Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

1. Gegenstand und Dauer

Der Kunde (Verantwortlicher) beauftragt den Anbieter (Auftragsverarbeiter, Angaben siehe Impressum) im Rahmen des Dienstleistungsvertrags „KI-Experte im Abo“. Der AVV gilt, solange der Anbieter personenbezogene Daten im Auftrag des Kunden verarbeitet.

2. Art, Zweck und Umfang

Der Anbieter verarbeitet Daten, um Abläufe des Kunden zu analysieren, KI-Werkzeuge und Automatisierungen einzurichten, zu betreiben, zu warten und Mitarbeitende zu schulen.

- Arten von Daten: Kontakt- und Kommunikationsdaten, Vertrags- und Auftragsdaten, Inhalte von Dokumenten und Nachrichten, die der Kunde bereitstellt, Nutzungsdaten der eingerichteten Werkzeuge.
- Betroffene: Kunden, Interessenten, Lieferanten und Beschäftigte des Kunden.
- Besondere Kategorien (Art. 9 DSGVO) werden nur verarbeitet, wenn der Kunde das im Einzelfall schriftlich anweist.

Welche Programme des Kunden betroffen sind, welche Daten darin liegen und wo verarbeitet wird, steht in Anlage 3. Sie wird aus den Angaben des Kunden erzeugt. Kommt ein Programm hinzu oder ändert sich der Ort der Verarbeitung, bestätigt der Kunde die Anlage neu; erst danach verarbeitet der Anbieter Daten aus diesem Programm. Der Chat im Board ist nicht Gegenstand dieses Vertrags; für ihn gilt die Datenschutzerklärung.

3. Weisungen

Der Anbieter verarbeitet Daten nur auf dokumentierte Weisung des Kunden; Weisungen erteilt der Kunde im Board oder in Textform. Hält der Anbieter eine Weisung für rechtswidrig, teilt er das unverzüglich mit.

4. Pflichten des Anbieters

- Vertraulichkeit: Alle Personen, die Daten verarbeiten, sind zur Vertraulichkeit verpflichtet.
- Sicherheit: Der Anbieter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO (Anlage 1).
- Unterstützung: Er unterstützt den Kunden bei Anfragen Betroffener, bei Datenschutz-Folgenabschätzungen und bei Meldungen nach Art. 33 und 34 DSGVO.
- Meldung: Verletzungen des Schutzes personenbezogener Daten meldet er unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis.
- Nachweise: Er stellt die Informationen bereit, die zum Nachweis dieser Pflichten nötig sind, und ermöglicht Überprüfungen nach Absprache.

5. Unterauftragsverarbeiter

Der Kunde stimmt den Unterauftragsverarbeitern in Anlage 2 zu. Über neue oder geänderte Unterauftragsverarbeiter informiert der Anbieter mindestens 14 Tage vorher; der Kunde kann aus wichtigem Grund widersprechen. Der Anbieter verpflichtet Unterauftragsverarbeiter vertraglich auf dieses Schutzniveau. Übermittlungen in Drittländer erfolgen nur mit geeigneten Garantien nach Art. 44 ff. DSGVO.

6. Ende des Auftrags

Nach Vertragsende löscht der Anbieter alle Daten des Kunden oder gibt sie auf Wunsch zurück, soweit keine gesetzliche Aufbewahrungspflicht besteht. Rechnungen und Vertragsnachweise bewahrt er nach den handels- und steuerrechtlichen Fristen auf.

Anlage 1: Technische und organisatorische Maßnahmen

- Zugänge des Kunden erhält der Anbieter bevorzugt über eigene Konten oder Freigaben. Schickt der Kunde Zugangsdaten (Link, Datei, Fernwartungs-ID, API-Schlüssel, Login) über die Seite „Zugänge“ im Board, werden sie mit AES-256-GCM verschlüsselt gespeichert; der Schlüssel liegt getrennt von der Datenbank.
- Zugangsdaten sehen nur der Kunde und der Anbieter, jedes Anzeigen wird protokolliert. Löscht der Kunde einen Zugang, meldet der Anbieter ihn als nicht funktionierend oder endet der Vertrag, wird der gespeicherte Wert sofort gelöscht.
- Das Board ist nur nach Anmeldung erreichbar; Passwörter werden mit Argon2 gespeichert, Sitzungen laufen nach 30 Tagen ab.
- Jeder Kunde sieht nur seine eigenen Daten; Änderungen an Zugängen werden protokolliert.
- Benachrichtigungen per E-Mail enthalten keine Inhalte aus dem Board.
- Datensicherungen, Verschlüsselung der Übertragung (TLS) und Löschung nach Vertragsende.
- [Weitere Maßnahmen zu Hosting, Verschlüsselung der Datenträger und Notfallplan ergänzen.]

Anlage 2: Unterauftragsverarbeiter

- Hosting: eigener Server des Anbieters in Deutschland, kein Unterauftragsverarbeiter.
- Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA: Netzanbindung, Verschlüsselung und Schutz vor Angriffen; Anfragen an den Server laufen durch Cloudflare. Drittland USA: EU-US Data Privacy Framework und Standardvertragsklauseln.
- Proton AG, Route de la Galaise 32, 1228 Plan-les-Ouates, Schweiz: E-Mail-Postfach, Versand der Benachrichtigungen (Betreff und Link, keine Inhalte aus dem Board) und Videogespräche über Proton Meet (Ende-zu-Ende-verschlüsselt, ohne Aufzeichnung). Schweiz: Angemessenheitsbeschluss der EU-Kommission.
- [Anbieter der eingesetzten KI-Modelle, nur falls ein Projekt KI auf Daten des Kunden anwendet, z. B. Opper AB, Stockholm, mit EU-Route: Sitz, Zweck. Vom Anwalt zu prüfen.]

Stripe verarbeitet die Zahlungsdaten des Kunden als eigener Verantwortlicher und ist daher hier nicht aufgeführt.

Anlage 3: Programme und Daten dieses Kunden

Diese Anlage wird für jeden Kunden aus seinen Angaben im Board erzeugt: welche Programme, welche Daten, welche Betroffenen und wo verarbeitet wird. Jede Änderung bestätigt der Kunde neu.