

Vertrag zur Auftragsverarbeitung

nach Artikel 28 Datenschutz-Grundverordnung (DSGVO)

Version 1.0 - Stand 17. August 2026

1. Parteien und elektronischer Vertragsschluss

Auftraggeber (Verantwortlicher): Der Elektrofachbetrieb, dessen Firma und Anschrift beim elektronischen Abschluss dieses Vertrags im Instaplaner-Konto angegeben und im Annahmenachweis gespeichert werden. Die annehmende Person bestätigt, zur Vertretung dieses Betriebs berechtigt zu sein.

Auftragnehmer (Auftragsverarbeiter): MindTrajour UG (haftungsbeschränkt), Straße der Jugend 18, 14974 Ludwigsfelde, Deutschland, eingetragen beim Amtsgericht Potsdam unter HRB 38673, vertreten durch die Geschäftsführer Larissa Lange und Adrian Rinnus, E-Mail: info@mindtrajour.com.

Dieser Vertrag wird elektronisch abgeschlossen. Der vom Auftragnehmer gespeicherte Annahmenachweis mit Benutzerkonto, Firma und Anschrift des Auftraggebers, E-Mail-Adresse der annehmenden Person, Vertragsversion, SHA-256-Prüfsumme des Vertragsdokuments und Annahmezeitpunkt ist Bestandteil dieses Vertrags. Beide Parteien können das unveränderte Vertragsdokument elektronisch speichern und ausdrucken.

2. Gegenstand, Rang und Dauer

1. Der Auftragnehmer stellt dem Auftraggeber die cloudbasierte Anwendung Instaplaner zur Erfassung, Bearbeitung und Ausgabe von Stromlauf- und Verteilungsplänen einschließlich optionaler Sprach- und KI-Verarbeitung bereit.
2. Soweit der Auftragnehmer dabei personenbezogene Daten verarbeitet, für deren Zwecke und wesentliche Mittel der Auftraggeber verantwortlich ist, erfolgt die Verarbeitung ausschließlich im Auftrag des Auftraggebers nach diesem Vertrag.
3. Für Kontodaten, Abrechnung, eigene Sicherheits- und Missbrauchsprävention sowie in der Datenschutzerklärung bezeichnete eigene Telemetriezwecke kann der Auftragnehmer selbst Verantwortlicher sein. Diese Verarbeitungen sind nicht Gegenstand dieses Vertrags.
4. Dieser Vertrag ergänzt den Hauptvertrag über Instaplaner. Bei Widersprüchen gehen die Regelungen dieses Vertrags für die Auftragsverarbeitung vor.
5. Der Vertrag gilt ab elektronischer Annahme für die Dauer des Hauptvertrags und darüber hinaus, solange der Auftragnehmer noch Auftragsdaten verarbeitet oder gesetzlich aufbewahren muss.

3. Beschreibung der Verarbeitung

Gegenstand, Zweck, Art und Dauer der Verarbeitung, Kategorien betroffener Personen und Datenarten sind in Anlage 1 festgelegt. Die dortige Beschreibung gilt zugleich als dokumentierte Anfangsweisung des Auftraggebers.

4. Weisungen

1. Der Auftragnehmer verarbeitet Auftragsdaten nur auf dokumentierte Weisung des Auftraggebers, einschließlich hinsichtlich einer Übermittlung in ein Drittland oder an eine internationale Organisation, sofern keine Verpflichtung nach dem Recht der Europäischen Union oder eines Mitgliedstaats besteht. In diesem Fall informiert der Auftragnehmer den Auftraggeber vor der Verarbeitung, soweit das betreffende Recht dies nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.
2. Weisungen ergeben sich aus diesem Vertrag, dem Hauptvertrag, den vom Auftraggeber gewählten Produktfunktionen und Einstellungen sowie ergänzenden Weisungen in Textform an info@mindtrajour.com.
3. Hält der Auftragnehmer eine Weisung für einen Verstoß gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder ihrer Mitgliedstaaten, informiert er den Auftraggeber unverzüglich. Er darf die Ausführung bis zur Bestätigung oder Änderung der Weisung aussetzen.
4. Führt eine zusätzliche Weisung zu einem nicht vom Hauptvertrag umfassten Aufwand, informiert der Auftragnehmer vorab über die voraussichtlichen Kosten. Gesetzlich geschuldete Unterstützung bleibt unberührt.

