Teil C · Auftragsverarbeitung

Vereinbarung nach Art. 28 Abs. 3 DSGVO

Der Besteller ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO, die Egger Communications UG (haftungsbeschränkt) ist Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO. Diese Vereinbarung gilt für alle Leistungen der Egger Communications UG (haftungsbeschränkt) aus Teil A. Für eine Website-Erstellung durch Frederic Egger (Einzelunternehmen) wird, soweit dabei personenbezogene Daten im Auftrag verarbeitet werden, eine eigene Vereinbarung geschlossen.

1. Gegenstand, Dauer, Art und Zweck

1.1 Gegenstand ist die Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter zur Erbringung der bestellten Leistungen vornimmt. Die Dauer entspricht der Laufzeit der Hauptleistung.

1.2 Zweck ist die Bereitstellung und der Betrieb der Betriebssoftware sowie — soweit bestellt — Hosting, Website-Pflege und Marketingfunktionen. Die Art umfasst alle Verarbeitungsvorgänge im Sinne des Art. 4 Nr. 2 DSGVO.

1.3 Eine Verarbeitung zu eigenen Zwecken findet nicht statt. Die Daten werden insbesondere nicht zu Werbezwecken, nicht zur Profilbildung und **nicht zum Training von Systemen künstlicher Intelligenz** verwendet.

2. Daten und betroffene Personen

2.1 Verarbeitet werden insbesondere Stamm- und Kontaktdaten, Auftrags-, Liefer- und Rechnungsdaten, Zahlungsdaten, Vertrags- und Servicehistorie, hochgeladene Dokumente, Beschäftigtendaten sowie Anmelde- und Protokolldaten.

2.2 Betroffene Personen sind Kunden und Interessenten, Beschäftigte, Lieferanten und Geschäftspartner des Verantwortlichen sowie Besucher seiner Websites.

2.3 Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) verarbeitet der Auftragsverarbeiter nur, soweit der Verantwortliche sie in das System einstellt. Ist das Modul HR & Zeiterfassung gebucht, gehören dazu Angaben über Arbeitsunfähigkeitszeiten der Beschäftigten (Gesundheitsdaten). Der Verantwortliche stellt sicher, dass für diese Daten eine Rechtsgrundlage besteht (Art. 9 Abs. 2 DSGVO), und vergibt die Zugriffsrechte so, dass nur befugte Personen sie sehen.

3. Weisungsrecht

3.1 Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung. Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können danach in Textform geändert werden.

3.2 Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies unverzüglich mit und darf die Ausführung bis zur Klärung aussetzen.

3.3 Die Verarbeitung durch den Auftragsverarbeiter selbst findet in der Bundesrepublik Deutschland statt. Soweit die im Anhang genannten weiteren Auftragsverarbeiter außerhalb des Europäischen Wirtschaftsraums verarbeiten, geschieht dies auf Grundlage der Standardvertragsklauseln der EU-Kommission oder eines Angemessenheitsbeschlusses nach Art. 45 DSGVO; die Nachweise werden auf Verlangen vorgelegt.

4. Pflichten des Auftragsverarbeiters

4.1 **Vertraulichkeit.** Alle zur Verarbeitung befugten Personen werden vor Aufnahme der Tätigkeit schriftlich zur Vertraulichkeit verpflichtet; die Verpflichtung wirkt über das Ende der Tätigkeit hinaus.

4.2 **Unterstützung.** Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Anträgen betroffener Personen (Kapitel III DSGVO) sowie bei den Pflichten aus den Art. 32 bis 36 DSGVO.

4.3 **Meldung.** Verletzungen des Schutzes personenbezogener Daten werden unverzüglich mitgeteilt, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, mit den Angaben nach Art. 33 Abs. 3 DSGVO.

4.4 **Nach Beendigung.** Nach Abschluss der Leistungen werden die Daten nach Wahl des Verantwortlichen zurückgegeben oder gelöscht; ohne Wahl werden sie gelöscht. Löschfristen siehe Anhang; für das Service-Tool gilt Teil B § 10a. Eigene gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters bleiben unberührt.

4.5 **Dokumentation.** Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und legt es auf Verlangen vor.

