Auftragsverarbeitungsvertrag

gemäß Art. 28 Abs. 3 DSGVO — Version 2026-06-12

zwischen

[FIRMENNAME]
[STRASSE, PLZ ORT]
vertreten durch [ANSPRECHPARTNER]
— nachfolgend „Verantwortlicher“ —

und

conever
Nils Löhr
[ADRESSE]
— nachfolgend „Auftragsverarbeiter“ —

Datum: [DATUM]

Inhaltsverzeichnis

§ 1 Gegenstand und Dauer der Verarbeitung

1. Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Nutzung der Software „conever“ (nachfolgend „Software“).

2. conever ist ein webbasiertes Controlling-Tool für Film- und TV-Produktionsunternehmen zur Verwaltung von Projektbudgets, Kostenplanung, Cashflow-Management und Ergebnisrechnung.

3. Die Dauer der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrages (SaaS-Nutzungsvertrag) zwischen den Parteien.

4. Dieser Vertrag tritt mit Unterzeichnung beider Parteien in Kraft.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zum Zweck der Bereitstellung und des Betriebs der Software conever. Dies umfasst insbesondere:

- Benutzerverwaltung und Authentifizierung
- Zuordnung von Nutzern zu Mandanten (Kundenunternehmen)
- Zugriffskontrolle und Berechtigungsmanagement
- Speicherung und Verarbeitung projektbezogener Finanzdaten
- Protokollierung von Systemzugriffen

§ 3 Art der personenbezogenen Daten

Folgende Kategorien personenbezogener Daten werden im Rahmen der Auftragsverarbeitung verarbeitet:

Kategorie	Beschreibung
Stammdaten	Vor- und Nachname, E-Mail-Adresse
Zugangsdaten	Benutzerkonto, verschlüsselte Passwörter, Rollenzuordnung
Nutzungsdaten	Login-Zeitpunkte, Systemaktivität
Organisationsdaten	Mandantenzugehörigkeit, Rollenzuordnung im Unternehmen
Projektdaten	Projektbezogene Finanzdaten, Budgets, Kostenpositionen

§ 4 Kategorien betroffener Personen

Von der Verarbeitung betroffen sind folgende Personengruppen:

- Mitarbeiter und freie Mitarbeiter des Verantwortlichen
- Geschäftsführer und Produktionsleiter
- Controller und sonstige berechtigte Nutzer der Software
- Ansprechpartner bei externen Dienstleistern (soweit im System erfasst)

§ 5 Pflichten und Rechte des Verantwortlichen

1. Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung, verantwortlich.

2. Der Verantwortliche hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen sind in Textform zu dokumentieren.

3. Der Verantwortliche ist verpflichtet, dem Auftragsverarbeiter alle für die Verarbeitung erforderlichen Informationen unverzüglich mitzuteilen.

4. Der Verantwortliche hat dafür Sorge zu tragen, dass die Nutzerkonten und Zugangsdaten seiner Mitarbeiter vertraulich behandelt werden.

§ 6 Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist durch Unionsrecht oder das Recht der Mitgliedstaaten hierzu verpflichtet.

2. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind.

3. Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (siehe § 7).

4. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Betroffenenrechte (Art. 12–23 DSGVO) sowie bei Datenschutz-Folgenabschätzungen.

5. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Verletzungen des Schutzes personenbezogener Daten.

6. Der Auftragsverarbeiter löscht nach Beendigung des Auftrags alle personenbezogenen Daten, sofern keine gesetzliche Aufbewahrungspflicht besteht (siehe § 10).

§ 7 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter setzt folgende Maßnahmen gemäß Art. 32 DSGVO um:

Zugangs- und Zugriffskontrolle

- Authentifizierung über E-Mail und Passwort (Supabase Auth, bcrypt-Hashing)
- Passwort-Policy: mindestens 10 Zeichen, Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen; erzwungene Upgrades bei Policy-Änderung
- Verpflichtende Zwei-Faktor-Authentifizierung (TOTP) für alle Nutzer
- Trusted-Device-Mechanismus (30 Tage, Token-basiert) zur Reduktion wiederholter 2FA-Abfragen
- Rollenbasiertes Berechtigungssystem (RBAC): 10 Basisrollen und 3 Zusatzrollen, N:N-Zuordnung, scope-basierte Rechte
- Row Level Security (RLS) auf Datenbankebene — mandantenspezifische Datenisolierung
- Audit-Log für sicherheitsrelevante Aktionen (Login, Datenveränderungen, Exporte, Rollenänderungen)

Verschlüsselung und Übertragung

- TLS 1.3 für sämtliche Datenübertragungen (HTTPS, HSTS)

- Verschlüsselte Datenbankverbindungen (PostgreSQL mit SSL)
- Verschlüsselte Speicherung von Passwörtern (bcrypt)
- Verschlüsselte Server-Backups (täglich, Off-Site-Speicherung)

Server- und Netzwerksicherheit

- SSH-Zugang ausschließlich über Tailscale-VPN — Public Port 22 geschlossen
- SSH-Passwort-Authentifizierung deaktiviert (nur Public-Key)
- Firewall (UFW): ausschließlich Ports 80/443 öffentlich erreichbar
- fail2ban zur automatisierten Abwehr von Brute-Force-Angriffen
- Wöchentlicher Security-Scan (Lynis) mit Reporting
- Tägliche Datei-Integritätsprüfung