5. Pflichten des Auftraggebers

1. Der Auftraggeber bleibt für die Rechtmäßigkeit der Erhebung und Verarbeitung der Auftragsdaten, die Erfüllung der Informationspflichten und die Wahrung der Betroffenenrechte verantwortlich.
2. Der Auftraggeber darf nur Daten eingeben, die für seine fachlichen Zwecke erforderlich sind, und muss Nutzerkonten, Endgeräte und Zugangsdaten angemessen schützen.
3. Besondere Kategorien personenbezogener Daten nach Artikel 9 DSGVO und Daten über strafrechtliche Verurteilungen nach Artikel 10 DSGVO sind nicht für die planmäßige Verarbeitung vorgesehen. Ihre gezielte Eingabe bedarf einer vorherigen dokumentierten Vereinbarung.
4. Der Auftraggeber informiert den Auftragnehmer unverzüglich über erkannte Fehler, Unregelmäßigkeiten oder datenschutzrechtliche Anforderungen, die die Auftragsverarbeitung betreffen.

6. Vertraulichkeit und Zugriffsbindung

1. Der Auftragnehmer gewährleistet, dass zur Verarbeitung befugte Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
2. Zugriff auf Auftragsdaten erhalten nur Personen, soweit dies für Betrieb, Support, Sicherheit oder die Erfüllung dieses Vertrags erforderlich ist. Berechtigungen werden nach dem Erforderlichkeitsprinzip vergeben und bei Wegfall des Bedarfs entzogen.
3. Der Auftragnehmer unterrichtet die eingesetzten Personen über die besonderen Datenschutzpflichten und stellt sicher, dass Auftragsdaten nicht eigenmächtig verarbeitet werden.

7. Sicherheit der Verarbeitung

1. Der Auftragnehmer trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen (TOMs). Sie gewährleisten unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umständen, Zwecken und Risiken ein dem Risiko angemessenes Schutzniveau nach Artikel 32 DSGVO.
2. Der Auftragnehmer darf die TOMs an technische Entwicklungen anpassen, wenn das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche nachteilige Änderungen teilt er dem Auftraggeber vorab mit.
3. Der Auftraggeber ist für die sichere Konfiguration und Nutzung der ihm zugänglichen Funktionen, insbesondere die Geheimhaltung seiner Zugangsdaten und die Sicherheit seiner Endgeräte, verantwortlich.

8. Unterstützung des Auftraggebers

1. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu beantworten.
2. Geht ein Betroffenenantrag unmittelbar beim Auftragnehmer ein und betrifft er erkennbar Auftragsdaten, leitet der Auftragnehmer ihn unverzüglich an den Auftraggeber weiter. Er antwortet nicht selbst, außer auf dokumentierte Weisung oder aufgrund gesetzlicher Verpflichtung.
3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der ihm verfügbaren Informationen bei der Einhaltung der Artikel 32 bis 36 DSGVO, insbesondere bei Sicherheitsbewertungen, Datenschutz-Folgenabschätzungen und erforderlichen Konsultationen von Aufsichtsbehörden.
4. Der Auftragnehmer informiert den Auftraggeber, wenn ihm bekannt wird, dass verarbeitete Auftragsdaten unrichtig oder veraltet sind und dies für den vereinbarten Zweck erheblich ist.

9. Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes von Auftragsdaten unverzüglich nach Bekanntwerden. Die Meldung enthält, soweit zu diesem Zeitpunkt verfügbar, Art und Umfang des Vorfalls, betroffene Daten und Personen, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen und eine Kontaktstelle.
2. Fehlende Angaben werden ohne unangemessene Verzögerung nachgereicht. Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei dessen Pflichten nach Artikel 33 und 34 DSGVO.
3. Die Meldung stellt kein Anerkenntnis eines Verschuldens oder einer Haftung dar.

