power handwerk

POWERHANDWERK · EINE MARKE DER KETESO GMBH

VERTRAG ZUR AUFTRAGSVERARBEITUNG

Anlage 2 zum Hauptvertrag · Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 Abs. 3 DSGVO

PH-AVV v2.2 · Stand 12.10.2026 · Status: Freigegeben zur Verwendung

PRÄAMBEL

Dieser Vertrag zur Auftragsverarbeitung (nachfolgend "AVV") konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit der Erbringung der Leistungen "Done-for-you Google-Business-Profile- und Local-SEO-Management" (nachfolgend "Hauptleistung"), die powerhandwerk, eine Marke der KETESO GmbH, für den Kunden erbringt. Er gilt für alle Verarbeitungen personenbezogener Daten, die KETESO im Auftrag und nach Weisung des Kunden im Rahmen der Hauptleistung durchführt.

Soweit in diesem AVV nichts Abweichendes geregelt ist, gelten die Begriffsbestimmungen der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, "DSGVO").

§ 1 VERTRAGSPARTEIEN UND ROLLENVERTEILUNG

(1) Vertragsparteien dieses AVV sind:

- **der Kunde** (nachfolgend auch "der Betrieb"), als datenschutzrechtlich **Verantwortlicher** im Sinne des Art. 4 Nr. 7 DSGVO, und
- **die KETESO GmbH**, J.-B.-Enderle-Str. 29, 89358 Kammeltal, eingetragen im Handelsregister des Amtsgerichts Memmingen unter HRB 21608, vertreten durch den Geschäftsführer Andreas Keller, handelnd unter der Marke "powerhandwerk" (nachfolgend "KETESO"), als datenschutzrechtlich **Auftragsverarbeiter** im Sinne des Art. 4 Nr. 8 DSGVO.

(2) Der Kunde ist allein verantwortlich für die Rechtmäßigkeit der Datenverarbeitung und für die Wahrung der Rechte der betroffenen Personen (Art. 5, Art. 6 DSGVO). KETESO verarbeitet die personenbezogenen Daten ausschließlich im Auftrag und nach den dokumentierten Weisungen des Kunden.

(3) Dieser AVV erfasst ausschließlich die Verarbeitungen im Rahmen der laufenden Hauptleistung. **Nicht von diesem AVV erfasst** ist der Versand von Bewertungsanfragen an die Endkunden des Betriebs; insoweit ist der Betrieb eigener und alleiniger Verantwortlicher (siehe § 3).

§ 2 GEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG

(1) Gegenstand. Gegenstand der Auftragsverarbeitung ist die Verarbeitung personenbezogener Daten durch KETESO im Rahmen der Hauptleistung, insbesondere die Pflege und Optimierung des Google-Unternehmensprofils des Kunden, die Beantwortung eingehender Bewertungen, das Erstellen und Veröffentlichen von Beiträgen, Fotos und Fragen-/Antwort-Einträgen, die technische Auszeichnung der Website sowie die Erstellung von Berichten und Analysen.

(2) Dauer. Die Dauer dieser Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrags. Sie endet automatisch mit dessen Beendigung, vorbehaltlich der nachvertraglichen Pflichten nach § 11 (Löschung und Rückgabe).

(3) Art der Verarbeitung. Die Verarbeitung umfasst je nach beauftragtem Paket insbesondere das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten, Bereitstellen, Abgleichen, Verknüpfen, Einschränken und Löschen personenbezogener Daten, ganz oder teilweise automatisiert, sowie eine etwaige Cloud- und KI-gestützte Verarbeitung (siehe § 13).

(4) Zweck. Zweck der Verarbeitung ist allein die Erbringung der vertraglich vereinbarten Hauptleistung gemäß Leistungsschein (Anlage 1). Eine Verarbeitung der Daten für eigene Zwecke der KETESO findet nicht statt.

---

§ 3 ABGRENZUNG: VERSAND VON BEWERTUNGSANFRAGEN (EIGENE VERANTWORTLICHKEIT DES BETRIEBS)

(1) powerhandwerk stellt dem Betrieb im Rahmen der Hauptleistung lediglich ein Werkzeug sowie vorbereitete Vorlagen für Bewertungsanfragen bereit. **Die Auswahl der Empfänger sowie der Versand der Bewertungsanfragen erfolgen ausschließlich durch den Betrieb selbst** an dessen eigene Kunden.

