagnenentwürfe)

6) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Endkunden des Auftraggebers
- Interessenten
- Lieferanten und sonstige Geschäftspartner des Auftraggebers
- Mitarbeiter und sonstige Ansprechpartner des Auftraggebers
- Personen, zu denen im Auftrag des Auftraggebers recherchiert wird oder die befragt werden (z. B. Angehörige der Fachkreise), sowie dabei erreichte Dritte (z. B. Praxispersonal)

§ 4 Technisch-organisatorische Maßnahmen

- 1) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den datenschutzrechtlichen Anforderungen gerecht wird. Er hat hierzu die Sicherheit der Datenverarbeitung gemäß Art. 28 Abs. 3 c), 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu

berücksichtigen. Die konkret vom Auftragnehmer getroffenen Maßnahmen sind in **Anlage 2** (Technische und Organisatorische Maßnahmen) aufgeführt.

- 2) Zum Nachweis der getroffenen Maßnahmen kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheits- oder Datenschutzaudit [z. B. nach BSI-Grundschutz]) vorlegen. Soweit ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- 3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 5 Weisungsbefugnis des Auftraggebers

- 1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen sowie die Verantwortung des Auftragnehmers als Auftragsverarbeiter bleiben hiervon unberührt.
- 2) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers nach Maßgabe der Regelungen des Projektvertrags. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen die Daten, die im Auftrag verarbeitet werden, nur nach dokumentierter Weisung des Auftraggebers erheben, verarbeiten und nutzen, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind (Art. 29 DSGVO). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt
- 3) Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate von Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Kopien von Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- 4) Der Auftraggeber erteilt Weisungen schriftlich oder in einem dokumentierten elektronischen Format (z. B. Textform). Grundsätzlich können Weisungen auch mündlich erteilt werden. Mündliche Weisungen sind jedoch unverzüglich vom Auftraggeber in dokumentierter Weise zu bestätigen (mindestens in Textform).

- 5) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftraggeber die Weisung bestätigt und den Auftragnehmer zur Durchführung dieser Weisung trotz dessen Bedenken im Hinblick auf eine mögliche Rechtswidrigkeit der Weisung anweist, wird der Auftraggeber den Auftragnehmer von allen Schäden und Kosten freistellen, die dem Auftragnehmer aufgrund der Durchführung dieser Weisung entstehen, falls die Weisung sich tatsächlich als rechtswidrig erweist und gegen den Auftragnehmer deshalb Ansprüche geltend gemacht oder ein Bußgeld verhängt werden sollten.

§ 6 Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- 1) Der Auftragnehmer hat, sofern er gesetzlich hierzu verpflichtet ist, einen Datenschutzbeauftragten schriftlich bestellt, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- 2) Der Auftragnehmer wird die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 b), 32 Abs. 4 DSGVO wahren. Zu diesem Zweck setzt der Auftragnehmer bei der Durchführung der Dienstleistungen gemäß dem Projektvertrag nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit fort.
- 3) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage der zuständigen Aufsichtsbehörde bei der Beantwortung dieser Anfrage zusammen.
- 4) Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- 5) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften angemessen zu unterstützen.

§ 7 Berichtigung, Einschränkung und Löschung von Daten, Betroffenenrechte

- 1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.
- 2) Sofern sich eine betroffene Person bezüglich der in Abs. 1 genannten Rechte oder zwecks Wahrnehmung ihrer weiteren Betroffenenrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und den Auftraggeber bei der Beantwortung der Anfrage im Rahmen seiner Möglichkeiten unterstützen.