10. Rückgabe und Löschung

1. Während der Vertragslaufzeit kann der Auftraggeber die in Instaplaner bereitgestellten Export- und Druckfunktionen nutzen. Soweit ein erforderlicher Export technisch nicht verfügbar ist, unterstützt der Auftragnehmer auf angemessene Anfrage.
2. Nach Beendigung des Hauptvertrags löscht oder gibt der Auftragnehmer nach Wahl des Auftraggebers alle Auftragsdaten zurück und löscht vorhandene Kopien, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Bis zur Löschung werden zurückbehaltene Daten gesperrt und nur zur Erfüllung der gesetzlichen Pflicht verarbeitet.
3. Flüchtige Sprachaufnahmen werden nach der Transkription aus dem Arbeitsspeicher entfernt. Projektdaten werden bei Löschung des Projekts oder Kontos aus der aktiven Datenbank entfernt. Sicherungs- und Wiederherstellungskopien werden nach den dokumentierten Zyklen der eingesetzten Infrastruktur überschrieben oder gelöscht.
4. Der Annahmenachweis dieses Vertrags wird als eigener Vertrags- und Rechenschaftsnachweis während der Geschäftsbeziehung und anschließend entsprechend gesetzlicher Aufbewahrungs- und Verjährungsfristen gespeichert. Er gehört nicht zu den auf Weisung zu löschenden Auftragsdaten.

11. Nachweise und Kontrollen

1. Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung von Artikel 28 DSGVO nachzuweisen. Dazu können dieser Vertrag, TOM-Dokumentationen, Prüfberichte, Zertifikate und geeignete Auskünfte gehören.
2. Der Auftraggeber darf die Einhaltung selbst oder durch einen unabhängigen, fachkundigen und zur Vertraulichkeit verpflichteten Prüfer kontrollieren. Regelprüfungen sind mit angemessener Vorankündigung während üblicher Geschäftszeiten durchzuführen. Bei einem konkreten Sicherheitsvorfall oder begründeten Verdacht gelten diese

Beschränkungen nur, soweit sie die wirksame Kontrolle nicht vereiteln.

3. Der Auftragnehmer trägt aktiv zu Kontrollen und behördlichen Prüfungen bei. Soweit gleichwertige Nachweise eine Vor-Ort-Prüfung ersetzen können, sollen diese vorrangig genutzt werden.
4. Verursacht eine Prüfung ohne festgestellten Verstoß einen erheblichen Zusatzaufwand, kann der Auftragnehmer angemessene, vorab mitgeteilte Kosten verlangen. Dies gilt nicht, soweit die Prüfung durch einen Verstoß des Auftragnehmers erforderlich wurde.

12. Unterauftragsverarbeiter

1. Der Auftraggeber erteilt die allgemeine schriftliche Genehmigung, die in Anlage 3 konkret bezeichneten Unterauftragsverarbeiter für die dort beschriebenen Leistungen einzusetzen.
2. Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage vor der beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters unaufgefordert per E-Mail. Die Information enthält Firma, Anschrift, Aufgabe und vorgesehenen Verarbeitungsort.
3. Der Auftraggeber kann innerhalb von 14 Tagen nach Zugang aus sachlichen Datenschutzgründen widersprechen. Die Parteien versuchen zunächst, die Bedenken durch Schutzmaßnahmen oder eine zumutbare Alternative zu lösen. Ist dies nicht möglich, kann jede Partei den betroffenen Dienst ohne Belastung für zukünftige Leistungszeiträume beenden.
4. Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter durch Vertrag im Wesentlichen zu denselben Datenschutzpflichten, stellt dessen hinreichende Garantien sicher und bleibt gegenüber dem Auftraggeber für die Erfüllung der Pflichten verantwortlich.
5. Reine Nebenleistungen ohne Zugriffsmöglichkeit auf Auftragsdaten, etwa Telekommunikation, Post, Reinigung oder allgemeine Zahlungsabwicklung, sind keine Unterauftragsverarbeitung im Sinne dieser Regelung.

13. Drittlandübermittlungen

1. Eine Verarbeitung außerhalb des Europäischen Wirtschaftsraums erfolgt nur unter Einhaltung von Kapitel V DSGVO und auf dokumentierter Weisung nach diesem Vertrag.
2. Soweit kein Angemessenheitsbeschluss besteht, verwendet der Auftragnehmer insbesondere die Standardvertragsklauseln der Europäischen Kommission nach Durchführungsbeschluss (EU) 2021/914 in der jeweils anwendbaren Modulkonstellation und prüft erforderliche zusätzliche Maßnahmen.
3. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die wesentlichen Informationen zum Übermittlungsinstrument, zu Verarbeitungsorten und zusätzlichen Schutzmaßnahmen zur Verfügung, soweit Rechte Dritter und Sicherheitsinteressen dem nicht entgegenstehen.