(2) Für den Versand der Bewertungsanfragen und die dabei stattfindende Verarbeitung der Kontaktdaten der Endkunden ist **allein der Betrieb datenschutzrechtlich Verantwortlicher** im Sinne des Art. 4 Nr. 7 DSGVO. Diese Verarbeitung ist **nicht Gegenstand dieses AVV** und stellt keine Auftragsverarbeitung durch KETESO dar.

(3) Die von powerhandwerk bereitgestellten Werkzeuge und Vorlagen werden so ausgestaltet, dass der Versand der Bewertungsanfragen technisch beim Betrieb liegt: powerhandwerk stellt lediglich Vorlagentexte, Direktlinks und QR-Material zur Verfügung; **die Auswahl der Empfänger und der eigentliche Versand erfolgen über die eigenen Versandwege des Betriebs (z. B. dessen eigene E-Mail-, SMS- oder Messenger-Kommunikation). Kontaktdaten der Endkunden des Betriebs werden nicht durch Systeme der KETESO oder ihrer Unter-Auftragsverarbeiter verarbeitet.**

(4) Der Betrieb stellt sicher und steht dafür ein, dass für den Versand eine wirksame Rechtsgrundlage besteht (insbesondere Einwilligung oder berechtigtes Interesse) und die Anforderungen des Wettbewerbsrechts (insbesondere § 7 UWG) eingehalten werden.

---

§ 4 ART DER PERSONENBEZOGENEN DATEN UND KATEGORIEN BETROFFENER PERSONEN

(1) Kategorien betroffener Personen. Von der Verarbeitung können folgende Kategorien betroffener Personen erfasst sein:

- Personen, die eine öffentliche Bewertung oder Frage zum Unternehmensprofil des Kunden abgegeben haben (Verfasser von Bewertungen und Fragen),
- Ansprechpartner und Mitarbeitende des Kunden, soweit deren Daten zur Profilpflege verarbeitet werden,
- gegebenenfalls auf vom Kunden bereitgestelltem Bild- und Textmaterial abgebildete oder benannte Personen (z. B. Mitarbeitende auf Fotos).

(2) Art der personenbezogenen Daten. Verarbeitet werden insbesondere folgende Datenarten:

- öffentlich auf der Plattform sichtbare Profil- und Nutzernamen sowie der Inhalt von Bewertungen, Fragen und Antworten,
- Kontakt- und Stammdaten von Ansprechpartnern des Kunden (Name, dienstliche E-Mail-Adresse, dienstliche Telefonnummer),
- Bild- und Tonmaterial, soweit es personenbezogene Daten enthält (z. B. Mitarbeiterfotos),
- Inhaltsdaten der vom Kunden bereitgestellten Materialien.

(3) Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO sind nicht Gegenstand der Verarbeitung. Der Kunde wird KETESO solche Daten nicht zur Verarbeitung übergeben. Soweit der Inhalt öffentlicher Bewertungen ausnahmsweise solche Daten enthält, beschränkt sich die Verarbeitung durch KETESO auf das für die Beantwortung der Bewertung unvermeidbare Maß.

§ 5 WEISUNGSRECHT DES VERANTWORTLICHEN

(1) KETESO verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach den dokumentierten Weisungen des Kunden, es sei denn, KETESO ist zu einer Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten verpflichtet (Art. 28 Abs. 3 lit. a DSGVO). In einem solchen Fall teilt KETESO dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Weisungen werden grundsätzlich in Textform (Art. 28 Abs. 9 DSGVO entsprechend) erteilt. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Der Hauptvertrag samt Leistungsschein (Anlage 1) gilt als Erstweisung; einzelne nachfolgende Weisungen konkretisieren diese.

(3) KETESO informiert den Kunden unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt (Art. 28 Abs. 3 S. 3 DSGVO). KETESO ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis der Kunde sie bestätigt oder ändert.

§ 6 VERTRAULICHKEIT

(1) KETESO stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO, Art. 29, Art. 32 Abs. 4 DSGVO).

(2) Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung der jeweiligen Tätigkeit und nach Beendigung dieses AVV fort.

(3) KETESO setzt zur Durchführung der Verarbeitung nur Personen ein, die zuvor mit den für sie relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden.

§ 7 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

(1) KETESO trifft alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in **Anlage 2a (Technische und organisatorische Maßnahmen)** beschrieben und Bestandteil dieses AVV.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. KETESO ist berechtigt, alternative angemessene Maßnahmen umzusetzen, sofern das nach Anlage 2a vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert KETESO und teilt sie dem Kunden auf Anfrage mit.