§ 8 Unterauftragsverhältnisse

- 1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung aus diesem Vertrag beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer selbst z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- 2) Der Auftraggeber erteilt hiermit seine allgemeine Zustimmung zum Einsatz von Unterauftragnehmern durch den Auftragnehmer, soweit die nachfolgenden Voraussetzungen erfüllt sind, insbesondere jeweils eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO vorliegt.
- 3) Der Auftraggeber stimmt insbesondere der Beauftragung der im Zeitpunkt des Vertragsschlusses eingesetzten und in Anlage 1 (Unterauftragnehmer) aufgeführten Unterauftragnehmer zu.
- 4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an einen Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung, insbesondere einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DSGVO gestattet.
- 5) Der Einsatz bzw. der Wechsel von bestehenden Unterauftragnehmern ist zulässig, soweit:
 - a) der Auftragnehmer die Beauftragung eines neuen Unterauftragnehmers bzw. einen Wechsel (Austausch bzw. Ersetzung) von Unterauftragnehmern dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform (E-Mail

ausreichend) unter Angabe des geplanten Datums des Einsatzes bzw. Wechsels anzeigt und

- b) der Auftraggeber nicht bis zum Ablauf der vom Auftragnehmer in dieser Mitteilung genannten Frist (mindestens vierzehn Tage ab dem Datum des Erhalts der in lit. a genannten Informationen) gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen den geplanten Einsatz bzw. Wechsel erhebt und
 - c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DSGVO zugrunde gelegt wird.
- 6) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- 7) Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Datenverarbeitung durch die von ihm beauftragten Unterauftragnehmer wie für seine eigenen Leistungen unter diesem Vertrag.

§ 9 Kontrollrechte des Auftraggebers

- 1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, soweit diese Prüfer keine Wettbewerber des Auftragnehmers sind. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, bei anlassbezogenen Prüfungen aber jederzeit auch ohne vorherige Anmeldung, von der Einhaltung dieses Vertrages durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Betriebs- und Geschäftszeiten ohne Störung des Betriebsablaufes zu überzeugen.
- 2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen, die zur Durchführung einer Kontrolle erforderlich sind, und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- 3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
 - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).
- 4) Sollte eine Prüfung vor Ort beim Auftragnehmer durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, darf der Auftragnehmer die Prüfung von der vorherigen Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten Dritter sowie der sonstigen Geschäfts- und Betriebsgeheimnisse des Auftragnehmers abhängig machen. Die Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn die Prüfung durch eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde durchgeführt wird. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Die Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 10 Unterstützungspflichten des Auftragnehmers

- 1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der ihm obliegenden Pflichten bzgl. der Sicherheit der Verarbeitung personenbezogener Daten, Meldepflichten bei Datenschutzverletzungen, Durchführung von Datenschutz-Folgeabschätzungen und vorherigen Konsultationen (Art. 32 bis 36 DSGVO). Zu den Unterstützungsleistungen des Auftragnehmers gehören insbesondere
- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen (vgl. § 4 dieses Vertrages);
 - b) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden. Der Auftraggeber wird den Auftragnehmer daher unverzüglich und vollständig informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten mit datenschutzrechtlicher Relevanz feststellt. Darüber hinaus unterrichtet der Auftragnehmer den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen oder anderen die Daten des Auftraggebers betreffenden Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Der Auftragnehmer wird alle erforderlichen und ihm zumutbaren Maßnahmen zur Sicherung der betroffenen Daten und zur Minderung möglicher Nachteile des Auftraggebers ergreifen;

- c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber der Aufsichtsbehörde und ggf. gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
 - d) die Unterstützung des Auftraggebers im Rahmen einer etwaigen Datenschutz-Folgenabschätzung;
 - e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen der Aufsichtsbehörde.
- 2) Für Unterstützungsleistungen, die nicht im Projektvertrag enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

§ 11 Löschung und Rückgabe von personenbezogenen Daten bzw. Vernichtung

- 1) Nach Abschluss der vertraglich vereinbarten Dienstleistungen oder früher nach Aufforderung durch den Auftraggeber – spätestens jedoch mit Beendigung der Dienstleistungen aus dem Projektvertrag – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten bzw. die Daten zu löschen, soweit nicht berechtigte Gründe im Sinne von Art. 17 Abs. 3 DSGVO der Löschung entgegenstehen. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer ist verpflichtet, über die Herausgabe, Löschung von personenbezogenen Daten oder Vernichtung von Datenträgern einen Nachweis zu führen und diesen dem Auftraggeber auf dessen Verlangen vorzulegen.
- 2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 12 Haftung der Parteien