14. Schlussbestimmungen

1. Änderungen dieses Vertrags bedürfen mindestens der Textform oder eines gleichwertig dokumentierten elektronischen Abschlusses. Eine neue Vertragsversion wird nicht allein durch Veröffentlichung wirksam, sondern muss vom Auftraggeber angenommen werden, soweit die Änderung nicht ausschließlich begünstigend oder redaktionell ist.
2. Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt der Vertrag im Übrigen wirksam. Die Parteien ersetzen die Bestimmung durch eine wirksame Regelung, die dem datenschutzrechtlichen Zweck am nächsten kommt.
3. Es gilt deutsches Recht. Zwingende Zuständigkeiten der Datenschutzaufsichtsbehörden und Gerichte bleiben unberührt.

Anlage 1 - Einzelheiten der Verarbeitung

A. Gegenstand und Zweck

- Bereitstellung einer mandantengeschützten Projektverwaltung für elektrische Anlagen.
- Erfassung, Strukturierung, Bearbeitung, Versionierung, Anzeige und PDF-Ausgabe von Stromlauf- und Verteilungsplänen.
- Optionale Transkription von Sprachaufnahmen und Erzeugung strukturierter, vom Nutzer zu bestätigender Änderungsvorschläge durch KI-Modelle.
- Support, Fehlerbehebung, Datensicherung, Wiederherstellung und Löschung, soweit hierfür Auftragsdaten verarbeitet werden müssen.

B. Art der Verarbeitung

Erheben und Erfassen durch Eingabe oder Sprache, Übermitteln, Speichern, Ordnen, Strukturieren, Auslesen, Abfragen, Verwenden, Abgleichen, Verknüpfen, Erzeugen technischer Vorschläge und Plandokumente, Einschränken, Exportieren und Löschen. Rohaudio wird nur vorübergehend im Arbeitsspeicher verarbeitet und nicht planmäßig dauerhaft gespeichert.

C. Dauer und Häufigkeit

Die Verarbeitung erfolgt bei Nutzung fortlaufend für die Dauer des Hauptvertrags. Rohaudio wird nur für die Dauer des jeweiligen Transkriptionsvorgangs verarbeitet. Projektdaten bleiben bis zur Löschung durch den Auftraggeber, zur Kontolöschung oder Vertragsbeendigung gespeichert; gesetzlich erforderliche oder technisch unvermeidbare Sicherungskopien werden anschließend nach den vorgesehenen Löschzyklen entfernt.

D. Kategorien betroffener Personen

- Kunden und Auftraggeber des Elektrofachbetriebs.
- Eigentümer, Mieter, Bewohner, Nutzer und Ansprechpartner der bearbeiteten Objekte.
- Beschäftigte, freie Mitarbeitende und Nachunternehmer des Auftraggebers.
- Sonstige Personen, deren Angaben oder Stimmen unbeabsichtigt in einer Sprachaufnahme enthalten sind.

E. Kategorien personenbezogener Daten

- Stamm- und Kontaktdaten wie Namen, Firma, Objekt- und Kontaktanschriften.
- Projekt- und Vertragsbezug, Projektbezeichnungen, Zeichnungsnummern und Zuordnung zu Objekten.
- Technische Anlagen-, Plan- und Dokumentationsdaten, soweit sie einer Person oder einem bewohnten Objekt zugeordnet werden können.
- Sprachaufnahmen, Stimmen und darin enthaltene Angaben während der flüchtigen Transkription.
- Transkripte, Prompts, Kontextdaten und KI-Antworten während der Verarbeitung eines Änderungsvorschlags.
- Nutzerkennungen und technische Sicherheitsmetadaten, soweit sie zur weisungsgebundenen Bereitstellung und Absicherung erforderlich sind.
- Optional hochgeladene Firmenbezeichnungen, Anschriften und Logos, soweit sie Personenbezug aufweisen.

F. Besondere Datenkategorien

Besondere Kategorien nach Artikel 9 DSGVO und Daten nach Artikel 10 DSGVO sind nicht Gegenstand der planmäßigen Verarbeitung. Sie können bei offenen Spracheingaben unbeabsichtigt vorkommen. Der Auftraggeber weist seine Nutzer an, solche Angaben nicht einzugeben; der Auftragnehmer verwendet sie nicht zu eigenen Zwecken und löscht sie nach den allgemeinen Regeln für Audio und Transkripte.

