RECHTLICHES

Auftragsverarbeitungsvertrag

Wer ChatFlamingo einsetzt, verarbeitet personenbezogene Daten seiner Besucher. Dafür schreibt Art. 28 DSGVO einen Vertrag vor. Fassung vom 26. September 2026.

Vertragsparteien

Verantwortlicher ist der Kunde, der ChatFlamingo auf seiner Website einsetzt.

Auftragsverarbeiterin ist die CertoClav Sterilizer GmbH, Peintner Straße 10, 4060 Leonding, Österreich, FN 122912d, Landesgericht Linz.

Dieser Vertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen und gilt mit dem Anlegen eines Kontos als geschlossen.

Beim Anlegen des Kontos bestätigt der Verantwortliche diesen Vertrag ausdrücklich durch Anhaken eines eigenen Kästchens. Wir halten fest, wann und in welcher Fassung das geschehen ist, und stellen dem Verantwortlichen den Nachweis auf Anforderung zur Verfügung. Damit ist die Schriftform des Art. 28 Abs. 9 DSGVO in elektronischer Form gewahrt.

1. Gegenstand und Dauer

Gegenstand ist die Verarbeitung personenbezogener Daten, die beim Betrieb des Chat-Widgets auf der Website des Verantwortlichen anfallen. Die Verarbeitung dauert so lange wie der zugrunde liegende Vertrag.

2. Art und Zweck der Verarbeitung

Bereitstellung eines Chat-Widgets mit Live-Chat, Speicherung der Gesprächsverläufe, Anzeige der Besucher im Dashboard, Versand von E-Mail-Tickets sowie — sofern

vom Verantwortlichen aktiviert — automatische Beantwortung von Fragen durch ein Sprachmodell.

3. Kategorien betroffener Personen

- Besucherinnen und Besucher der Website des Verantwortlichen
- Beschäftigte des Verantwortlichen, die das Dashboard nutzen

4. Arten personenbezogener Daten

- Inhalte der Chat-Nachrichten und Gesprächsverläufe
- Kontaktdaten, soweit von Besuchern angegeben oder aus dem Gesprächstext erkannt (Name, E-Mail-Adresse, Telefonnummer)
- Nutzungsdaten: aufgerufene Seiten, Seitenverlauf, Verweildauer, Browser und Betriebssystem
- IP-Adresse und der daraus ermittelte ungefähre Standort, sofern die Standortermittlung nicht abgeschaltet ist
- von Besuchern hochgeladene Dateien und Bilder
- Zugangs- und Profildaten der Dashboard-Nutzer

Besondere Kategorien nach Art. 9 DSGVO sind nicht Gegenstand dieses Vertrags. Der Verantwortliche stellt sicher, dass solche Daten nicht planmäßig über den Chat erhoben werden.

5. Weisungen

Wir verarbeiten die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Als Weisung gelten auch die Einstellungen, die der Verantwortliche im Dashboard vornimmt. Halten wir eine Weisung für rechtswidrig, teilen wir das mit.

6. Vertraulichkeit

Alle Personen, die Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet.

7. Technische und organisatorische Maßnahmen

Die Maßnahmen nach Art. 32 DSGVO sind in Anlage 1 beschrieben. Zu den eingebauten Maßnahmen gehören insbesondere:

- eine eigene Datenbank je Kunde statt eines gemeinsamen Datenbestands
- Bindung des Widgets an die vom Verantwortlichen freigegebenen Domains
- vom Verantwortlichen einstellbare Löschfristen für Anhänge und ganze Gespräche
- abschaltbare Standortermittlung aus der IP-Adresse
- Rollen im Dashboard (Inhaber, Administrator, nur lesen)
- Begrenzung der Anfragen je Besucher und Sperrfunktion

Die vollständige Beschreibung steht in Anlage 1 am Ende dieses Vertrags.

8. Unterauftragsverarbeiter

Der Verantwortliche stimmt dem Einsatz der in Anlage 2 genannten Unterauftragsverarbeiter zu. Wechsel oder Hinzunahme teilen wir mit einer Frist von vier Wochen in Textform mit. Der Verantwortliche kann innerhalb dieser Frist aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Widerspricht er, können wir den Vertrag hinsichtlich der betroffenen Leistung zum Zeitpunkt des Wechsels kündigen; ein Anspruch auf Fortführung mit dem bisherigen Unterauftragsverarbeiter besteht nicht.

