POWERHANDWERK · EINE MARKE DER KETESO GMBH

LISTE DER UNTER-AUFTRAGSVERARBEITER

Anlage 2b zum Auftragsverarbeitungsvertrag (AVV, Anlage 2) · Unter-Auftragsverarbeiter nach Art. 28 Abs. 2 und 4 DSGVO

PH-SUB v1.2 · Stand 12.10.2026 · Status: Freigegeben zur Verwendung

1. VORBEMERKUNG

Diese Anlage enthält die zum Stand 12.10.2026 von KETESO eingesetzten Unter-Auftragsverarbeiter im Sinne des Art. 28 Abs. 2 und 4 DSGVO. Der Kunde hat dem Einsatz der nachfolgend aufgeführten Unter-Auftragsverarbeiter mit Abschluss des AVV allgemein zugestimmt (AVV § 8 Abs. 1). Änderungen dieser Liste richten sich nach AVV § 8 Abs. 3 (Vorabinformation und Widerspruchsrecht). Verweise dieser Anlage auf die Anlage 2a beziehen sich auf die Fassung, die für den jeweiligen Kunden gilt. Die in Anlage 2a § 8 (Fassung 1.2) beschriebenen Maßnahmen für die Anthropic Ireland, Limited sind Teil der Angaben zu diesem Unter-Auftragsverarbeiter und gelten auch, soweit für den Kunden noch eine frühere Fassung der Anlage 2a gilt.

Die Cloud-Infrastruktur wird über ein auf die KETESO GmbH laufendes AWS-Konto betrieben (Konto-Nr. 603433800788; Kontoinhaber-Stammdaten: KETESO GmbH, Johann-Baptist-Enderle-Str. 29, 89358 Kammeltal, verifiziert per Konto-Audit vom 07.07.2026). Für die Datenhaltung und den Betrieb des Kundenverwaltungs- und Arbeitsportals setzt KETESO zusätzlich die Dienste Supabase (Datenbank/Backend, Projekt-Region eu-central-1) und Vercel (Hosting) ein; beide sind nachfolgend als Unter-Auftragsverarbeiter aufgeführt. Für die KI-gestützte Text- und Auswertungsarbeit außerhalb des Kundenverwaltungs- und Arbeitsportals setzt KETESO den Dienst Claude der Anthropic Ireland, Limited im gewerblichen Tarif ein (Arbeitsbereich der KETESO GmbH); Anthropic ist nachfolgend ebenfalls als Unter-Auftragsverarbeiter aufgeführt. Für den Versand von E-Mails aus dem Portal an den Kunden (Brevo), die Versionsverwaltung und Ablage der Kundenprojekte (GitHub) und Online-Formulare für Abfragen beim Kunden (Tally) setzt KETESO weitere Dienste ein; sie sind nachfolgend ebenfalls als Unter-Auftragsverarbeiter aufgeführt.