G. Verantwortliche Kontaktstellen

Auftragnehmer: info@mindtrajour.com. Die Kontaktstelle des Auftraggebers ist die im Instaplaner-Konto hinterlegte geschäftliche E-Mail-Adresse, soweit keine andere Adresse in Textform mitgeteilt wird.

Anlage 2 - Technische und organisatorische Maßnahmen

A. Zutritts-, Zugangs- und Zugriffskontrolle

- Produktive Infrastruktur wird in kontrollierten Rechenzentren der in Anlage 3 genannten Anbieter betrieben; der Auftragnehmer betreibt keine eigenen Serverräume für Auftragsdaten.
- Zugriff auf die Anwendung erfordert ein verifiziertes, individuell zugeordnetes Supabase-Auth-Konto. Die öffentliche Registrierung ist deaktiviert; Pilotkonten werden nur kontrolliert freigeschaltet.
- Sitzungen werden serverseitig geprüft. Authentifizierungsinformationen werden in geschützten Cookies verarbeitet; privilegierte Service-Schlüssel werden nicht an den Browser ausgeliefert.
- Projekt- und Revisionszugriffe werden serverseitig an die verifizierte Benutzerkennung gebunden. PostgreSQL Row Level Security, eingeschränkte RPC-Berechtigungen und negative Datenbanktests verhindern den Zugriff auf Daten anderer Konten.
- Der Zugriff des Auftragnehmers auf Produktionssysteme und Anbieter-Dashboards ist auf berechtigte Personen und den betrieblich erforderlichen Umfang beschränkt.

B. Verschlüsselung und Übertragung

- Browser, Anwendungsserver und externe Dienste kommunizieren über verschlüsselte HTTPS/TLS-Verbindungen.
- Datenbanken und verwaltete Speicherdienste verwenden die Verschlüsselungsmechanismen der jeweiligen Infrastruktur für ruhende Daten.
- Geheimnisse und API-Schlüssel werden ausschließlich in geschützten Hosting-Umgebungsvariablen oder Anbieter-Geheimnisspeichern gehalten und nicht in das Repository oder Client-Bundles aufgenommen.

C. Mandantentrennung und Datenminimierung

- Das aktuelle Pilotmodell ordnet jedes Konto einem Betrieb zu; Zugriffe auf Projekte werden aus der serverseitig verifizierten Benutzerkennung abgeleitet und nicht aus frei wählbaren Client-IDs.
- Öffentliche Schemas enthalten keine frei lesbaren Projekttabellen. Bewusst freigegebene API-Funktionen liefern nur die für den jeweiligen Anwendungsfall erforderlichen Daten.
- Fehler- und Leistungsdaten enthalten keine planmäßigen Audio-, Transkript-, Prompt-, Modellantwort- oder Planinhalte. Zugangsdaten, Schlüssel, vollständige URLs und Suchparameter werden aus technischen Meldungen entfernt oder maskiert.
- Rohaudio wird nur im Arbeitsspeicher gehalten, nach der Transkription überschrieben und weder in Datei- noch Objektspeicher oder Anwendungsprotokolle geschrieben.
- KI-Anfragen fordern, soweit vom Anbieter unterstützt, Zero Data Retention und den Ausschluss von Training oder anderweitiger Datensammlung an. Inhaltsprotokollierung ist nicht aktiviert.

D. Integrität und Nachvollziehbarkeit

- Eingaben werden vor Datenbank- und KI-Verarbeitung anhand definierter Schemas und fachlicher Regeln validiert.
- Elektrische Planstände werden als unveränderliche Revisionen mit Versionsnummer und SHA-256-Inhaltsprüfsumme gespeichert. Änderungen erzeugen neue Revisionen statt bestehende Nachweise unbemerkt zu überschreiben.
- Schemaänderungen erfolgen durch versionierte, vorwärtsgerichtete Datenbankmigrationen. Berechtigungsänderungen werden mit positiven und negativen pgTAP-Tests geprüft.
- Der elektronische AVV-Abschluss speichert Vertragsversion, Dokumentprüfsumme, Vertragsparteien-Snapshot und Annahmezeitpunkt unveränderlich je Version.