(3) KETESO überprüft die Wirksamkeit der getroffenen Maßnahmen regelmäßig (Art. 32 Abs. 1 lit. d DSGVO).

§ 8 UNTER-AUFTRAGSVERARBEITER

(1) Genehmigte Unter-Auftragsverarbeiter. Der Kunde erteilt KETESO mit Abschluss dieses AVV die allgemeine Genehmigung im Sinne des Art. 28 Abs. 2 S. 1 DSGVO zur Inanspruchnahme der in **Anlage 2b (Unter-Auftragsverarbeiter)** aufgeführten Unter-Auftragsverarbeiter. Zum Zeitpunkt des Vertragsschlusses sind dies:

- **Amazon Web Services EMEA SARL**, 38 Avenue John F. Kennedy, L-1855 Luxemburg, Region **eu-central-1 (Frankfurt am Main, Deutschland)**, zum Zweck des Cloud-Hostings (Rechen-, Speicher- und Datenbankdienste) sowie der Cloud- und KI-gestützten Verarbeitung (Amazon Bedrock) als Infrastruktur für die Hauptleistung;
- **Supabase Pte. Ltd.**, 65 Chulia Street #38-02/03, OCBC Centre, Singapur 049513, zum Zweck der Datenbank- und Backend-Dienste für das Kundenverwaltungs- und Arbeitsportal (Speicherung der im Rahmen der Hauptleistung verarbeiteten Daten, u. a. Profildaten und Bewertungsinhalte), Projekt-Region **eu-central-1 (Frankfurt am Main, Deutschland)**, betrieben auf AWS-Infrastruktur;
- **Vercel Inc.**, 440 N Barranca Ave #4133, Covina, CA 91723, USA, zum Zweck des Hostings und der Auslieferung der Web-Anwendungen des Kundenverwaltungs- und Arbeitsportals, serverseitige Verarbeitung bevorzugt in der EU-Region (Frankfurt);
- **Anthropic Ireland, Limited**, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Irland (nachfolgend „Anthropic"), zum Zweck der KI-gestützten Text- und Auswertungsarbeit außerhalb des Kundenverwaltungs- und Arbeitsportals (insbesondere Erstellung und Übersetzung von Berichten, Website-Texten, Profil-Beiträgen und Antworten auf Bewertungen) über den Dienst Claude im gewerblichen Tarif; Speicherung in den USA, Verarbeitung auch in weiteren Drittländern (siehe Absatz 2 und Anlage 2b Abschnitt 3);
- **Brevo GmbH**, Köpenicker Str. 126, 10179 Berlin, Deutschland (nachfolgend „Brevo"), zum Zweck des Versands von E-Mails aus dem Kundenverwaltungs- und Arbeitsportal der KETESO an den Kunden (insbesondere Freigaben von Antworten auf Bewertungen, Berichte und Benachrichtigungen); Datenhaltung nach Angaben des Anbieters in der EU (Frankreich, Deutschland, Belgien), Verarbeitung durch weitere Unter-Auftragsverarbeiter der Brevo teilweise auch in Drittländern (siehe Absatz 2 und Anlage 2b Abschnitte 2 und 3);
- **GitHub, Inc.**, 88 Colin P. Kelly Jr. Street, San Francisco, CA 94107, USA (nachfolgend „GitHub"), zum Zweck der Versionsverwaltung und Ablage von Quellcode, Inhalten und Arbeitsunterlagen der Kundenprojekte, insbesondere der Kundenwebsites, in privaten Repositories der GitHub-Organisation der KETESO (Dienst GitHub Team); Speicherung in den USA, Verarbeitung auch in weiteren Drittländern (siehe Absatz 2 und Anlage 2b Abschnitt 3);
- **Tally BV**, Sint-Pietersnieuwstraat 11, 9000 Gent, Belgien (nachfolgend „Tally"), zum Zweck der Bereitstellung von Online-Formularen, mit denen KETESO Angaben, Texte und Dateien (zum Beispiel Fotos) beim Kunden abfragt, insbesondere zum Onboarding; Datenhaltung nach Angaben des Anbieters in Europa (siehe Absatz 2 und Anlage 2b Abschnitte 2 und 3).