2. LISTE DER UNTER-AUFTRAGSVERARBEITER

NAME / ANSCHRIFT	LEISTUNG	ORT DER VERARBEITUNG	GARANTIEN
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg (Vertragsentität am 07.07.2026 aus dem Konto verifiziert: Seller-Angabe der AWS-Tax-Settings)	Cloud-Hosting (Rechen-, Speicher- und Datenbankdienste) sowie Cloud- und KI-gestützte Verarbeitung (Amazon Bedrock) als Infrastruktur für die Hauptleistung	**Datenhaltung: Region eu-central-1 (Frankfurt am Main, Deutschland)**; KI-Inferenz über EU-Inferenzprofile ausschließlich in EU-Regionen. Datenbelegenheit ausschließlich innerhalb der EU; die Regionsbindung ist auf Kontoebene technisch erzwungen (siehe Anlage 2a § 1.3). Kein gezielter Drittlandtransfer im Standardbetrieb; potenzielles Zugriffsrisiko durch US-Stellen aufgrund der US-Konzernmutter (Amazon.com Inc.) ist durch AWS DPA, EU-Standardvertragsklauseln und Verschlüsselung adressiert (siehe Abschnitt 3)	Auftragsverarbeitungsvertrag mit AWS: AWS GDPR Data Processing Addendum, als Bestandteil der AWS Service Terms automatisch in das Vertragsverhältnis einbezogen, in der jeweils geltenden Fassung; Verschlüsselung bei Übertragung und Speicherung; Zertifizierungen u. a. ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3, BSI C5; technische und organisatorische Maßnahmen nach Art. 32 DSGVO (siehe Anlage 2a § 7)
Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapur 049513 (Vertragspartner nach den Supabase Terms of Service; Anschrift gemäß Supabase-DPA, bei Inkraftsetzung aus der jeweils aktuellen DPA-Fassung zu übernehmen)	Datenbank- und Backend-Dienste für das Kundenverwaltungs- und Arbeitsportal der KETESO (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; Datenbelegenheit innerhalb der EU. Sitz des Anbieters im Drittland (Singapur); Fernzugriff zu Support-/Betriebszwecken durch EU-Standardvertragsklauseln abgesichert (siehe Abschnitt 3)	Data Processing Addendum der Supabase Pte. Ltd. (Version 1 vom 01.08.2026), als Bestandteil der Supabase Terms of Service mit deren Annahme automatisch in das Vertragsverhältnis einbezogen, in der jeweils geltenden Fassung, mit EU-Standardvertragsklauseln (Modul 2 und Modul 3, soweit erforderlich; irisches Recht); Verschlüsselung bei Übertragung (TLS 1.2) und Speicherung (AES-256); nach Angaben des Anbieters Zertifizierungen SOC 2 Type 2 und ISO 27001; für Singapur besteht kein Angemessenheitsbeschluss der Europäischen Kommission; technische und

NAME / ANSCHRIFT	LEISTUNG	ORT DER VERARBEITUNG	GARANTIEN
			organisatorische Maßnahmen nach Art. 32 DSGVO
Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, USA (Anschrift gemäß Vercel-DPA, bei Inkraftsetzung aus der jeweils aktuellen DPA-Fassung zu übernehmen)	Hosting und Auslieferung der Web-Anwendungen der KETESO (Kundenverwaltungs- und Arbeitsportal)	Serverseitige Verarbeitung bevorzugt in der EU-Region (Frankfurt); Auslieferung über ein weltweites Edge-Netzwerk, Zugriff der US-Gesellschaft möglich. Transfer in die USA durch Zertifizierung nach dem EU-US Data Privacy Framework (DPF) sowie EU-Standardvertragsklauseln abgesichert (siehe Abschnitt 3)	Data Processing Addendum von Vercel; DPF-zertifiziert (EU-US, Swiss-US); EU-Standardvertragsklauseln; Verschlüsselung bei Übertragung und Speicherung; Zertifizierungen u. a. SOC 2 Type II, ISO 27001
Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Irland (Vertragspartner für Kunden mit Sitz im EWR nach den Anthropic Commercial Terms of Service)	KI-gestützte Text- und Auswertungsarbeit außerhalb des Kundenverwaltungs- und Arbeitsportals der KETESO (insbesondere Erstellung und Übersetzung von Berichten, Website-Texten, Profil-Beiträgen und Antworten auf Bewertungen) über den Dienst Claude im gewerblichen Tarif „Team“, einschließlich des Werkzeugs Claude Code	**Speicherung in den USA.** Die KI-Verarbeitung kann nach Angaben des Anbieters standardmäßig in ausgewählten Ländern in den USA, Europa, Asien und Australien erfolgen; interne Vorgänge des Anbieters (etwa Sicherheitsprüfung, Support, Bearbeitung von Vorfällen) auch in weiteren Ländern, in denen Anthropic oder verbundene Unternehmen tätig sind. Infrastruktur über Google Cloud Platform, Amazon Web Services und Microsoft Azure. Drittlandtransfer, Aufbewahrung und Training siehe Abschnitt 3	Data Processing Addendum der Anthropic (Fassung vom 24.02.2025), als Bestandteil der Commercial Terms of Service automatisch in das Vertragsverhältnis einbezogen, in der jeweils geltenden Fassung, mit EU-Standardvertragsklauseln (Modul 2 und Modul 3, soweit erforderlich; irisches Recht); Verschlüsselung bei Übertragung (TLS 1.2 oder höher) und Speicherung (AES-256); Zertifizierungen für den Tarif Team u. a. SOC 2 Type II, ISO/IEC 27001:2022, ISO/IEC 42001:2023, CSA STAR; keine Zertifizierung nach dem EU-US Data Privacy Framework; technische und organisatorische Maßnahmen nach Art. 32 DSGVO (siehe Anlage 2a § 8)
Brevo GmbH, Köpenicker Str. 126, 10179 Berlin, Deutschland (Amtsgericht Charlottenburg, HRB 133191; Vertragspartnerin der KETESO nach den	Versand von E-Mails aus dem Kundenverwaltungs- und Arbeitsportal der KETESO an den Kunden (insbesondere Freigaben von Antworten auf Bewertungen, Berichte	**Speicherung in der EU:** nach der Liste der Unter-Auftragsverarbeiter von Brevo bei OVH SAS in Frankreich und Deutschland sowie bei Google Cloud in Belgien. Weitere Unter-Auftragsverarbeiter von	Auftragsverarbeitungsvertrag mit Brevo: Datenschutzvereinbarung (Data Processing Agreement) der Brevo als Anhang 3 der Allgemeinen Nutzungsbedingungen der Brevo-Dienste (Seitenkopf: Fassung vom 16.10.2025,

