Auftragsverarbeitungsvereinbarung (AVV)

Stand: Januar 2026

Vorbemerkung

Diese Vereinbarung zur Auftragsverarbeitung („AVV") ergänzt die Allgemeinen Geschäftsbedingungen („AGB") zwischen der RelationFlow Ltd. („Anbieter") und dem Kunden. Diese AVV tritt automatisch mit Abschluss des Vertrages in Kraft.

Im Rahmen der Nutzung der Plattform Corporate LLM verarbeitet der Anbieter personenbezogene Daten im Auftrag des Kunden. Der Kunde ist dabei Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, der Anbieter handelt als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO.

Diese AVV regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten.

1. Begriffsbestimmungen

1.1 „Kundendaten" sind alle personenbezogenen Daten, die der Kunde oder seine autorisierten Nutzer im Rahmen der Nutzung der Plattform hochladen oder eingeben und die der Anbieter im Auftrag des Kunden verarbeitet.

1.2 „Verantwortlicher" ist die natürliche oder juristische Person, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 7 DSGVO).

1.3 „Auftragsverarbeiter" ist die natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSGVO).

1.4 „Datenschutzgesetze" bezeichnet alle anwendbaren Datenschutzvorschriften, insbesondere die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) und das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG).

1.5 „Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).

1.6 „Verarbeitung" ist jeder Vorgang im Zusammenhang mit personenbezogenen Daten, wie das Erheben, Speichern, Verwenden, Übermitteln oder Löschen (Art. 4 Nr. 2 DSGVO).

1.7 „Sicherheitsvorfall" ist jede Verletzung der Sicherheit, die zur Zerstörung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von Kundendaten führt.

1.8 „Unterauftragsverarbeiter" ist jeder Auftragsverarbeiter, den der Anbieter zur Unterstützung bei der Erbringung der Dienstleistungen beauftragt.

1.9 „Plattform" bezeichnet die Software-as-a-Service-Lösung Corporate LLM.

1.10 „Dienstleistungen" hat die in den AGB festgelegte Bedeutung.

2. Geltungsbereich

2.1 Diese AVV regelt die Rechte und Pflichten der Parteien in Bezug auf die Verarbeitung von Kundendaten durch den Anbieter im Rahmen der Dienstleistungen.

2.2 Der Kunde beauftragt den Anbieter als Auftragsverarbeiter mit der Verarbeitung von Kundendaten. Der Kunde ist Verantwortlicher, der Anbieter handelt ausschließlich im Auftrag und nach Weisung des Kunden.

2.3 Diese AVV gilt für alle Kundendaten, auf die der Anbieter im Rahmen der Dienstleistungen Zugriff hat. Dies umfasst:

- Daten, die der Kunde oder seine Nutzer auf der Plattform eingeben oder hochladen
- Daten, die bei der Nutzung der Plattform generiert werden
- Daten, die dem Anbieter auf andere Weise im Rahmen der Dienstleistungen zugänglich werden

2.4 Die Einzelheiten der Verarbeitung (Kategorien betroffener Personen, Arten der Daten, Zwecke) sind in Anlage 1 spezifiziert.

3. Verarbeitung im Auftrag

3.1 Der Anbieter ergreift angemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung von Kundendaten den Anforderungen der Datenschutzgesetze entspricht und die Rechte der betroffenen Personen gewahrt werden.

3.2 Die Verarbeitung von Kundendaten erfolgt grundsätzlich innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR). Übermittlungen in Drittländer finden nur statt, wenn eine geeignete Rechtsgrundlage vorliegt (z.B. Angemessenheitsbeschluss, Standardvertragsklauseln).

3.3 Der Kunde ist für die Rechtmäßigkeit der Verarbeitung der Kundendaten sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich. Der Kunde stellt den Anbieter von Ansprüchen Dritter frei, die aufgrund einer rechtswidrigen Verarbeitung von Kundendaten gegen den Anbieter geltend gemacht werden.

4. Weisungen des Kunden

4.1 Der Anbieter verarbeitet Kundendaten ausschließlich auf Grundlage dokumentierter Weisungen des Kunden. Die Nutzung der Plattform gemäß den AGB gilt als Weisung.

4.2 Ist der Anbieter gesetzlich verpflichtet, Kundendaten ohne Weisung des Kunden zu verarbeiten, informiert er den Kunden vorab über diese Verpflichtung, sofern dies nicht gesetzlich untersagt ist.