(2) Datenbelegenheit des Portals in der EU; Drittlandbezüge. Die Datenhaltung des Kundenverwaltungs- und Arbeitsportals erfolgt im Rahmen der Standardkonfiguration ausschließlich innerhalb der Europäischen Union: Die Speicherung ist auf die Region eu-central-1 (Frankfurt am Main) beschränkt (AWS direkt sowie Supabase, dessen Projekt-Region auf AWS-Infrastruktur in Frankfurt betrieben wird); die serverseitige Verarbeitung durch Vercel erfolgt bevorzugt in der EU-Region (Frankfurt); die KI-Inferenz über Amazon Bedrock erfolgt unter Verwendung von EU-Inferenzprofilen ausschließlich in EU-Regionen. Die Datenbelegenheit des Portals (Speicherung und Verarbeitung der Daten) ist damit auf die EU beschränkt; ein gezielter Transfer personenbezogener Daten in ein Drittland im Sinne der Art. 44 ff. DSGVO findet insoweit im Standardbetrieb nicht statt.

Für die KI-gestützte Text- und Auswertungsarbeit außerhalb des Portals setzt KETESO den Unter-Auftragsverarbeiter Anthropic ein. Insoweit werden personenbezogene Daten in Drittländer übermittelt, insbesondere in die USA; Verarbeitungsorte, Aufbewahrung und Garantien ergeben sich aus Anlage 2b Abschnitt 3. Für die Versionsverwaltung und Ablage der Kundenprojekte setzt KETESO den Unter-Auftragsverarbeiter GitHub ein; insoweit werden personenbezogene Daten in die USA übermittelt (siehe die nachfolgende Aufzählung und Anlage 2b Abschnitt 3).

Soweit gleichwohl Drittlandbezüge bestehen, sind diese durch geeignete Garantien nach Art. 44 ff. DSGVO abgesichert:

- **Amazon Web Services EMEA SARL** (Luxemburg) gehört zu einem Konzern mit Muttergesellschaft in den USA (Amazon.com Inc.); das hieraus folgende potenzielle Zugriffsrisiko durch US-Stellen (insbesondere FISA 702, US CLOUD Act) ist durch das geltende AWS Data Processing Addendum, dessen EU-Standardvertragsklauseln und die technischen Maßnahmen (insbesondere Verschlüsselung bei Übertragung und Speicherung) adressiert.
- **Supabase Pte. Ltd.** hat ihren Sitz in einem Drittland (Singapur); die Datenbelegenheit des eingesetzten Projekts liegt in der EU (Frankfurt). Für einen etwaigen Fernzugriff des Anbieters zu Support- und Betriebszwecken gelten die EU-Standardvertragsklauseln aus dem Supabase Data Processing Addendum.
- **Vercel Inc.** ist eine US-Gesellschaft und nach dem EU-US Data Privacy Framework (DPF) sowie dem Swiss-US DPF zertifiziert; ergänzend gelten die EU-Standardvertragsklauseln aus dem Vercel Data Processing Addendum.
- **Anthropic** (Vertragspartner in Irland) speichert die Daten in den USA und kann sie in weiteren Drittländern verarbeiten; die Übermittlung ist durch das Data Processing Addendum der Anthropic mit EU-Standardvertragsklauseln abgesichert; für Übermittlungen an bestimmte verbundene Unternehmen und Dritte in Ländern ohne Angemessenheitsbeschluss stützt sich Anthropic nach seiner Datenschutzerklärung auf EU-Standardvertragsklauseln; eine Zertifizierung nach dem EU-US Data Privacy Framework besteht nicht.
- **Brevo GmbH** (Berlin, Deutschland) hat ihren Sitz in der EU und speichert die Daten nach Angaben des Anbieters in Frankreich, Deutschland und Belgien. Soweit Brevo Unter-Auftragsverarbeiter in Drittländern einsetzt (nach der Liste des Anbieters insbesondere Konzerngesellschaften in den USA und in Indien für Kundendienst und Wartung sowie Dienstleister für das Auslieferungsnetz), sind diese Übermittlungen nach Angaben von Brevo durch EU-Standardvertragsklauseln mit begleitenden Maßnahmen und, soweit der Empfänger zertifiziert ist, durch das EU-US Data Privacy Framework abgesichert; die Einzelheiten je Empfänger ergeben sich aus der Liste der Unter-Auftragsverarbeiter in der Datenschutzvereinbarung der Brevo.
- **GitHub, Inc.** ist eine US-Gesellschaft und nach dem EU-US Data Privacy Framework (DPF) sowie dem Swiss-US DPF zertifiziert; ergänzend gelten die EU-Standardvertragsklauseln (Modul 2 und Modul 3, soweit erforderlich) aus dem GitHub Data Protection Agreement. Die Daten werden in den USA gespeichert und können in weiteren Ländern verarbeitet werden, in denen GitHub oder seine Unter-Auftragsverarbeiter tätig sind.
- **Tally BV** hat ihren Sitz in Belgien und speichert die Formulardaten nach eigenen Angaben in Europa (Hosting und Speicherung bei Google Cloud, Belgien); ein gezielter Transfer in ein Drittland findet insoweit nicht statt. Für hochgeladene Dateien nutzt Tally nach eigenen Angaben Cloudflare mit Speicherung in der EU; für optionale E-Mail-Benachrichtigungen nutzt Tally nach eigenen Angaben SendGrid (USA). Tally hat sich im Auftragsverarbeitungsvertrag verpflichtet, Daten nur ausnahmsweise und nur, soweit zur Vertragserfüllung erforderlich, in einem Land außerhalb des EWR ohne Angemessenheitsbeschluss der Europäischen Kommission zu verarbeiten, dies auf Grundlage von EU-Standardvertragsklauseln oder anderer nach dem Datenschutzrecht vorgesehener Mechanismen abzusichern und KETESO vorab über die getroffenen Maßnahmen zu informieren. Eine Zertifizierung der Tally BV nach dem EU-US Data Privacy Framework besteht nicht.