Verfügbarkeit und Belastbarkeit

- Server-Hosting: Hetzner Online GmbH, Rechenzentrum Nürnberg (Deutschland / EU)
- Supabase-Stack self-hosted (PostgreSQL, Auth, Storage, Edge Functions) — keine Daten außerhalb der EU
- Content Delivery über Netlify mit globalem CDN und europäischen Edge-Servern
- Automatische, verschlüsselte Backups (täglich, 30 Tage Retention, Off-Site)
- Externes Uptime-Monitoring mit Alerting

Mandantentrennung

- Vollständige Datentrennung auf Datenbankebene durch Row Level Security (RLS)
- Jeder Mandant kann ausschließlich auf seine eigenen Daten zugreifen
- Technische Durchsetzung auf PostgreSQL-Ebene — keine rein softwareseitige Trennung
- Tenant-ID als Pflichtfeld in jedem Datensatz — applikationsseitig erzwungen

§ 8 Unterauftragsverarbeiter

1. Der Verantwortliche stimmt dem Einsatz folgender Unterauftragsverarbeiter zu:

Unterauftragsverarbeiter	Zweck und Standort
Hetzner Online GmbH	Server-Hosting (PostgreSQL, Authentifizierung, Dateispeicherung, Edge Functions, Backups) — Rechenzentrum Nürnberg, Deutschland (EU)
Netlify, Inc.	Webhosting, CDN und Serverless Functions — globales CDN mit europäischen Edge-Servern; Standort USA (Standardvertragsklauseln)
Resend, Inc.	Transaktionaler E-Mail-Versand (SMTP, z. B. Einladungen, Benachrichtigungen) — Standort USA (Standardvertragsklauseln)
Anthropic PBC	KI-gestützte Analyse (optional, ausschließlich auf ausdrückliche Einwilligung des Nutzers; keine Trainingsnutzung) — Standort USA (Standardvertragsklauseln)

2. Der Auftragsverarbeiter wird den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf Unterauftragsverarbeiter informieren. Der Verantwortliche kann gegen solche Änderungen innerhalb von 14 Tagen Einspruch erheben.

3. Der Auftragsverarbeiter stellt sicher, dass mit jedem Unterauftragsverarbeiter vergleichbare Datenschutzpflichten vereinbart werden.

§ 9 Kontrollrechte des Auftraggebers

1. Der Verantwortliche hat das Recht, die Einhaltung der technischen und organisatorischen Maßnahmen sowie der vertraglichen Vereinbarungen zu überprüfen.

2. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

3. Inspektionen werden nach angemessener Vorankündigung (mindestens 14 Tage) und unter Berücksichtigung der Betriebsgeheimnisse des Auftragsverarbeiters durchgeführt.

4. Die Kosten einer Inspektion trägt der Verantwortliche, sofern kein Verstoß festgestellt wird.

§ 10 Löschung und Rückgabe von Daten

1. Nach Beendigung des Hauptvertrages löscht der Auftragsverarbeiter sämtliche personenbezogenen Daten des Verantwortlichen, sofern keine gesetzliche Aufbewahrungspflicht besteht.

2. Auf Wunsch des Verantwortlichen erfolgt vor der Löschung eine Rückgabe der Daten in einem maschinenlesbaren Format (CSV/Excel-Export).

3. Die Löschung wird dem Verantwortlichen schriftlich bestätigt.

4. Die Löschung erfolgt spätestens 30 Tage nach Vertragsende.

§ 11 Haftung

1. Die Haftung der Parteien richtet sich nach den gesetzlichen Bestimmungen der DSGVO, insbesondere Art. 82 DSGVO.

2. Der Auftragsverarbeiter haftet für Schäden, die durch eine nicht den Weisungen des Verantwortlichen entsprechende Verarbeitung oder durch Verstöße gegen die DSGVO verursacht werden.

3. Die Haftung des Auftragsverarbeiters ist auf den jährlichen Vertragswert begrenzt, soweit gesetzlich zulässig.

§ 12 Laufzeit und Kündigung

1. Dieser Vertrag gilt für die Dauer des Hauptvertrages (SaaS-Nutzungsvertrag).

2. Eine Kündigung des Hauptvertrages bewirkt automatisch die Beendigung dieses Auftragsverarbeitungsvertrages.

3. Das Recht zur außerordentlichen Kündigung bei schwerwiegenden Verstößen gegen Datenschutzbestimmungen bleibt unberührt.

4. Im Falle der Kündigung gelten die Regelungen des § 10 zur Löschung und Rückgabe der Daten.

§ 13 Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform.
2. Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
3. Es gilt das Recht der Bundesrepublik Deutschland.
4. Gerichtsstand ist [ORT].

Unterschriften

Für den Verantwortlichen:	**Für den Auftragsverarbeiter:**
Ort, Datum	Ort, Datum
[ANSPRECHPARTNER] *Verantwortlicher*	Nils Löhr *Auftragsverarbeiter — conever*