- 1) Der Auftragnehmer haftet für die Erfüllung seiner Pflichten aus diesem Vertrag nach den Bestimmungen des Projektvertrags. Die dort getroffene Haftungsvereinbarung erstreckt sich auch auf die Haftung für die Verletzung von Pflichten aus diesem Vertrag.
- 2) Im Verhältnis zu dem Betroffenen gelten die Regelungen zur Haftung in Art. 82 DSGVO. Die Parteien stellen sich jeweils von der Haftung gegenüber dem Betroffenen frei, wenn

eine Partei nachweist, dass sie nicht für den Umstand, durch den der Schaden bei dem Betroffenen eingetreten ist, verantwortlich ist.

§ 13 Sonstiges

- 1) Ein Zurückbehaltungsrecht an den im Rahmen des Auftrags verarbeiteten Daten gemäß § 273 BGB steht dem Auftragnehmer nicht zu.
- 2) 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 Verantwortlichem im Sinne der DSGVO liegen.
- 3) Ausschließlicher Gerichtsstand für alle Streitigkeiten im Zusammenhang mit diesem Vertrag ist Berlin, soweit nicht ein ausschließlicher gesetzlicher Gerichtsstand besteht.
- 4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.
- 5) Bestandteil dieses Vertrages werden folgende Anlagen:
 - **Anlage 1** – Unterauftragnehmer
 - **Anlage 2** – Technische und organisatorische Maßnahmen

Anlage 1 – Unterauftragnehmer

Firma Unterauftragnehmer	Leistung	Land / Ort der Datenverarbeitung	Sicherstellung des angemessenen Datenschutz-niveaus
ElevenLabs	Spracherkennung (Speech-to-Text) Generierung von Sprachantworten aus Text (Text-to-Speech)	USA	Zertifizierung unter dem EU-U.S. Data Privacy Framework
Deepgram	Spracherkennung (Speech-to-Text)	USA	Abschluss von EU- Standardvertragsklauseln
Microsoft Ireland Operations Limited, Dublin, Irland (Dienst: Azure OpenAI in Microsoft Foundry)	Verarbeitung von Texteingaben, Generierung von Antworten und Erzeugung von Text- Einbettungen (Embeddings) mittels folgender Modelle von Azure OpenAI: gpt-6.1-sol, gpt-6- sol, gpt-6-luna, gpt-5.6-sol, gpt-5.6-terra, gpt- 5.6-luna, gpt-5.5, gpt-5.4, gpt-5.4-mini, gpt-5.4- nano, gpt-4o; Embeddings: text-embedding-3- large, text-embedding-3-small, text-embedding- ada-002. Erfasst sind auch Nachfolgeversionen dieser Modellfamilien, soweit sie in denselben Bereitstellungsarten (Spalte 3) eingesetzt werden.	EU/EWR und Schweiz: Verarbeitung ausschließlich in den Azure- Bereitstellungsarten „Data Zone“ (EU) oder „Standard“ bzw. „Regional Provisioned“ in einer Azure-Region in der EU; die Data Zone EU folgt der Microsoft EU Data Boundary. Bereitstellungsarten mit globaler Verarbeitung („Global“) werden nicht eingesetzt. Speicherung im Ruhezustand in der Region der Azure- Ressource (Germany West Central, Deutschland; Sweden Central, Schweden.)	Verarbeitung innerhalb der EU/des EWR; soweit Verarbeitung in der Schweiz: Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO, Entscheidung 2000/518/EG). Vertragliche Grundlage: Microsoft Products and Services Data Protection Addendum.
Pipecat Cloud (Daily, Co.)	Orchestrierung und Ausführung der Voice- Agent-Pipeline	USA, aber Serverstandorte innerhalb Deutschlands/EU	n/a, im Übrigen: Zertifizierung unter dem EU-U.S. Data Privacy Framework
Amazon Web Services (AWS)	Hosting der Plattform	Deutschland/EU	n/a