Die vollständige Liste steht in Anlage 2 am Ende dieses Vertrags.

9. Übermittlung in Drittländer

Die in Anlage 2 genannten Unterauftragsverarbeiter verarbeiten Daten auch in den Vereinigten Staaten. Grundlage der Übermittlung sind die Standardvertragsklauseln der Europäischen Kommission nach Art. 46 Abs. 2 lit. c DSGVO, die wir mit jedem dieser Empfänger abgeschlossen haben. Soweit ein Empfänger unter dem EU-US Data Privacy Framework zertifiziert ist, stützt sich die Übermittlung zusätzlich auf den Angemessenheitsbeschluss der Kommission vom 10. Juli 2023 nach Art. 45 DSGVO.

Ergänzend gelten: Verschlüsselung bei Übertragung und Speicherung, Beschränkung der übermittelten Daten auf das für die jeweilige Verarbeitung Erforderliche, keine Verwendung zu Trainingszwecken und die Pflicht des Empfängers, uns über behördliche

Auskunftsersuchen zu unterrichten, soweit das rechtlich zulässig ist. Wir unterrichten den Verantwortlichen unverzüglich, wenn uns eine solche Anfrage bekannt wird.

10. Unterstützung des Verantwortlichen

Wir unterstützen den Verantwortlichen im Rahmen des Möglichen bei der Beantwortung von Anfragen betroffener Personen sowie bei Datenschutz-Folgenabschätzungen und Meldepflichten nach Art. 32 bis 36 DSGVO.

11. Meldung von Verletzungen

Verletzungen des Schutzes personenbezogener Daten melden wir dem Verantwortlichen unverzüglich nach Bekanntwerden.

Die Meldung erfolgt spätestens 24 Stunden, nachdem uns die Verletzung bekannt geworden ist, in Textform an die im Dashboard hinterlegte Adresse. Sie enthält, soweit verfügbar, die Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen und die ergriffenen Maßnahmen. Liegen nicht alle Angaben vor, melden wir zuerst das Bekannte und reichen den Rest unverzüglich nach.

12. Löschung und Rückgabe

Nach Ende des Vertrags löschen wir die Daten oder geben sie zurück, je nach Wahl des Verantwortlichen, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Unabhängig davon greifen während der Vertragslaufzeit die vom Verantwortlichen eingestellten Löschfristen.

Der Verantwortliche teilt uns seine Wahl innerhalb von 30 Tagen nach Vertragsende mit. Innerhalb dieser Frist stellen wir eine maschinenlesbare Kopie der Daten zum Herunterladen bereit. Danach löschen wir die Daten einschließlich der Sicherungskopien spätestens innerhalb von weiteren 30 Tagen und bestätigen die Löschung auf Anforderung in Textform. Diese Frist entspricht Punkt 8.4 der Allgemeinen Geschäftsbedingungen.

13. Nachweise und Kontrollen

Wir stellen dem Verantwortlichen die zum Nachweis der Einhaltung erforderlichen Informationen zur Verfügung und ermöglichen Überprüfungen.

Überprüfungen kündigt der Verantwortliche mindestens zwei Wochen vorher in Textform an. Sie finden während unserer Geschäftszeiten statt, dürfen den Betrieb nicht unangemessen beeinträchtigen und erfolgen höchstens einmal je Kalenderjahr — außer es liegt ein konkreter Anlass vor, etwa eine gemeldete Verletzung oder eine Anordnung der Aufsichtsbehörde.

Wir können eine Überprüfung vor Ort durch aussagekräftige Nachweise ersetzen, insbesondere durch aktuelle Berichte unabhängiger Prüfer oder Zertifikate. Genügen diese dem Verantwortlichen nicht, bleibt sein Recht auf eine Prüfung vor Ort bestehen.

Jede Seite trägt ihre eigenen Kosten. Für den Aufwand einer anlasslosen Prüfung vor Ort können wir eine angemessene Vergütung verlangen.

14. Haftung

Für die Haftung aus diesem Vertrag gilt Punkt 12 der Allgemeinen Geschäftsbedingungen entsprechend.

