# Auftragsverarbeitungsvertrag

*gemäß Art. 28 DSGVO*

Stand: 27. März 2026

## Parteien

**Auftragsverarbeiter (AV):** vencly GmbH, Leopoldstraße 31, 80802 München

**Handelsregister:** HRB 290524, Amtsgericht München

**Geschäftsführer:** Clemens Eugen Theodor Pompeÿ

**USt-IdNr.:** DE367131457

**E-Mail:** datenschutz@vencly.com

**Auftraggeber/Verantwortlicher (AG):** [Firmenname des Kunden]

**Adresse:** [Straße, PLZ, Ort]

**Handelsregister:** [HRB … AG …]

**Vertreten durch:** [Geschäftsführer/Vorstand]

**E-Mail Datenschutz:** [datenschutz@…]

(Auftragsverarbeiter und Auftraggeber nachfolgend einzeln „Partei", gemeinsam „Parteien")

## § 1 Gegenstand und Dauer

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV") regelt die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit der Nutzung der SaaS-Plattform AutoToDo (autotodo.vercel.app), die vom Auftragsverarbeiter betrieben wird.

Der AVV gilt für die gesamte Laufzeit des zugrundeliegenden Hauptvertrags (Nutzungsvertrag AutoToDo) und endet automatisch mit dessen Beendigung.

## § 2 Art, Zweck und Gegenstand der Verarbeitung

| Feld | Beschreibung |
|---|---|
| Art der Verarbeitung | Erhebung, Speicherung, Analyse, Übermittlung, Löschung |
| Zweck | Verarbeitung von Meeting-Transkripten zur KI-gestützten Erstellung und Verwaltung von Listen offener Punkte (LOP); Export als XLSX |
| Kategorien betroffener Personen | Mitarbeiter und Gesprächsteilnehmer des Auftraggebers, soweit in Transkripten erwähnt |

| | |
|---|---|
| Kategorien personenbezogener Daten | Namen, Funktionsbezeichnungen, Gesprächsinhalte, Aufgabenzuweisungen aus Meeting-Protokollen |
| Ort der Verarbeitung | Frankfurt, Deutschland (EU); ggf. US-amerikanische KI-Anbieter bei BYOK (siehe § 7) |

## § 3 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich:

- Personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers zu verarbeiten (Art. 28 Abs. 3 lit. a DSGVO).
- Sicherzustellen, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.
- Alle erforderlichen technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 DSGVO umzusetzen (siehe Anlage 1).
- Die Bedingungen gemäß Art. 28 Abs. 2 und 4 DSGVO für die Inanspruchnahme von Unterauftragsverarbeitern einzuhalten (§ 6 dieses AVV).
- Den Auftraggeber unverzüglich zu informieren, wenn eine Weisung nach seiner Auffassung gegen datenschutzrechtliche Vorschriften verstößt.
- Den Auftraggeber bei der Erfüllung von Betroffenenanfragen (Art. 15–22 DSGVO) sowie bei der Meldung und Dokumentation von Datenschutzvorfällen zu unterstützen.
- Alle personenbezogenen Daten nach Beendigung des Vertrags zu löschen oder zurückzugeben, sofern keine gesetzliche Aufbewahrungspflicht besteht.
- Dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO bereitzustellen und Überprüfungen zu ermöglichen.

## § 4 Pflichten des Auftraggebers

Der Auftraggeber verpflichtet sich:

- Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in seinem Verantwortungsbereich sicherzustellen.
- Den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten feststellt.
- Weisungen an den Auftragsverarbeiter schriftlich (einschließlich E-Mail) zu erteilen.
- Die im BYOK-Modell verwendeten KI-API-Keys eigenverantwortlich zu verwalten und die Datenschutzkonformität des gewählten KI-Anbieters selbst sicherzustellen (§ 7).