Firma Unterauftragnehmer	Leistung	Land / Ort der Datenverarbeitung	Sicherstellung des angemessenen Datenschutz-niveaus
Amazon Web Services EMEA SARL, Luxemburg (Dienst: Amazon Bedrock)	Verarbeitung von Texteingaben und Generierung von Antworten mittels der Sprachmodelle Claude Opus 5.5 und Claude Sonnet 5.5 (Anbieter der Modelle: Anthropic; Betrieb ausschließlich durch AWS, ohne Zugriff von Anthropic auf Eingaben und Antworten). Erfasst sind auch Nachfolgeversionen dieser Modellfamilien, soweit sie über dasselbe EU-Inferenzprofil eingesetzt werden.	EU/EWR, Schweiz und Vereinigtes Königreich: Verarbeitung ausschließlich über die EU-Inferenzprofile von Amazon Bedrock (Kennung „eu.“); globale Inferenzprofile („global.“) werden nicht eingesetzt.	Verarbeitung innerhalb der EU/des EWR; soweit Verarbeitung in der Schweiz oder im Vereinigten Königreich: Angemessenheitsbeschlüsse der EU-Kommission (Art. 45 DSGVO). Vertragliche Grundlage: AWS Data Processing Addendum.
Google Firebase	Anmeldung und Nutzerverwaltung	USA	Zertifizierung unter dem EU-U.S. Data Privacy Framework
Google Cloud	Hosting von Campaign OS	EU	n/a
Vercel	Hosting der Weboberfläche von Campaign OS	USA, aber Serverstandorte innerhalb Deutschlands/EU	Abschluss von EU-Standardvertragsklauseln
Twilio	Telefonie (Rufnummern, Gesprächsverbindung, Gesprächsaufzeichnung)	USA	Zertifizierung unter dem EU-U.S. Data Privacy Framework

Anlage 2 – Technische und organisatorische Maßnahmen

1. Vertraulichkeit

(a) Zutrittskontrolle:

- **Technische Maßnahmen:** Manuelles Schließsystem, Schließsystem mit Codesperre, Sicherheitsschlösser, Außentüren mit Sicherheitsbeschlägen, Türen mit Knauf an der Außenseite, Videoüberwachung des Gebäudes/Eingangs.
- **Organisatorische Maßnahmen:** Prozess einer Alarmierungskette, Schlüssel-/Transponder-Regelung, Besucherbegleitung durch Mitarbeiter, sorgfältige Auswahl der Reinigungsdienste, Richtlinien zum Verschluss von Büroräumen.

(b) Zugangskontrolle:

- **Technische Maßnahmen:** Login mit Benutzername + Passwort, Login mit biometrischen Daten, Zwei-Faktor-Authentifizierung, Antivirensoftware Server, Antivirensoftware Clients, Antivirensoftware mobile Endgeräte, Hardware-Firewall, Intrusion Detection Systeme, Remote-Zugriff über verschlüsseltes VPN, verschlüsselte Datenträger, verschlüsseltes Notebook/Tablet, automatische Desktopsperre, Sperre von Schnittstellen (USB, Firewire etc.).
- **Organisatorische Maßnahmen:** Einsatz einer Passwortrichtlinie, Abstufung der Berechtigungen je nach Aufgabenstellung, Zuordenbarkeit von Benutzerprofilen zu Personen, Beschränkung der Zugangsrechte auf die Daten, die notwendig sind, automatische Bildschirmsperre, Benutzersperrung nach mehrfacher falscher Passwordeingabe, minimale Anzahl von Administratoren, Erlass einer Richtlinie zur Nutzung von Telearbeitsplätzen zur Gewährleistung des gleichen Sicherheitsniveaus wie in den Betriebsräumen des Auftragnehmers, zentrale Passwortvergabe, Richtlinie „Löschen/Vernichten“, Richtlinie „Clean Desk“, Mobile Device Policy.