NAME / ANSCHRIFT	LEISTUNG	ORT DER VERARBEITUNG	GARANTIEN
Allgemeinen Nutzungsbedingungen der Brevo-Dienste für Nutzer mit Sitz in Deutschland; Tochtergesellschaft der Sendinblue SAS, Paris, Frankreich)	und Benachrichtigungen)	Brevo (Auslieferungsnetz, Kundendienst, Wartung) verarbeiten teilweise auch in den USA oder von Drittländern aus (u. a. USA, Indien). Drittlandtransfer siehe Abschnitt 3	abgerufen am 12.10.2026), ohne gesonderte Unterzeichnung Bestandteil des Vertragsverhältnisses, in der jeweils geltenden Fassung; Verschlüsselung bei Übertragung (TLS 1.2 und 1.3); Zertifizierung ISO/IEC 27001:2022 nach Angabe des Anbieters; technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Anhang 4 der Nutzungsbedingungen, Stand 17.07.2026)
GitHub, Inc., 88 Colin P. Kelly Jr. Street, San Francisco, CA 94107, USA (Vertragspartner der KETESO nach dem GitHub Customer Agreement; Anschrift gemäß GitHub Data Protection Agreement, Fassung Oktober 2025)	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** (GitHub.com ohne Wahl einer Datenresidenz-Region). Eine Verarbeitung kann auch in weiteren Ländern erfolgen, in denen GitHub oder seine Unter-Auftragsverarbeiter tätig sind (Infrastruktur unter anderem über Microsoft Azure und Amazon Web Services). Transfer in die USA durch Zertifizierung nach dem EU-US Data Privacy Framework (DPF) sowie EU-Standardvertragsklauseln abgesichert (siehe Abschnitt 3)	GitHub Data Protection Agreement (Fassung Oktober 2025) als Bestandteil des GitHub Customer Agreement, das KETESO für ihre GitHub-Organisation abgeschlossen hat, in der jeweils geltenden Fassung; DPF-zertifiziert (EU-US, Swiss-US); EU-Standardvertragsklauseln (Modul 2 und Modul 3, soweit erforderlich; niederländisches Recht); Verschlüsselung der Übertragung über öffentliche Netze durch GitHub oder den Kunden; Zertifizierungen nach Angaben des Anbieters soweit einschlägig, unter anderem SOC 1 Type 2, SOC 2 Type 2 und ISO/IEC 27001; technische und organisatorische Maßnahmen nach Art. 32 DSGVO
Tally BV, Sint-Pietersnieuwstraat 11, 9000 Gent, Belgien (Anbieter und Vertragspartner nach den Allgemeinen Geschäftsbedingungen von Tally; belgische Unternehmensnummer 0776.979.007)	Online-Formulare, mit denen KETESO Angaben, Texte und Dateien (zum Beispiel Fotos) beim Kunden abfragt, insbesondere zum Onboarding	**Speicherung in Europa** (nach Angaben des Anbieters; Hosting und Speicherung bei Google Cloud, Belgien). Hochgeladene Dateien werden nach Angaben des Anbieters bei Cloudflare in der EU gespeichert. Für E-Mail-Benachrichtigungen setzt Tally nach Angaben des Anbieters optional SendGrid (USA) ein.	Auftragsverarbeitungsvertrag (Data Processing Agreement) der Tally BV, Fassung vom 09.09.2024, als Bestandteil der Allgemeinen Geschäftsbedingungen von Tally (Sonderbedingungen für berufliche Nutzer) mit Anlegen des Kontos automatisch in das Vertragsverhältnis einbezogen, in der jeweils geltenden Fassung; Recht und Gerichtsstand nach den