4.6 **Betreuungszugang.** Für Wartung und Unterstützung unterhält der Auftragsverarbeiter in der Betriebssoftware zwei persönliche Betreuungszugänge (Frédéric Heinrich Egger, Eric Egger). Zugegriffen wird nur auf Bitte oder Weisung des Verantwortlichen, zur Behebung einer Störung oder zur Einspielung sicherheitsrelevanter Aktualisierungen; ein anlassloser Einblick in Inhaltsdaten findet nicht statt. Jede Anmeldung wird protokolliert und ist für den Verantwortlichen einsehbar; ein Zugriff ohne vorherige Anfrage wird ihm spätestens am folgenden Werktag mitgeteilt. Der Verantwortliche kann die Supportanmeldungen in den Grundeinstellungen jederzeit abschalten. Einzelheiten regelt Teil B § 6a.

5. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- Betrieb in Rechenzentren in Deutschland (STRATO GmbH) mit Zutrittskontrolle.
- Verschlüsselte Übertragung (TLS, 256 Bit) für alle Zugriffe.
- Persönliche Benutzerkonten, Rollen- und Rechtevergabe je Modul, Zwei-Faktor-Anmeldung wählbar.
- Mandantentrennung — jede Installation arbeitet auf einer eigenen Datenbank.
- Protokollierung sicherheitsrelevanter Vorgänge, gegen Änderung und Löschung gesichert.
- Getrennte Aufbewahrung der Sicherungen: Neben dem Server selbst liegt jede Sicherung in einem gesonderten Online-Speicher.
- Sicherung der Datenbanken und Dateien mindestens einmal täglich; Speicherort der Sicherungen: auf dem jeweiligen Server und täglich gespiegelt im Online-Speicher STRATO HiDrive der STRATO GmbH (Rechenzentren in Deutschland).
- Sperre wiederholter Fehlanmeldungen und regelmäßige Prüfung der Server auf Schadsoftware.
- Anmeldungen der Betreuung werden protokolliert und sind für den Verantwortlichen einsehbar; die Supportanmeldungen lassen sich in den Grundeinstellungen abschalten (Ziffer 4.6).
- Überprüfung und Bewertung der Wirksamkeit dieser Maßnahmen mindestens jährlich (Art. 32 Abs. 1 Buchst. d DSGVO).

6. Nachweis, Subunternehmer, Haftung

6.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind, insbesondere die aktuelle Dokumentation der Maßnahmen nach Ziffer 5. Er ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer, der kein Wettbewerber des Auftragsverarbeiters ist, und trägt dazu bei. Inspektionen vor Ort sind mindestens 14 Tage vorher anzukündigen, finden zu den üblichen Geschäftszeiten statt und sollen den Betrieb nicht unverhältnismäßig stören; ohne konkreten Anlass finden sie höchstens einmal im Kalenderjahr statt. Den Aufwand für Inspektionen vor Ort kann der Auftragsverarbeiter nach der jeweils gültigen Preisliste berechnen, es sei denn, die Prüfung ergibt einen erheblichen Verstoß.

6.2 Der Verantwortliche genehmigt allgemein den Einsatz weiterer Auftragsverarbeiter; die derzeit eingesetzten sind im Anhang mit Sitz, Leistung, Verarbeitungsort und Rechtsgrundlage aufgeführt. Änderungen werden vorab in Textform mitgeteilt; ein Widerspruch aus sachlichem Grund ist binnen 14 Tagen möglich. Widerspricht der Verantwortliche und kann der Auftragsverarbeiter die Leistung ohne den betreffenden Unterauftragsverarbeiter nicht in zumutbarer Weise erbringen, ist jede Partei berechtigt, den Vertrag zum Wirksamwerden der Beauftragung zu kündigen. Der Auftragsverarbeiter verpflichtet jeden weiteren Auftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die in dieser Vereinbarung festgelegt sind, insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Kommt ein weiterer Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes weiteren Auftragsverarbeiters.