E. Verfügbarkeit, Wiederherstellung und Belastbarkeit

- Die Anwendung nutzt verwaltete Hosting- und Datenbankdienste mit Anbietermaßnahmen für Verfügbarkeit, Redundanz, Wiederherstellung und Schutz vor Infrastrukturstörungen.
- Fehler werden inhaltsminimiert erfasst, damit technische Ausfälle erkannt und behoben werden können.
- Datenbankänderungen und kritische Nutzerflüsse werden vor Auslieferung automatisiert geprüft. Wiederherstellungs- und Exportmöglichkeiten werden risikoorientiert bewertet.
- Ein bestimmter Wiederherstellungszeitpunkt oder eine unterbrechungsfreie Verfügbarkeit wird nur geschuldet, wenn dies im Hauptvertrag ausdrücklich vereinbart ist.

F. Löschung und Speicherbegrenzung

- Nutzer können Projekthinhalte über die Anwendung ausgeben; Projekt- und Kontolöschungen entfernen die zugeordneten aktiven Datensätze kaskadierend.
- Rohaudio wird unmittelbar nach dem Transkriptionsvorgang aus dem Arbeitsspeicher entfernt. Transkripte und KI-Antworten werden nicht in Inhaltsprotokollen gespeichert.
- Bei Vertragsende werden Auftragsdaten nach Abschnitt 10 gelöscht oder zurückgegeben. Verbleibende Anbieter-Sicherungen werden nach deren dokumentierten Zyklen überschrieben.
- Vertrags- und Annahmennachweise werden getrennt von Projektdaten und nur für Rechenschaft, Vertragsnachweis und gesetzliche Aufbewahrung gespeichert.

G. Sicherheitsorganisation und Vorfallmanagement

- Zur Datenverarbeitung befugte Personen sind auf Vertraulichkeit und den zulässigen Verarbeitungsumfang verpflichtet.
- Sicherheits- und Datenschutzvorfälle werden aufgenommen, bewertet, eingedämmt, dokumentiert und nach Abschnitt 9 an den Auftraggeber gemeldet.
- Sicherheitsrelevante Fehlerausgaben werden redigiert, damit keine Geheimnisse oder Auftragsinhalte in Telemetrie gelangen.
- Abhängigkeiten, Zugriffsregeln, Datenbankrichtlinien und technische Schutzmaßnahmen werden bei wesentlichen Produkt- oder Anbieteränderungen überprüft.

H. Unterstützung bei Betroffenenrechten

- Eigentümergebundene Datenzugriffe ermöglichen die gezielte Suche, Berichtigung, Ausgabe und Löschung der einem Konto zugeordneten Projektdaten.
- Supportanfragen werden anhand der verifizierten Kontokennung zugeordnet. Daten werden nicht allein anhand frei mitgeteilter fremder Kennungen offengelegt oder gelöscht.
- Der Auftragnehmer unterstützt den Auftraggeber bei Auskunft, Berichtigung, Einschränkung, Übertragbarkeit und Löschung im technisch verfügbaren Umfang.

Anlage 3 - Genehmigte Unterauftragsverarbeiter

1. Vercel Inc.

Anschrift: 440 N Barranca Avenue #4133, Covina, CA 91723, USA. **Aufgabe:** Hosting und Auslieferung der Webanwendung, serverseitige Ausführung von Anwendungslogik, Verarbeitung von Anfragen im Arbeitsspeicher, Netzwerk- und Sicherheitsdienste. **Verarbeitungsorte und Garantien:** Je nach Konfiguration Europäische Union und USA; Vercel DPA, Standardvertragsklauseln Modul 3 und gegebenenfalls anwendbarer Angemessenheitsbeschluss. Das Vercel DPA gilt nach dessen aktueller Fassung für Pro- und Enterprise-Pläne.

2. Supabase Pte. Ltd

Anschrift: 65 Chulia Street, #38-02/03, OCBC Centre, Singapore 049513. **Aufgabe:** Authentifizierung, PostgreSQL-Datenbank, private Dateispeicherung und zugehörige Sicherheits- und Betriebsleistungen. **Verarbeitungsorte und Garantien:** Primäre Projektregion Europäische Union; Support- und Konzernzugriffe können Drittländer betreffen. Supabase DPA, Standardvertragsklauseln Modul 3 und zusätzliche dokumentierte Schutzmaßnahmen.