NAME / ANSCHRIFT	LEISTUNG	ORT DER VERARBEITUNG	GARANTIEN
		Drittlandtransfer siehe Abschnitt 3	Allgemeinen Geschäftsbedingungen von Tally (Recht Belgiens, Gerichte in Gent); Verschlüsselung bei Übertragung und Speicherung nach Angaben des Anbieters; technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Anlage I des Auftragsverarbeitungsvertrags); Sitz des Anbieters in der EU, keine Zertifizierung nach dem EU-US Data Privacy Framework

3. DRITTLANDTRANSFER

Die Datenhaltung des Kundenverwaltungs- und Arbeitsportals erfolgt im Standardbetrieb 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 KI-Inferenz des Portals über Amazon Bedrock erfolgt unter Verwendung von EU-Inferenzprofilen ausschließlich in EU-Regionen und ist zustandslos (keine dauerhafte Speicherung der Ein- und Ausgaben, keine Nutzung zum Modell-Training; siehe Anlage 2a § 1.5). Für die KI-gestützte Text- und Auswertungsarbeit außerhalb des Portals setzt KETESO den Dienst Claude der Anthropic ein; insoweit werden personenbezogene Daten in Drittländer übermittelt, insbesondere in die USA (siehe unten). Für die Versionsverwaltung und Ablage der Kundenprojekte setzt KETESO GitHub ein; insoweit werden personenbezogene Daten in die USA übermittelt (siehe unten).

Soweit gleichwohl Drittlandbezüge bestehen, sind diese wie folgt abgesichert (Art. 44 ff. DSGVO):

- **AWS EMEA SARL** (Luxemburg) gehört zu einem Konzern mit Muttergesellschaft in den USA (Amazon.com Inc.). Ein hieraus folgendes potenzielles Zugriffsrisiko durch US-Stellen (insbesondere nach FISA 702 und US CLOUD Act) wird durch das mit AWS geltende Data Processing Addendum, dessen EU-Standardvertragsklauseln und die technischen Maßnahmen (insbesondere Verschlüsselung bei Übertragung und Speicherung) adressiert.
- **Supabase Pte. Ltd.** hat ihren Sitz in 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. Die serverseitige Verarbeitung erfolgt bevorzugt in der EU-Region (Frankfurt).
- **Anthropic Ireland, Limited** (Irland) ist Vertragspartner der KETESO. Die Daten werden in den USA gespeichert; die KI-Verarbeitung kann nach Angaben des Anbieters in ausgewählten Ländern in den USA, Europa, Asien und Australien erfolgen, interne Vorgänge des Anbieters auch in weiteren Ländern, in denen Anthropic oder verbundene Unternehmen tätig sind. Die Übermittlung ist durch das Data Processing Addendum der Anthropic mit EU-Standardvertragsklauseln (Modul 2 und Modul 3, soweit erforderlich) abgesichert. Für Übermittlungen an bestimmte verbundene Unternehmen und Dritte in Ländern ohne Angemessenheitsbeschluss stützt sich Anthropic nach seiner Datenschutzerklärung auf EU-Standardvertragsklauseln; seine Unter-Auftragsverarbeiter verpflichtet Anthropic vertraglich auf Datenschutzpflichten, die im Wesentlichen ebenso schützend sind wie das Data Processing Addendum, soweit sie zur Art der Leistung passen. Eine Zertifizierung nach dem EU-US Data Privacy Framework besteht nicht. Unterhaltungen und im Produkt gespeicherte Sitzungen bleiben bis zur Löschung durch KETESO

gespeichert und werden danach innerhalb von 30 Tagen entfernt; Ein- und Ausgaben von Claude-Code-Sitzungen auf dem eigenen Rechner werden standardmäßig 30 Tage aufbewahrt; eine Nutzung zum Training von Modellen ist vertraglich ausgeschlossen. KETESO hat vor dem Einsatz eine Transfer-Folgenabschätzung durchgeführt (abgeschlossen am 13.10.2026).