(c) Zugriffskontrolle:

- **Technische Maßnahmen:** Protokollierung von Zugriffen auf Daten, Protokollierung von Zugriffen auf Anwendungen, physische Löschung von Datenträgern.
- **Organisatorische Maßnahmen:** Einsatz von Berechtigungskonzepten, Verwaltung und Überprüfung der Benutzerrechte durch Administratoren, Prozess zum Entzug von Berechtigungen nach Ausscheiden des Mitarbeiters, Prozess zur Anpassung von Berechtigungen nach internem Wechsel des Arbeitsplatzes, minimale Anzahl von Administratoren, Erlass einer Richtlinie zur Nutzung von Telearbeitsplätzen zur Gewährleistung des gleichen Sicherheitsniveaus wie in den Betriebsräumen des Auftragnehmers.

(d) Daten-Trennung:

- **Technische Maßnahmen:** Trennung von Testumgebung und Produktivsystem, physikalische Systemtrennung (Fileserver, Datenbanken, Applikationen), mandantenfähige Anwendungen.
- **Organisatorische Maßnahmen:** Einsatz von Berechtigungskonzepten, Einsatz von Datenbankberechtigungen, Zweckattribute für Datensätze.

(e) Pseudonymisierung und Verschlüsselung von Daten:

- **Technische Maßnahmen:** Pseudonymisierung von Daten mittels Trennung von zuordenbaren Merkmalen zu den personenbezogenen Daten in getrennten Systemen möglich.
- **Organisatorische Maßnahmen:** Interne Richtlinien zur Anwendung der Pseudonymisierung.

2. Integrität

(a) Eingabekontrolle:

- **Technische Maßnahmen:** Protokollierung bei Eingabe, Änderung und Löschung von Daten, manuelle oder automatisierte Kontrolle der Protokolle.
- **Organisatorische Maßnahmen:** Prozess zur Kontrolle der Protokollierung, Prozess zur Aufbewahrung der Protokolldateien, Zugriffsregelung zu den Protokollen, Liste der Anwendungen, mit denen Daten eingegeben, geändert oder gelöscht werden, Zuordenbarkeit von Benutzernamen zu Eingabe, Änderung und Löschung von Daten, Zuweisung von Berechtigungen zur Eingabe, Änderung und Löschung von Daten.

(b) Weitergabekontrolle:

- **Technische Maßnahmen:** E-Mail-Transportverschlüsselung (TLS 1.2 oder 1.3), transportverschlüsselte Datenleitung (wie sftp, https), VPN Tunneling von Datenleitungen (Home-Office, Remote-Standorte), Verschlüsselung von mobilen Datenträgern, Signaturverfahren, Protokollierung von Datenzugriffen, -abruf, -transport, sichere Transportbehälter für mobile Datenträger.
- **Organisatorische Maßnahmen:** Kontrolle der Zugriffsprotokolle, Datenweitergabe in anonymisierter Form, Dokumentation der Empfänger von Daten sowie der Dauer der geplanten Überlassung bzw. der Löschfristen, Richtlinie zur Nutzung von mobilen Datenträgern, Prozess zur Kontrolle der Protokollierung, Protokollierung der persönlichen Übergabe von Daten, Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen.

3. Verfügbarkeit und Belastbarkeit

- **Technische Maßnahmen:** Brand- und Rauchmeldeanlage, Serverraum Überwachung auf Temperatur und Feuchtigkeit, Feuerlöscher im Serverraum, klimatisierter Serverraum, Überschwemmungsschutz, Einsatz USV, Serverstromnetz getrennt vom restlichen Stromnetz, Einsatz Schutzkontaktsteckdosen, RAID-System/Festplattenspiegelung, Datenschutztresor (S60/S120 DIS), gesonderte Alarmanlage im Serverraum, redundante Datenhaltung/-sicherung in getrennten Brandschutzzonen, getrennte Partitionen für Betriebssystem und Peripheriedaten, Videoüberwachung Serverraum.
- **Organisatorische Maßnahmen:** Einsatz Datensicherungs- und Wiederherstellungsplan (3-2-1-Prinzip), Verschlüsselung der Datensicherungen, Backup und Recovery-Konzept (ausformuliert), Richtlinie zur Dokumentation und Kontrolle der Datensicherung, Aufbewahrung einer Datensicherung an sicherem Ort außerhalb des Gebäudes, regelmäßige Tests der Wiederherstellungsfähigkeit der Sicherungen, keine sanitären

Anschlüsse im oder oberhalb des Serverraums, getrennte Partitionen für Betriebssysteme und Daten.