3. OpenRouter, Inc.

Anschrift: 169 Madison Avenue, New York, NY 10016, USA. **Aufgabe:** Technische Weiterleitung von Audio, Transkripten und Prompts an freigegebene Modellanbieter sowie Rückübermittlung der Ergebnisse. **Verarbeitungsorte und Garantien:** USA und Verarbeitungsorte der nachfolgend genannten Modellanbieter; OpenRouter Data Processing Agreement für Enterprise/API-Nutzung, Standardvertragsklauseln Modul 3, deaktivierte Inhaltsprotokollierung und Zero-Data-Retention-Anforderung.

4. Groq UK Limited und verbundene Groq-Infrastruktur

Anschrift: 3 Hammersmith Grove, London W6 0ND, Vereinigtes Königreich. **Aufgabe:** Sprachtranskription des Modells Whisper Large V3 Turbo als nachgelagerter Unterauftragsverarbeiter von OpenRouter. **Verarbeitungsorte und Garantien:** Vereinigtes Königreich und gegebenenfalls USA; Angemessenheitsbeschluss für das Vereinigte Königreich, für weitere Übermittlungen Standardvertragsklauseln und Zero-Data-Retention-Endpunkt.

5. OpenAI Ireland Ltd.

Anschrift: 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland. **Aufgabe:** KI-Inferenz für strukturierte Änderungsvorschläge als nachgelagerter Unterauftragsverarbeiter von OpenRouter. **Verarbeitungsorte und Garantien:** Europäische Union und je nach bereitgestelltem Endpunkt weitere in der OpenAI-Unterauftragsverarbeiterliste bezeichnete Orte; OpenAI DPA und Standardvertragsklauseln für erforderliche Drittlandübermittlungen.

6. Microsoft Ireland Operations Limited

Anschrift: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland. **Aufgabe:** Azure-basierte alternative Bereitstellung des freigegebenen OpenAI-Modells als nachgelagerter Unterauftragsverarbeiter von OpenRouter. **Verarbeitungsorte und Garantien:** Europäische Union und gegebenenfalls weitere dokumentierte Azure-Regionen; Microsoft-Datenschutzbedingungen und Standardvertragsklauseln für erforderliche Drittlandübermittlungen.

Die Modellrouting-Konfiguration ist auf die hier bezeichneten Anbieter und auf Endpunkte ohne Training beziehungsweise mit den vereinbarten Datenschutzfiltern zu begrenzen. Eine Erweiterung auf andere Modell- oder Infrastrukturprovider gilt als Änderung der Unterauftragsverarbeiterliste nach Abschnitt 12.

Dokumentationsgrundlagen

Die Vertragsfassung wurde anhand folgender amtlicher oder anbieterseitiger Primärquellen erstellt und am 17. August 2026 gegen den bezeichneten Stand geprüft:

- Artikel 28 und 32 DSGVO: <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=de>
- EU-Standardvertragsklauseln Verantwortlicher/Auftragsverarbeiter, Durchführungsbeschluss (EU) 2021/915: https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj
- EU-Standardvertragsklauseln für Drittlandübermittlungen, Durchführungsbeschluss (EU) 2021/914: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
- EDSA-Stellungnahme 22/2024 zur Auftragsverarbeiterkette: https://www.edpb.europa.eu/documents/opinion-of-the-board-art-64/opinion-222024-on-certain-obligations-following-from-the_en
- Berliner Checkliste zur Prüfung von AV-Verträgen: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/dokumente/2022-BlnBDI_Checkliste-Pruefung-AVV_v1.0.pdf
- Vercel DPA und Unterauftragsverarbeiter: <https://vercel.com/legal/dpa> und <https://security.vercel.com>
- Supabase DPA: <https://supabase.com/downloads/docs/Supabase%2BDPA%2B260601.pdf>
- OpenRouter Datenschutz, DPA-Hinweis und Routing: <https://openrouter.ai/privacy/> und <https://openrouter.ai/docs/guides/routing/provider-selection>
- OpenAI DPA und Unterauftragsverarbeiter: <https://openai.com/policies/data-processing-addendum/> und <https://openai.com/policies/sub-processor-list/>

Die Dokumentationsgrundlagen erläutern die Entstehung der Fassung; sie erweitern nicht den vereinbarten Leistungsumfang. Änderungen der tatsächlichen Anbieter, Regionen oder Schutzmaßnahmen erfordern eine erneute Prüfung und gegebenenfalls eine neue Vertragsversion oder Unterauftragsverarbeiterinformation.