Auftragsverarbeitungsvertrag

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Dokument-Version:	1.0
Gültig ab:	07.06.2026
Letzte Aktualisierung:	07.06.2026

§ 1 Vertragsparteien

Auftraggeber (Verantwortlicher)
Ihr Unternehmen

Auftragnehmer (Auftragsverarbeiter)
Samia Zahoor – Webentwicklung
Alsterkrugchaussee 595
22335 Hamburg, Deutschland
datenschutz@notizflow.de

Der Auftraggeber und der Auftragnehmer schließen den folgenden Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO (nachfolgend „AVV" oder „Vertrag").

§ 2 Gegenstand und Dauer der Verarbeitung

Gegenstand der Auftragsverarbeitung ist die Erbringung des SaaS-Dienstes „Notizflow" (KI-gestützte Meeting-Intelligenz) durch den Auftragnehmer für den Auftraggeber. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers.

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Nutzungsvertrags (Hauptvertrag) zwischen den Parteien.

§ 3 Art und Zweck der Verarbeitung

Die Verarbeitung umfasst folgende Tätigkeiten:

- Speicherung und Verarbeitung von Audioaufnahmen von Meetings
- Automatische Transkription von Audioaufnahmen (mittels KI-Diensten)
- KI-gestützte Zusammenfassung und Analyse von Transkripten
- Erstellung von strukturierten Gesprächsprotokollen und Action Items

- Speicherung der verarbeiteten Daten zur Anzeige im Nutzer-Dashboard
- Versand transaktionaler E-Mails im Zusammenhang mit der Dienstleistung

§ 4 Art der personenbezogenen Daten

Folgende Kategorien personenbezogener Daten werden verarbeitet:

- Name und E-Mail-Adresse des Nutzers (Konto-Daten)
- Audioaufnahmen von Meetings (können Stimmen und Namen von Gesprächspartnern enthalten)
- Transkripte und Zusammenfassungen (können Namen, Unternehmen, Projekt- und Vertriebsdaten enthalten)
- Meeting-Metadaten (Titel, Datum, Dauer, Teilnehmerliste)
- Nutzungsdaten (Login-Zeitstempel, verarbeitete Meeting-Anzahl)

§ 5 Kategorien betroffener Personen

- Nutzer des Auftraggebers (Mitarbeiter, Freiberufler)
- Gesprächspartner, die in den Aufnahmen erscheinen (Kunden, Interessenten, Geschäftspartner)

§ 6 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich insbesondere:

1. personenbezogene Daten ausschließlich nach dokumentierter Weisung des Auftraggebers zu verarbeiten;
2. alle zur Verarbeitung befugten Personen zur Vertraulichkeit zu verpflichten;
3. alle erforderlichen technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 DSGVO umzusetzen;
4. die Bedingungen des Art. 28 Abs. 2 und 4 DSGVO für das Hinzuziehen weiterer Auftragsverarbeiter einzuhalten;
5. den Auftraggeber bei der Erfüllung von Anfragen betroffener Personen (Art. 15–22 DSGVO) zu unterstützen;
6. den Auftraggeber bei Datenschutzverletzungen unverzüglich zu informieren;
7. alle Daten nach Beendigung des Hauptvertrags zu löschen oder zurückzugeben;
8. dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung bereitzustellen.

§ 7 Weitere Auftragsverarbeiter (Subunternehmer)

Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen. Der Auftragnehmer informiert den Auftraggeber über Änderungen und räumt ihm die Möglichkeit ein, Einwände zu erheben.

Zum Zeitpunkt des Vertragsabschlusses eingesetzte Subunternehmer:

- **Hetzner Online GmbH** (Hosting, Datenbank, Objektspeicher, lokale KI-Transkription) — Deutschland, AVV vorhanden
- **Anthropic / OpenAI via LiteLLM** (Zusammenfassung) — DPA + SCC falls Drittland
- **Stripe Payments Europe Ltd.** (Abrechnung) — Irland, DPA vorhanden
- **Resend** (E-Mail-Versand) — EU-Region, DPA vorhanden

§ 8 Technische und organisatorische Maßnahmen (TOMs)

Der Auftragnehmer hat folgende TOMs implementiert:

- TLS-Verschlüsselung aller Datenübertragungen (Let's Encrypt)
- Verschlüsselung der Datenbank und des Objektspeichers at rest (Hetzner)
- Passwörter ausschließlich mit bcrypt (cost 12) gespeichert
- Kurzzeitige JWT-Tokens (24 Stunden Gültigkeit)
- Rate Limiting und Zugriffsschutz auf alle API-Endpunkte
- Presigned URLs für Objektspeicher (kein öffentlicher Zugriff)
- Regelmäßige Datensicherungen (7 Tage rollend, verschlüsselt)
- Automatische Löschung von Audioaufnahmen nach 90 Tagen
- Zugriffskontrolle: Nur der Gründer hat Serverzugang in V1
- Passwortschutz auf allen administrativen Konten; Zwei-Faktor-Authentifizierung für zukünftige Teamzugänge geplant

§ 9 Weisungsrecht

Der Auftraggeber ist gegenüber dem Auftragnehmer weisungsbefugt bezüglich der Verarbeitung personenbezogener Daten. Weisungen erfolgen schriftlich oder per E-Mail. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich.

§ 10 Beendigung und Datenlöschung

Nach Beendigung des Hauptvertrags löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers spätestens innerhalb von 30 Tagen,

sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Auf Anfrage stellt der Auftragnehmer eine Löschbestätigung aus.

§ 11 Anwendbares Recht und Gerichtsstand

Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist Hamburg.

Auftraggeber (Verantwortlicher)	**Auftragnehmer (Auftragsverarbeiter)**
Ort, Datum, Unterschrift	Ort, Datum, Unterschrift
Ihr Unternehmen	Samia Zahoor · Notizflow