Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO)

Muster für die Beratung im Browser von Brief verstanden. Stand: 17. Oktober 2026

Zwischen

[Name der Organisation], [Anschrift] – „Verantwortlicher“

und

Marcin Weber, Kirschgartenstraße 27, 67146 Deidesheim, hallo@briefverstanden.app – „Auftragsverarbeiter“

§ 1 Gegenstand und Zweck

Der Auftragsverarbeiter erklärt im Rahmen der Beratung des Verantwortlichen Schriftstücke in einfacher Sprache und übersetzt sie (Beratung im Browser auf briefverstanden.app/beratung). Grundlage ist der Hauptvertrag nach den AGB für Organisationen.

§ 2 Art der Daten und Betroffene

- **Daten:** Inhalte von Briefen, E-Mails und Nachrichten als Foto, PDF oder Text. Sie können Namen, Anschriften, Aktenzeichen, Kontonummern, Beträge und im Einzelfall besondere Kategorien nach Art. 9 DSGVO enthalten (zum Beispiel Gesundheitsdaten). Dazu die dienstlichen E-Mail-Adressen der Mitarbeitenden für die Anmeldung.
- **Betroffene:** Klientinnen und Klienten des Verantwortlichen, in den Schriftstücken genannte Dritte, Mitarbeitende des Verantwortlichen.

§ 3 Dauer

Inhalte werden nur für die Dauer der einzelnen Anfrage verarbeitet und nicht gespeichert. Der Vertrag gilt so lange wie der Hauptvertrag.

§ 4 Weisungen

1. Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen. Die Nutzung der Beratung im Browser gilt als Weisung, die angefragte Erklärung zu erstellen.
2. Er nutzt die Daten für keine eigenen Zwecke, insbesondere nicht zum Training von KI und nicht für Werbung.
3. Hält er eine Weisung für rechtswidrig, teilt er das unverzüglich mit.

§ 5 Vertraulichkeit

Personen, die Zugang zu den Daten haben könnten, sind zur Vertraulichkeit verpflichtet. Zurzeit ist das nur der Auftragsverarbeiter selbst.

§ 6 Sicherheit

Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Anlage 1 (Art. 32 DSGVO). Er darf sie anpassen, wenn das Schutzniveau nicht sinkt.

§ 7 Unterauftragsverarbeiter

1. Der Verantwortliche stimmt den Unterauftragsverarbeitern in Anlage 2 zu.
2. Neue oder geänderte Unterauftragsverarbeiter teilt der Auftragsverarbeiter mindestens 4 Wochen vorher per E-Mail mit. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen; dann kann jede Seite den Hauptvertrag zum Änderungstermin kündigen.
3. Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich auf ein gleichwertiges Schutzniveau. Übermittlungen in die USA stützen sich auf das EU-US Data Privacy Framework oder EU-Standardvertragsklauseln.

§ 8 Unterstützung

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Anfragen betroffener Personen, bei der Datenschutz-Folgenabschätzung und bei Anfragen von Aufsichtsbehörden, soweit er dazu Informationen hat. Da Inhalte nicht gespeichert werden, kann er zu einzelnen Briefen in der Regel keine Auskunft geben.

§ 9 Datenschutzverletzungen

Der Auftragsverarbeiter meldet eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, per E-Mail an die Kontaktperson. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO.

§ 10 Löschung und Rückgabe

Inhalte von Schriftstücken werden nach jeder Anfrage verworfen. Bei Anthropic werden sie in der Regel spätestens nach 30 Tagen gelöscht. Anmeldedaten der Mitarbeitenden löscht der Auftragsverarbeiter mit Ende des Hauptvertrags, Abrechnungsdaten nach Ablauf der gesetzlichen Aufbewahrungsfristen.

§ 11 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt auf Anfrage alle Informationen bereit, die zum Nachweis dieser Pflichten nötig sind. Kontrollen vor Ort sind nach Absprache mit 4 Wochen Vorlauf möglich; jede Seite trägt ihre eigenen Kosten.

§ 12 Haftung

Die Haftung richtet sich nach Art. 82 DSGVO. Im Übrigen gelten die Haftungsregeln des Hauptvertrags.

§ 13 Schluss

Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag vor, soweit es um den Datenschutz geht. Änderungen bedürfen der Textform. Es gilt deutsches Recht.

[Ort, Datum, Unterschrift] – Verantwortlicher

[Ort, Datum, Unterschrift] – Auftragsverarbeiter

Anlage 1: Technische und organisatorische Maßnahmen

- **Keine Speicherung der Inhalte:** Fotos, Texte und Erklärungen werden weder auf dem Server noch im Browser gespeichert.
- **Verschlüsselung:** alle Verbindungen nur über HTTPS (TLS).
- **Zugang:** Anmeldung nur per persönlichem E-Mail-Link (15 Minuten gültig, einmal nutzbar), Sitzungen enden nach 30 Tagen, Anmelde- und Sitzungsschlüssel nur als Hash gespeichert, Sitzungs-Cookie HttpOnly.
- **Trennung:** jede Organisation und jeder Standort hat eigene Zähler; Mitarbeitende sehen keine Daten anderer Organisationen.
- **Verwaltung:** Zugriff auf die Verwaltung nur durch den Auftragsverarbeiter, mit eigenem Schlüssel.
- **Keine Inhalts-Protokolle:** Server-Protokolle enthalten keine Inhalte von Anfragen; gezählt werden nur Zahlen je Tag.
- **Missbrauchsschutz:** Begrenzung der Anfragen je Standort, Gerät und IP-Adresse.
- **Verfügbarkeit:** Betrieb auf der verteilten Infrastruktur von Cloudflare.

Anlage 2: Unterauftragsverarbeiter

Dienstleister	Aufgabe	Sitz	Grundlage für Übermittlung
Cloudflare, Inc., 101 Townsend St., San Francisco, USA	Hosting von Website und Server	USA	EU-US Data Privacy Framework, Standardvertragsklauseln
Anthropic PBC, 548 Market Street, San Francisco, USA	Erklärung mit der KI Claude; kein Training, Löschung in der Regel nach spätestens 30 Tagen	USA	Standardvertragsklauseln
Resend, Inc., USA	Versand von Anmelde-Links und Hinweis-Mails	USA	Standardvertragsklauseln