6.3 Für die im Anhang genannten Dienste mit Sitz außerhalb der Bundesrepublik Deutschland gilt: Es werden nur die Inhalte übermittelt, die für die jeweilige Funktion nötig sind. Jede dieser Verbindungen lässt sich in den Grundeinstellungen einzeln abschalten; ist sie gesperrt, wird sie technisch nicht aufgebaut. An OpenAI werden Inhalte nur übermittelt, wenn ein Benutzer eine KI-Funktion im Einzelfall aufruft und den Abruf bestätigt (Teil B § 3 Abs. 2, § 3a). Daten aus dem Service-Tool werden nicht zum Training von Systemen künstlicher Intelligenz verwendet; dies ist mit dem betreffenden Anbieter vertraglich vereinbart.

6.4 Für die Haftung im Verhältnis der Parteien gilt Teil B § 7 entsprechend. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt, ebenso der Ausgleich nach Art. 82 Abs. 5 DSGVO, soweit er auf Vorsatz oder grober Fahrlässigkeit beruht. Bei Widersprüchen geht diese Vereinbarung vor, soweit sie die Verarbeitung personenbezogener Daten betrifft.

Anhang zu Teil C

Weitere Auftragsverarbeiter und Löschfristen

Weitere Auftragsverarbeiter

UNTERNEHMEN UND SITZ	LEISTUNG	ORT UND GRUNDLAGE
STRATO GmbH Otto-Ostrowski-Str. 7, 10249 Berlin	Server-, Hosting- und E-Mail-Infrastruktur; Online-Speicher HiDrive für die Sicherungskopien	Deutschland — Vereinbarung nach Art. 28 DSGVO
OpenAI Ireland Ltd. The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	Textfunktionen mit künstlicher Intelligenz, nur nach Bestätigung im Einzelfall; abschaltbar	Irland (EWR); Verarbeitung auch in den Vereinigten Staaten — Vereinbarung nach Art. 28 DSGVO mit Standardvertragsklauseln
DataForSEO OÜ Vesivärava tn 50-201, 10152 Tallinn, Estland	Messung von Suchmaschinen-Platzierungen; abschaltbar	Estland (EU); Unterauftragsverarbeiter teils Drittland — Vereinbarung nach Art. 28 DSGVO mit Standardvertragsklauseln

Die Verarbeitung durch den Auftragsverarbeiter selbst findet in der Bundesrepublik Deutschland statt; Software und Datenbanken laufen auf Servern der STRATO GmbH in Deutschland. Sicherungskopien werden ausschließlich in Deutschland gespeichert, und zwar: auf dem jeweiligen Server und täglich gespiegelt im Online-Speicher STRATO HiDrive der STRATO GmbH (Rechenzentren in Deutschland). Die Nachweise zu den vorstehenden Vereinbarungen werden auf Verlangen vorgelegt.

Anhang zu Teil C

Löschfristen je Leistung

LEISTUNG	ART DER DATEN	LÖSCHFRIST
Betriebssoftware	Stamm-, Auftrags-, Rechnungs- und Zahlungsdaten, Dokumente, Beschäftigtendaten	Herausgabe nach Teil B § 10a; Löschung nach Ablauf des Abrufzeitraums (mindestens 30 Kalendertage nach Ende des Übergangszeitraums bzw. ohne Wechselverlangen nach Vertragsende); in den Sicherungen mit Ablauf von deren Aufbewahrungsdauer. Eine Aufbewahrung über diesen Zeitpunkt hinaus erfolgt nur aufgrund eines gesondert vereinbarten Archivzugangs
Anmeldung und Protokoll	Benutzerkennung, Zeitstempel, IP-Adresse	12 Monate
E-Mail-Postfächer	E-Mail-Inhalte und -Anhänge, Adressdaten, Verbindungsdaten	Inhalte 30 Tage nach Vertragsende; Protokolldaten 6 Monate
Webspace und Website	Inhaltsdaten, Formularanfragen, Zugriffsprotokolle	Zugriffsprotokolle 7 Tage; Inhaltsdaten 2 Monate nach Vertragsende
Website-Pflege	Inhalte, Bild- und Videomaterial, Kontaktdaten der Ansprechpartner	Arbeitskopien 3 Monate nach Abschluss der Arbeit

Die Fristen gelten, soweit keine eigene gesetzliche Aufbewahrungspflicht des Auftragsverarbeiters entgegensteht. Auf Verlangen wird die Löschung in Textform bestätigt.