4.3 Der Kunde erteilt Weisungen schriftlich, per E-Mail oder über die Funktionen der Plattform. Weisungen, die über den in dieser AVV und den AGB festgelegten Umfang hinausgehen, bedürfen einer gesonderten Vereinbarung.

4.4 Der Anbieter darf Kundendaten nicht für eigene Zwecke verwenden. Ausgenommen sind:

- Sicherungskopien zur Sicherstellung der ordnungsgemäßen Verarbeitung
- Daten zur Erfüllung gesetzlicher Aufbewahrungspflichten
- Anonymisierte oder aggregierte Daten für interne Analysezwecke

5. Unterauftragnehmer

5.1 Der Anbieter setzt Unterauftragsverarbeiter nur mit Zustimmung des Kunden ein. Der Kunde erteilt hiermit seine allgemeine Zustimmung zur Beauftragung von Unterauftragsverarbeitern.

5.2 Der Kunde stimmt der Beauftragung der in Anlage 2 aufgeführten Unterauftragsverarbeiter mit Wirkung ab Inkrafttreten dieser AVV zu.

5.3 Der Anbieter informiert den Kunden über jede beabsichtigte Änderung der Unterauftragsverarbeiter (Hinzufügung oder Austausch). Der Kunde kann aus begründetem Anlass innerhalb von 14 Tagen nach Benachrichtigung schriftlich Widerspruch einlegen. Die Parteien werden in diesem Fall eine einvernehmliche Lösung anstreben.

5.4 Der Anbieter verpflichtet Unterauftragsverarbeiter vertraglich zu denselben Datenschutzpflichten, die in dieser AVV festgelegt sind. Der Anbieter stellt sicher, dass Unterauftragsverarbeiter angemessene technische und organisatorische Maßnahmen zur Einhaltung der Datenschutzgesetze ergreifen.

5.5 Soweit Unterauftragsverarbeiter in Drittländern ansässig sind, stellt der Anbieter sicher, dass eine geeignete Rechtsgrundlage für die Übermittlung vorliegt (z.B. Angemessenheitsbeschluss, Standardvertragsklauseln).

5.6 Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Anbieter dem Kunden gegenüber für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

6. Prüfrechte

6.1 Der Anbieter stellt dem Kunden auf schriftliche Anfrage alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus dieser AVV nachzuweisen.

6.2 Der Kunde oder ein von ihm beauftragter Prüfer kann die Einhaltung dieser AVV überprüfen. Prüfungen sind auf einmal pro Kalenderjahr beschränkt und müssen mindestens 30 Tage vorher schriftlich angekündigt werden. Die Prüfungen erfolgen während der üblichen Geschäftszeiten und dürfen den Betrieb des Anbieters nicht unangemessen beeinträchtigen.

6.3 Der Anbieter kann zum Nachweis der Einhaltung aktuelle Prüfzeugnisse, Berichte oder Zertifizierungen von unabhängigen Stellen vorlegen. In diesem Fall ist der Kunde nicht berechtigt, zusätzliche Prüfungen durchzuführen.

6.4 Der Kunde trägt die Kosten für die Durchführung von Prüfungen, es sei denn, die Prüfung ergibt wesentliche Verstöße des Anbieters gegen diese AVV.

7. Vertraulichkeit

Der Anbieter gewährleistet, dass alle Personen, die zur Verarbeitung von Kundendaten berechtigt sind, zur Vertraulichkeit verpflichtet wurden — entweder durch vertragliche Vereinbarung oder aufgrund gesetzlicher Verschwiegenheitspflichten.

8. Sicherheitsmaßnahmen

8.1 Der Anbieter ergreift unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Zwecke der Verarbeitung angemessene technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

8.2 Die vom Anbieter getroffenen Maßnahmen sind in Anlage 3 beschrieben. Der Kunde bestätigt, dass diese Maßnahmen ein angemessenes Schutzniveau für die Verarbeitung von Kundendaten gewährleisten.

8.3 Der Anbieter ist berechtigt, die technischen und organisatorischen Maßnahmen jederzeit durch gleichwertige oder bessere Maßnahmen zu ersetzen.

9. Meldepflichten

9.1 Der Anbieter informiert den Kunden unverzüglich, wenn ihm ein Sicherheitsvorfall bekannt wird, der Kundendaten betrifft.