Sollte im Kundenverwaltungs- und Arbeitsportal ausnahmsweise eine Verarbeitung außerhalb der EU/des EWR oder durch ein außerhalb der EU/des EWR betriebenes KI-Modell erforderlich werden (etwa bei regionsübergreifender KI-Inferenz oder bei Nutzung eines nicht in der EU-Region betriebenen Modells), wird KETESO dies erst nach Schaffung einer geeigneten Garantie nach Art. 46 DSGVO (insbesondere EU-Standardvertragsklauseln) und nach Durchführung einer Transfer-Folgenabschätzung sowie nach vorheriger Information des Kunden umsetzen.

(3) Änderung der Unter-Auftragsverarbeiter. Beabsichtigt KETESO, einen weiteren Unter-Auftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, informiert sie den Kunden hierüber rechtzeitig in Textform, mindestens vier Wochen vor der beabsichtigten Beauftragung (Art. 28 Abs. 2 S. 2 DSGVO). Der Kunde kann der Änderung innerhalb von vier Wochen ab Zugang der Information aus wichtigem, datenschutzrechtlich begründetem Grund in Textform widersprechen. Widerspricht der Kunde nicht fristgerecht, gilt die Änderung als genehmigt.

(4) Wichtiger Grund / Sonderkündigung. Widerspricht der Kunde aus wichtigem, datenschutzrechtlich begründetem Grund und ist eine für beide Seiten zumutbare Lösung nicht möglich, steht KETESO ein Sonderkündigungsrecht hinsichtlich der betroffenen Leistung zu. Macht KETESO hiervon Gebrauch, steht dem Kunden ein Recht zur Kündigung des Hauptvertrags aus wichtigem Grund zu.

(5) Pflichten gegenüber Unter-Auftragsverarbeitern. KETESO erlegt jedem Unter-Auftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in diesem AVV festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Kommt der Unter-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet KETESO gegenüber dem Kunden für die Einhaltung dieser Pflichten.

(6) Keine Unterauftragsverarbeitung sind Nebenleistungen, die KETESO als reine Hilfsleistung in Anspruch nimmt (z. B. Telekommunikationsleistungen, Wartung/Pflege ohne Datenzugriff, Entsorgung von Datenträgern). KETESO ist jedoch verpflichtet, auch hierbei angemessene Schutzmaßnahmen sicherzustellen.

---

§ 9 UNTERSTÜTZUNG BEI BETROFFENENRECHTEN

(1) KETESO unterstützt den Kunden im Rahmen ihrer Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte (insbesondere Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) nachzukommen (Art. 28 Abs. 3 lit. e DSGVO).

(2) Wendet sich eine betroffene Person unmittelbar an KETESO, leitet KETESO dieses Ersuchen unverzüglich an den Kunden weiter und beantwortet es nicht selbst, es sei denn, sie ist hierzu vom Kunden ausdrücklich angewiesen.