Die Haftung nach Art. 82 DSGVO gegenüber betroffenen Personen bleibt davon unberührt. Im Innenverhältnis trägt jede Seite den Anteil, der ihrem Verantwortungsbeitrag entspricht.

Anlage 1 — Technische und organisatorische Maßnahmen

Maßnahmen nach Art. 32 DSGVO, Stand 26. September 2026.

Vertraulichkeit

- **Eigene Datenbank je Kunde.** Die Gespräche eines Kunden liegen nicht im selben Datenbestand wie die eines anderen. Eine Verwechslung über Kundengrenzen hinweg ist damit ausgeschlossen.
- **Domain-Bindung.** Das Widget läuft nur auf den Domains, die der Verantwortliche im Dashboard freigegeben hat. Anfragen von anderen Herkünften werden abgewiesen.

- **Zugriff nach Rollen.** Im Dashboard gibt es die Rollen Inhaber, Administrator und nur lesen. Jede Anmeldung erfolgt personenbezogen.
- **Zugriff auf unserer Seite nur nach Bedarf.** Mitarbeitende erhalten Zugriff auf Kundendaten nur, soweit das für Wartung und Störungsbehebung erforderlich ist, und sind zur Vertraulichkeit verpflichtet.

Integrität

- **Verschlüsselte Übertragung.** Alle Verbindungen laufen über TLS. Unverschlüsselte Aufrufe werden auf die verschlüsselte Adresse umgeleitet.
- **Verschlüsselte Speicherung.** Datenbanken und Sicherungen sind im Ruhezustand verschlüsselt.
- **Protokollierung.** Administrative Zugriffe auf Kundendaten werden protokolliert.
- **Missbrauchsbremse.** Begrenzung der Anfragen je Besucher, Monatsbudget je Konto, Sperrfunktion für einzelne Besucher.

Verfügbarkeit und Belastbarkeit

- **Sicherungen.** Tägliche Sicherung der Datenbanken; die Wiederherstellung wird regelmäßig erprobt.
- **Trennung der Umgebungen.** Entwicklung und Betrieb laufen getrennt. In der Entwicklung werden keine echten Kundendaten verwendet.

Löschung

- **Fristen durch den Verantwortlichen.** Löschfristen für Anhänge und ganze Gespräche stellt der Verantwortliche im Dashboard selbst ein; sie laufen automatisch ab.
- **Standortermittlung abschaltbar.** Ein Schalter im Dashboard beendet das Nachschlagen des ungefähren Standorts aus der IP-Adresse.
- **Nach Vertragsende.** Löschung nach Punkt 12 dieses Vertrags, einschließlich der Sicherungskopien.

Überprüfung

- Die Maßnahmen werden mindestens einmal jährlich und anlassbezogen überprüft und bei Bedarf angepasst. Der Stand dieser Anlage wird dabei fortgeschrieben.

Anlage 2 — Unterauftragsverarbeiter

Stand 26. September 2026.

Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107, USA · Auslieferung der Website und Schutz vor Angriffen · Verarbeitung weltweit, Standardvertragsklauseln
Salesforce, Inc. (Heroku)	415 Mission Street, San Francisco, CA 94105, USA · Betrieb der Anwendung und der Datenbanken · Rechenzentrum in der Europäischen Union, Standardvertragsklauseln
Anthropic PBC	San Francisco, CA, USA · Sprachmodell für die Antworten der KI · Verarbeitung in den USA, Standardvertragsklauseln, keine Verwendung zu Trainingszwecken
OpenAI Ireland Ltd.	1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, Irland · Sprachmodell für die Antworten der KI · Verarbeitung auch in den USA durch OpenAI, L.L.C., Standardvertragsklauseln, keine Verwendung zu Trainingszwecken

Für die Zahlungsabwicklung steht hier kein Unterauftragsverarbeiter: Die Zahlung läuft über die Stripe Payments Europe, Ltd. und — bei Buchung über den Shopify App Store — über die Shopify International Limited. Beide verarbeiten dabei die Vertragsdaten des Kunden, nicht die Daten seiner Website-Besucher, die Gegenstand dieses Vertrags sind. Eine externe Fehlerüberwachung ist derzeit nicht im Einsatz. Kommt ein Unterauftragsverarbeiter hinzu, gilt das Verfahren aus Punkt 8.