## § 5 Technische und organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter implementiert mindestens die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Änderungen, die das Schutzniveau wesentlich herabsetzen, bedürfen der vorherigen Zustimmung des Auftraggebers.

| Maßnahme | Umsetzung |
|---|---|

| | |
|---|---|
| Transportverschlüsselung | TLS 1.3 mit HSTS (erzwungen) |
| Speicherverschlüsselung | AES-256-GCM mit Auth-Tag |
| Zugriffskontrolle | Row Level Security (RLS) auf Datenbankebene; Workspace-Isolation |
| Authentifizierung | 256-Bit kryptografisch sichere API-Token |
| Security-Header | HSTS, X-Frame-Options, X-Content-Type-Options (nosniff) |
| Serverstandort | Frankfurt, Deutschland (EU) |
| Datensparsamkeit | Keine Speicherung von Transkriptinhalten auf AV-Infrastruktur bei BYOK |
| Datenlöschung | Automatische Löschung 90 Tage nach Vertragsende |

## § 6 Unterauftragsverarbeiter

Der Auftraggeber erteilt hiermit die allgemeine Genehmigung für den Einsatz der nachfolgenden Unterauftragsverarbeiter. Der Auftragsverarbeiter informiert den Auftraggeber über beabsichtigte Änderungen mit angemessener Vorlaufzeit (mindestens 30 Tage). Der Auftraggeber kann Änderungen aus wichtigem datenschutzrechtlichem Grund widersprechen.

| Anbieter | Zweck / Standort / Rechtsgrundlage Drittlandtransfer |
|---|---|
| Vercel Inc., San Francisco, USA | Hosting und Betrieb der AutoToDo-Plattform; Grundlage: EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) |
| Supabase Inc. | Datenbankbetrieb; Serverstandort Frankfurt (EU); [SCCs sofern US-Entität tätig] |
| [Zahlungsanbieter TODO] | Zahlungsabwicklung; [Standort / Grundlage TODO] |

## § 7 BYOK – Verarbeitung durch KI-Drittanbieter

AutoToDo bietet ein Bring-Your-Own-Key-Modell (BYOK): Der Auftraggeber hinterlegt eigenverantwortlich einen API-Key eines KI-Anbieters (Anthropic Inc. oder OpenAI Inc.). Bei aktiviertem BYOK werden Transkriptinhalte direkt vom Browser des Endnutzers an den gewählten KI-Anbieter übermittelt; sie passieren nicht die Infrastruktur des Auftragsverarbeiters.

Für diese Übermittlung gilt:

- Der Auftraggeber ist alleiniger Verantwortlicher für die datenschutzrechtliche Zulässigkeit der Übermittlung an den gewählten KI-Anbieter.
- Es obliegt dem Auftraggeber, mit dem KI-Anbieter ggf. einen separaten Auftragsverarbeitungsvertrag abzuschließen.
- Anthropic: https://www.anthropic.com/privacy – Drittlandtransfer (USA) via EU-SCCs.
- OpenAI: https://openai.com/privacy – Drittlandtransfer (USA) via EU-SCCs.
- Der Auftragsverarbeiter haftet nicht für Datenschutzverstöße, die ausschließlich beim KI-Drittanbieter entstehen; § 3 Abs. 5 bleibt unberührt.

## § 8 Datenpannen und Meldepflichten

Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden, über Datenschutzverletzungen gemäß Art. 33, 34 DSGVO, die Daten des Auftraggebers betreffen. Die Meldung enthält mindestens:

- Art der Verletzung (soweit bekannt)
- Kategorien und ungefähre Anzahl betroffener Personen und Datensätze
- Wahrscheinliche Folgen der Verletzung
- Ergriffene oder vorgeschlagene Abhilfemaßnahmen

Der Auftraggeber ist für die Meldung an die zuständige Aufsichtsbehörde (BayLDA) verantwortlich.

---

## § 9 Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die Einhaltung der datenschutzrechtlichen Vorschriften und dieses AVV beim Auftragsverarbeiter in angemessenem Umfang selbst oder durch einen beauftragten Dritten zu überprüfen. Kontrollen sind mit einer Ankündigungsfrist von mindestens 14 Werktagen anzukündigen und dürfen den Betrieb des Auftragsverarbeiters nicht unverhältnismäßig beeinträchtigen. Kosten trägt der Auftraggeber.