(3) Für die Erfüllung von Betroffenenrechten ist der Kunde als Verantwortlicher zuständig. Ein etwaiger angemessener Aufwand für über die Standardunterstützung hinausgehende Maßnahmen kann nach gesonderter Vereinbarung vergütet werden, soweit die Inanspruchnahme nicht auf einem Pflichtverstoß der KETESO beruht.

---

§ 10 MELDEPFLICHTEN UND SONSTIGE UNTERSTÜTZUNGSPFLICHTEN

(1) Verletzung des Schutzes personenbezogener Daten. KETESO meldet dem Kunden jede ihr bekannt gewordene Verletzung des Schutzes personenbezogener Daten, die die im Auftrag verarbeiteten Daten betrifft, unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, in Textform (Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO). Die Meldung enthält mindestens die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben, soweit KETESO diese vorliegen.

(2) KETESO unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach den Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung an die Aufsichtsbehörde, Benachrichtigung betroffener Personen, Datenschutz-Folgenabschätzung, vorherige Konsultation) (Art. 28 Abs. 3 lit. f DSGVO).

(3) Meldungen an die zuständige Aufsichtsbehörde sowie Benachrichtigungen betroffener Personen obliegen dem Kunden als Verantwortlichem.

---

§ 11 LÖSCHUNG UND RÜCKGABE NACH BEENDIGUNG

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht KETESO nach Wahl des Kunden alle im Auftrag verarbeiteten personenbezogenen Daten oder gibt sie an den Kunden zurück und löscht vorhandene Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 3 lit. g DSGVO).

(2) Der Kunde teilt seine Wahl nach Absatz 1 spätestens bei Beendigung des Hauptvertrags in Textform mit. Trifft der Kunde innerhalb von 30 Tagen nach Beendigung keine Wahl, löscht KETESO die Daten.

(3) Daten, die KETESO aufgrund gesetzlicher Aufbewahrungspflichten weiter speichern muss, werden bis zum Ablauf der jeweiligen Frist gesperrt und sodann gelöscht.

(4) KETESO bestätigt die Löschung oder Rückgabe auf Verlangen des Kunden in Textform.

(5) Der laufende Zugriff von KETESO auf das Google-Unternehmensprofil endet mit Beendigung des Hauptvertrags; das Profil verbleibt im Eigentum und im Inhaber-Zugang des Kunden.

---

§ 12 NACHWEISE UND KONTROLLRECHTE (AUDIT)

(1) KETESO stellt dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen, einschließlich Inspektionen, die vom Kunden oder einem von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Nachweis kann nach Wahl der KETESO auch durch die Vorlage geeigneter, aktueller Zertifizierungen, Testate oder Berichte unabhängiger Stellen (z. B. Prüfberichte, Zertifikate nach anerkannten Standards) geführt werden, insbesondere hinsichtlich der durch den Unter-Auftragsverarbeiter eingesetzten Infrastruktur.

(3) Vor-Ort-Kontrollen sind mit angemessener Vorankündigung (mindestens zwei Wochen), während der üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs und in der Regel nicht häufiger als einmal je Kalenderjahr durchzuführen. Bei konkretem Anlass (insbesondere nach einer Datenschutzverletzung oder auf Verlangen einer Aufsichtsbehörde) ist eine anlassbezogene Kontrolle auch darüber hinaus zulässig.

(4) Der mit der Kontrolle beauftragte Prüfer darf nicht in einem Wettbewerbsverhältnis zu KETESO stehen und ist zur Vertraulichkeit zu verpflichten. Ein etwaiger angemessener Aufwand der KETESO für über die Standardnachweise hinausgehende Kontrollunterstützung kann nach gesonderter Vereinbarung vergütet werden.

---

§ 13 CLOUD- UND KI-GESTÜTZTE VERARBEITUNG; AI-ACT-HINWEIS

(1) Im Rahmen der Hauptleistung kann KETESO Cloud-Dienste und KI-gestützte Verfahren einsetzen, insbesondere zur Erstellung und Aufbereitung von Texten, zur Analyse öffentlich sichtbarer Profil- und Bewertungsdaten sowie zur Berichterstellung. Die im Kundenverwaltungs- und Arbeitsportal eingesetzte KI-Infrastruktur wird über den hierfür in § 8 genannten Unter-Auftragsverarbeiter (Amazon Web Services, Amazon Bedrock mit EU-Inferenzprofilen in EU-Regionen, Region eu-central-1) bereitgestellt; die in § 8 genannten Unter-Auftragsverarbeiter Supabase und Vercel betreffen den Betrieb des Portals. Für die KI-gestützte Text- und Auswertungsarbeit außerhalb des Portals setzt KETESO den in § 8 genannten Unter-Auftragsverarbeiter Anthropic (Dienst Claude im gewerblichen Tarif) ein.