9.2 Die Information umfasst, soweit bekannt:

- Art des Vorfalls
- Betroffene Kategorien und ungefähre Anzahl der betroffenen Personen
- Betroffene Kategorien und ungefähre Anzahl der betroffenen Datensätze
- Wahrscheinliche Folgen des Vorfalls
- Ergriffene oder vorgeschlagene Maßnahmen zur Behebung

9.3 Der Kunde trägt die angemessenen Kosten für die Bereitstellung dieser Informationen, es sei denn, der Sicherheitsvorfall ist auf grobe Fahrlässigkeit oder Vorsatz des Anbieters zurückzuführen.

10. Unterstützungspflichten

10.1 Der Anbieter unterstützt den Kunden mit angemessenen technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflichten nach den Datenschutzgesetzen, insbesondere bei:

- Beantwortung von Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, etc.)
- Meldung von Datenschutzverletzungen an Aufsichtsbehörden
- Durchführung von Datenschutz-Folgenabschätzungen

10.2 Der Anbieter informiert den Kunden unverzüglich, wenn er der Auffassung ist, dass eine Weisung des Kunden gegen Datenschutzgesetze verstößt.

10.3 Der Kunde trägt die angemessenen Kosten für die in diesem Abschnitt beschriebenen Unterstützungsleistungen, sofern diese über die gesetzlichen Pflichten des Anbieters hinausgehen.

11. Laufzeit und Beendigung

11.1 Diese AVV tritt mit Abschluss des Vertrages in Kraft und gilt für die Dauer des Vertragsverhältnisses.

11.2 Mit Beendigung des Vertrages endet auch diese AVV. Bestimmungen, die für den ordnungsgemäßen Abschluss der Verarbeitung erforderlich sind (insbesondere zur Löschung und Rückgabe von Daten), bleiben über die Beendigung hinaus in Kraft.

12. Datenlöschung und Rückgabe

12.1 Nach Beendigung des Vertrages löscht der Anbieter alle Kundendaten oder gibt sie an den Kunden zurück — nach Wahl des Kunden.

12.2 Der Kunde teilt dem Anbieter innerhalb von 30 Tagen nach Vertragsende mit, ob die Daten zurückgegeben oder gelöscht werden sollen. Die Rückgabe erfolgt in einem gängigen, maschinenlesbaren Format (JSON).

12.3 Erfolgt innerhalb dieser Frist keine Mitteilung, ist der Anbieter berechtigt, die Kundendaten zu löschen.

12.4 Gesetzliche Aufbewahrungspflichten bleiben von den vorstehenden Regelungen unberührt.

12.5 Der Anbieter bestätigt die Löschung oder Rückgabe auf Anfrage des Kunden.

13. Datenschutzbeauftragter

Der Anbieter bestellt einen Datenschutzbeauftragten, soweit dies gesetzlich erforderlich ist. Die Kontaktdaten werden dem Kunden auf Anfrage mitgeteilt.

Alternativ kann der Kunde datenschutzrechtliche Anfragen an support@corporatellm.de richten.

14. Vergütung

14.1 Alle vom Anbieter im Rahmen dieser AVV erbrachten Leistungen sind durch die im Vertrag vereinbarte Vergütung abgegolten, sofern in dieser AVV nicht ausdrücklich etwas anderes bestimmt ist.

14.2 Soweit Leistungen in dieser AVV als vergütungspflichtig bezeichnet sind (z.B. Unterstützung bei Audits, Informationen bei Sicherheitsvorfällen), werden diese nach Aufwand zu den im Vertrag vereinbarten Sätzen vergütet. Sind keine Sätze vereinbart, gelten die zum Zeitpunkt der Leistung gültigen Standardsätze des Anbieters.

15. Haftung

15.1 Für die Haftung des Anbieters gelten die Haftungsregelungen der AGB entsprechend.

15.2 Behördliche Bußgelder, die gegen den Kunden verhängt werden, können gegenüber dem Anbieter nur geltend gemacht werden, soweit sie auf einem Verstoß des Anbieters gegen diese AVV oder Datenschutzgesetze beruhen. Die Haftung ist auf den Anteil begrenzt, der dem Verschulden des Anbieters entspricht.

16. Schlussbestimmungen

16.1 Diese AVV ist Bestandteil des Vertrages. Bei Widersprüchen zwischen den AGB und dieser AVV haben die Bestimmungen dieser AVV Vorrang, soweit sie die Verarbeitung von Kundendaten betreffen.