4. Regelmäßige Überprüfung, Bewertung und Evaluierung

- **Technische Maßnahmen:** Software-Lösungen für Datenschutz-Management im Einsatz, zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung (z. B. Wiki, Intranet ...), anderweitiges dokumentiertes Sicherheitskonzept, Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt.
- **Organisatorische Maßnahmen:** Interner Datenschutzbeauftragter, Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet, regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich, interner Informationssicherheitsbeauftragter, Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt, Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach, formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden, Leitlinie für Datenschutz und Informationssicherheit durch Geschäftsführung, Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten, Prozess zur Meldung von Datenschutzverstößen, Führung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO.

(a) Notfallreaktionsplan:

- **Technische Maßnahmen:** Einsatz von Intrusion Detection Lösungen, Einsatz von Intrusion Prevention Lösungen, Firewall mit Angriffserkennung und Blockademechanismen, Einsatz von Virenschutzlösungen mit mindestens täglicher Aktualisierung, Einsatz von Anti Spam Lösungen für E-Mail, Einsatz von Anomalie Erkennungs-Systemen mit verteilten Sensoren, Separierung von Netzwerkkomponenten, Trennbarkeit von Netzwerksegmenten, Reserve-Internetanschluss, Gesonderte Alarmanlage im Serverraum, Redundante Datenhaltung/-sicherung in getrennten Brandschutzzonen, Getrennte Partitionen für Betriebssystem und Peripheriedaten.
- **Organisatorische Maßnahmen:** Prozess zur Erkennung, Meldung und Dokumentation von Datenschutz- und Sicherheitsvorfällen, Prozess zur Einbindung von IT-Dienstleistern in Sicherheitsvorfälle, Etablierung von Meldekettten bei Vorfällen, Prozess zur Übernahme von Verantwortlichkeiten, Vertretungen, Prozess zur Krisenkommunikation, Prozess zum Domain-Delisting bei Spamlisten-Providern im Falle von Sperrungen, Einbindung von DSB und USB in Sicherheitsvorfälle und Datenpannen.

(b) Datenschutzfreundliche Voreinstellungen:

- **Technische Maßnahmen:** Einhaltung der Datensparsamkeit, Ermöglichung der Wahrung des Widerrufsrechts durch technische Maßnahmen.
- **Organisatorische Maßnahmen:** Richtlinien zur Einhaltung datenschutzfreundlicher Voreinstellungen, Prozess zur Etablierung datenschutzfreundlicher Voreinstellungen.

(c) Auftragskontrolle:

- **Organisatorische Maßnahmen:** Sorgfältige Auswahl des (Unter-)Auftragnehmers unter den Gesichtspunkten Datenschutz und Datensicherheit, vorherige Prüfung der vom (Unter-)Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen und deren Dokumentation, Abschluss notwendiger Vereinbarungen zur Auftragsverarbeitung (AV-Vertrag), Einbeziehung notwendiger Garantien bei Datentransfer in Drittländer (EU-Standardvertragsklauseln), sofern erforderlich, schriftliche Weisung an den (Unter-)Auftragnehmer, Verpflichtung der Mitarbeiter des (Unter-)Auftragnehmers auf das Datengeheimnis sowie die Verschwiegenheit nach § 203 StGB, sofern notwendig, Benennung eines Datenschutzbeauftragten durch den (Unter-)Auftragnehmer bei Benennungspflicht, Vereinbarung wirksamer Kontrollrechte, Regelung zur Beauftragung weiterer Unterauftragnehmer, Sicherstellung der Vernichtung von personenbezogenen Daten nach Beendigung des Auftrags, Bei längerer Zusammenarbeit: laufende Kontrolle des (Unter-)Auftragnehmers und seines Schutzniveaus, Regelung der Mitwirkung des (Unter-) Auftragnehmers bei der Wahrnehmung von Betroffenenrechten, Datenschutzverstößen und Kontrollen durch die Aufsichtsbehörde.