- **Brevo GmbH** (Berlin, Deutschland) ist Vertragspartnerin der KETESO und hat ihren Sitz in der EU; die Daten werden nach Angaben des Anbieters in Frankreich, Deutschland und Belgien gespeichert. Soweit Brevo für Auslieferungsnetz, Kundendienst und Wartung Unter-Auftragsverarbeiter in Drittländern einsetzt (nach der Liste des Anbieters u. a. Brevo, Inc. und Cloudflare, Inc. in den USA sowie die Brevo CRM Solution Private Limited in Indien), stützt Brevo diese Übermittlungen nach eigenen Angaben auf EU-Standardvertragsklauseln mit begleitenden Maßnahmen und, soweit der Empfänger nach dem EU-US Data Privacy Framework zertifiziert ist, auf diese Zertifizierung. Die Garantie je Empfänger weist Brevo in der Liste der Unter-Auftragsverarbeiter ihrer Datenschutzvereinbarung aus.
- **GitHub, Inc.** (USA) ist Vertragspartner der KETESO 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, das für KETESO über das GitHub Customer Agreement der GitHub-Organisation gilt. Die Daten werden in den USA gespeichert und können in weiteren Ländern verarbeitet werden, in denen GitHub oder seine Unter-Auftragsverarbeiter tätig sind. Nach Beendigung der Leistungen löscht GitHub die Daten oder gibt sie nach Wahl der KETESO zurück; vorhandene Kopien löscht GitHub nach seiner eigenen Aufbewahrungs- und Löschrichtlinie.
- **Tally BV** (Belgien) ist Vertragspartner der KETESO und speichert die Formulardaten nach Angaben des Anbieters in Europa (Hosting und Speicherung bei Google Cloud, Belgien); ein gezielter Drittlandtransfer findet insoweit nicht statt. Hochgeladene Dateien werden nach Angaben des Anbieters bei Cloudflare in der EU gespeichert. Für E-Mail-Benachrichtigungen setzt Tally nach Angaben des Anbieters optional SendGrid (USA) ein. Nach dem Auftragsverarbeitungsvertrag darf Tally Daten nur ausnahmsweise und nur, soweit zur Vertragserfüllung erforderlich, in einem Land außerhalb des EWR ohne Angemessenheitsbeschluss der Europäischen Kommission verarbeiten, und zwar auf Grundlage von EU-Standardvertragsklauseln oder anderer nach dem Datenschutzrecht vorgesehener Mechanismen; Tally muss KETESO vorab über die getroffenen Maßnahmen 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, wird dies erst nach Schaffung geeigneter Garantien nach Art. 46 DSGVO (insbesondere EU-Standardvertragsklauseln), nach Durchführung einer Transfer-Folgenabschätzung und nach vorheriger Information des Kunden umgesetzt (siehe AVV § 8 Abs. 2).

4. HINWEIS ZU ERFÜLLUNGSGEHILFEN / SONSTIGEN BETEILIGTEN

Personen, die KETESO innerhalb ihrer eigenen, von KETESO kontrollierten Systeme und ausschließlich nach Weisung der KETESO ohne eigene Datenhaltung einsetzt, sind keine Unter-Auftragsverarbeiter im Sinne des Art. 28 DSGVO, sondern Personal bzw. Erfüllungsgehilfen der KETESO (Art. 29, Art. 32 Abs. 4 DSGVO; § 278 BGB). Sie unterliegen der Vertraulichkeitsverpflichtung nach AVV § 6 und werden in dieser Liste nicht gesondert aufgeführt.

Reine Nebenleistungen ohne Zugriff auf personenbezogene Daten (z. B. Telekommunikation, Wartung ohne Datenzugriff, Entsorgung) sind ebenfalls keine Unter-Auftragsverarbeitung (siehe AVV § 8 Abs. 6).

Dokument PH-SUB, Version 1.2, Stand 12.10.2026, Status: Freigegeben zur Verwendung (anwaltlich geprüfte Fassung). Neu gegenüber Version 1.1: Unter-Auftragsverarbeiter Anthropic, Brevo, GitHub und Tally aufgenommen; Firmierung, Anschrift und Garantien der Supabase sowie die Anschrift der Vercel berichtigt; Vorbemerkung und Drittlandtransfer (Abschnitt 3) angepasst.