(2) Eine ausschließlich automatisierte Entscheidung im Einzelfall mit rechtlicher Wirkung oder ähnlich erheblicher Beeinträchtigung gegenüber betroffenen Personen im Sinne des Art. 22 DSGVO findet nicht statt. Inhalte mit Außenwirkung (z. B. Antworten auf Bewertungen, Beiträge) werden vor Veröffentlichung redaktionell verantwortet.

(3) Soweit nach der Verordnung (EU) 2024/1689 (KI-Verordnung, “AI Act”) Transparenzpflichten gegenüber betroffenen Personen bestehen, unterstützt KETESO den Kunden bei deren Erfüllung. Der Kunde weist auf den Einsatz KI-gestützter Verfahren in seiner Datenschutzerklärung hin.

(4) Trainingszwecke fremder KI-Anbieter sind ausgeschlossen; die im Auftrag verarbeiteten personenbezogenen Daten werden nicht zum Training von KI-Modellen Dritter verwendet.

§ 14 HAFTUNG

(1) Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Verhältnis der Parteien untereinander gelten ergänzend die Haftungsregelungen des Hauptvertrags, soweit diese mit Art. 82 DSGVO und den übrigen zwingenden Vorgaben der DSGVO vereinbar sind.

(2) Der Kunde ist als Verantwortlicher für die Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen verantwortlich. Stellt eine betroffene Person oder eine Aufsichtsbehörde Ansprüche, die auf einem Umstand beruhen, der dem Verantwortungsbereich des Kunden zuzuordnen ist (insbesondere fehlende Rechtsgrundlage, rechtswidrige Weisung, Versand von Bewertungsanfragen nach § 3), stellt der Kunde KETESO im Innenverhältnis von diesen Ansprüchen frei, soweit KETESO die Verletzung nicht zu vertreten hat.

§ 15 SCHLUSSBESTIMMUNGEN

(1) Dieser AVV ist Anlage 2 zum Hauptvertrag und gilt für dessen Laufzeit. Bei Widerspruch zwischen diesem AVV und dem übrigen Hauptvertrag gehen hinsichtlich der Datenverarbeitung die Regelungen dieses AVV vor.

(2) Änderungen und Ergänzungen dieses AVV sowie seiner Anlagen bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Textformerfordernisses. Rechtserhebliche mündliche Individualabreden, die nach Vertragsschluss getroffen werden, haben jedoch Vorrang vor dieser Klausel.

(3) Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt. Die Parteien werden die unwirksame Bestimmung durch eine wirksame ersetzen, die dem wirtschaftlichen und datenschutzrechtlichen Zweck der unwirksamen am nächsten kommt.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz der KETESO GmbH.

(5) Bestandteil dieses AVV sind:

- **Anlage 2a** Technische und organisatorische Maßnahmen (TOM)
- **Anlage 2b** Unter-Auftragsverarbeiter

ORT, DATUM	DER KUNDE (VERANTWORTLICHER)	KETESO GMBH (AUFTRAGSVERARBEITER)
[…]	[Unterschrift, Name in Druckbuchstaben]	[Unterschrift, Andreas Keller, Geschäftsführer]

Dokument PH-AVV, Version 2.2, Stand 12.10.2026, Status: Freigegeben zur Verwendung (anwaltlich geprüfte Fassung). Neu gegenüber Version 2.1: § 8 Absatz 1 um die Unter-Auftragsverarbeiter Anthropic, Brevo, GitHub und Tally ergänzt sowie Firmierung und Anschrift der Supabase (nunmehr Supabase Pte. Ltd.) und die Anschrift der Vercel berichtigt; § 8 Absatz 2 mit der Datenbelegenheit des Portals in der EU und den Drittlandbezügen über Anthropic, Brevo, GitHub und Tally; § 13 Absatz 1 um die KI-gestützte Arbeit außerhalb des Portals über Anthropic ergänzt.