Alternativ kann der Auftragsverarbeiter einen aktuellen Prüfbericht (ISO 27001, SOC 2 o. ä.) vorlegen, sofern vorhanden.

---

## § 10 Löschung und Rückgabe

Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter alle personenbezogenen Daten des Auftraggebers spätestens innerhalb von 90 Tagen, sofern keine gesetzliche Aufbewahrungspflicht besteht. Auf schriftliche Anforderung stellt der Auftragsverarbeiter dem Auftraggeber die Daten zuvor in einem gängigen Format zur Verfügung. Der Auftragsverarbeiter bestätigt die Löschung schriftlich.

---

## § 11 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO sowie den Haftungsregelungen des Hauptvertrags. Bei Datenschutzverletzungen, die ausschließlich dem Auftragsverarbeiter zuzurechnen sind, haftet dieser gegenüber dem Auftraggeber nach Maßgabe der gesetzlichen Bestimmungen. Haftungsbeschränkungen gelten nicht für Schäden aus grober Fahrlässigkeit, Vorsatz oder Verletzung von Körper, Leben oder Gesundheit.

---

## § 12 Schlussbestimmungen

Dieser AVV unterliegt deutschem Recht. Gerichtsstand ist München. Sollten einzelne Bestimmungen unwirksam sein, bleibt der AVV im Übrigen wirksam. Änderungen bedürfen der Schriftform. Im Konflikt zwischen AVV und Hauptvertrag hat der AVV in datenschutzrechtlichen Fragen Vorrang.

---

## Unterschriften

Durch ihre Unterschriften bestätigen die Parteien die Kenntnisnahme und Akzeptanz dieses Auftragsverarbeitungsvertrags.

| **Auftragsverarbeiter** | **Auftraggeber** |
|---|---|
| vencly GmbH | [Firmenname] |
| Leopoldstraße 31, 80802 München | [Adresse] |
| | |
| *Ort, Datum* | *Ort, Datum* |
| | |
| *Unterschrift, Stempel* | *Unterschrift, Stempel* |

# Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die folgenden Maßnahmen sind zum Zeitpunkt des Vertragsschlusses implementiert und werden fortlaufend dem Stand der Technik angepasst:

## 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zugriffskontrolle: Rollenbasierte Zugriffsverwaltung; Row Level Security auf Datenbankebene; Workspace-Isolation.
- Eingabekontrolle: Logging aller Datenbankzugriffe; Audittrail für sicherheitsrelevante Ereignisse.
- Weitergabekontrolle: Verschlüsselung aller Verbindungen via TLS 1.3 + HSTS; kein Transfer personenbezogener Daten ohne Rechtsgrundlage.
- Trennungsgebot: Logische Mandantentrennung; Daten verschiedener Kunden werden nicht gemeinsam verarbeitet.

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Übertragungsintegrität: TLS 1.3 mit AEAD-Cipher (AES-256-GCM); Auth-Tag verhindert unbemerkte Manipulation.
- Speicherintegrität: Verschlüsselte Speicherung mit Integritätsprüfung; regelmäßige Konsistenzprüfungen.

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitsziel: 99 % p.a. außerhalb geplanter Wartungsfenster.
- Backup: Tägliche Datensicherung mit 7-Tage-Aufbewahrung; Backup-Wiederherstellungstests quartalsweise.
- Skalierbarkeit: Automatische horizontale Skalierung über Vercel-Infrastruktur.

## 4. Verfahren zur Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Security-Header: HSTS, X-Frame-Options, X-Content-Type-Options (nosniff), CSP.
- Dependency-Scanning: Automatisiertes Scanning auf bekannte Schwachstellen in Abhängigkeiten.
- Incident-Response: Definierter Prozess zur Erkennung, Meldung und Behebung von Datenschutzverletzungen (Meldepflicht < 24 h intern).