16.2 Der Anbieter ist berechtigt, diese AVV zu ändern, um Änderungen der Datenschutzgesetze oder behördlicher Anforderungen zu berücksichtigen. Der Anbieter informiert den Kunden mindestens 30 Tage vorab schriftlich oder per E-Mail über solche Änderungen.

16.3 Sollte eine Bestimmung dieser AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine Regelung, die dem wirtschaftlich Gewollten am nächsten kommt.

16.4 Im Übrigen gelten die Schlussbestimmungen der AGB entsprechend.

Anlage 1: Verarbeitungsdetails

1. Kategorien betroffener Personen

- Nutzer der Plattform (Single-User)
- Mitarbeiter des Kunden (bei Enterprise)
- Personen, auf die sich vom Nutzer eingegebene Daten beziehen

2. Arten von Kundendaten

- Namen und E-Mail-Adressen der Nutzer
- Chat-Verläufe und Prompts (Eingaben der Nutzer)
- Hochgeladene Dateien und Dokumente
- Generierte Antworten und Outputs
- Nutzungsstatistiken

3. Besondere Kategorien personenbezogener Daten

Im bestimmungsgemäßen Nutzungsfall sollten besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO (z.B. Gesundheitsdaten, religiöse Überzeugungen, politische Meinungen) nicht vom Kunden eingegeben werden.

4. Art der Verarbeitung

- Speicherung und Hosting von Kundendaten
- Übermittlung von Prompts an KI-Anbieter
- Generierung und Speicherung von KI-Antworten
- Erstellung von Nutzungsstatistiken

5. Zweck der Verarbeitung

Bereitstellung der Plattform Corporate LLM und der damit verbundenen Dienstleistungen gemäß den Weisungen des Kunden.

Anlage 2: Unterauftragnehmer

Der Anbieter setzt folgende Unterauftragsverarbeiter ein:

Hosting & Infrastruktur

Vercel Inc.

440 N Barranca Ave #4133, Covina, CA 91723, USA

Aufgabe: Website- und App-Hosting, Analytics/Page Speed Insights

Ort der Verarbeitung: USA/EU

Garantie: EU-US Data Privacy Framework, Standardvertragsklauseln (SCC)

Supabase Inc.

970 Toa Payoh North #07-04, Singapore 318992

Aufgabe: Datenbank, Authentifizierung

Ort der Verarbeitung: EU (Frankfurt)

Garantie: Standardvertragsklauseln (SCC)

Upstash Inc.

1000 N West Street, Suite 1200, Wilmington, DE 19801, USA

Aufgabe: Caching, Rate Limits

Ort der Verarbeitung: EU

Garantie: Standardvertragsklauseln (SCC)

KI-Dienste

Microsoft Corporation (Azure)

One Microsoft Way, Redmond, WA 98052, USA

Aufgabe: Hosting von OpenAI-Modellen

Ort der Verarbeitung: EU

Garantie: EU-US Data Privacy Framework, Standardvertragsklauseln (SCC)

Amazon Web Services EMEA SARL

38 avenue John F. Kennedy, L-1855 Luxemburg

Aufgabe: Hosting von Anthropic-Modellen (Amazon Bedrock)

Ort der Verarbeitung: EU

Garantie: EU-US Data Privacy Framework, Standardvertragsklauseln (SCC)

Google Ireland Limited

Gordon House, Barrow Street, Dublin 4, Irland

Aufgabe: Hosting von Google- und Anthropic-Modellen

Ort der Verarbeitung: EU

Garantie: EU-US Data Privacy Framework, Standardvertragsklauseln (SCC)

Zahlung

Stripe Payments Europe Ltd.

1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland

Aufgabe: Zahlungsabwicklung

Ort der Verarbeitung: EU

E-Mail & Kommunikation

Resend Inc.

2261 Market Street #4059, San Francisco, CA 94114, USA

Aufgabe: Versand transaktionaler E-Mails

Ort der Verarbeitung: USA

Garantie: Standardvertragsklauseln (SCC)

Analyse & Monitoring

Functional Software Inc. (Sentry)

45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA

Aufgabe: Fehlerüberwachung

Ort der Verarbeitung: USA

Garantie: EU-US Data Privacy Framework, Standardvertragsklauseln (SCC)

PostHog Inc.

2261 Market Street #4008, San Francisco, CA 94114, USA

Aufgabe: Produktanalyse

Ort der Verarbeitung: EU

Garantie: Standardvertragsklauseln (SCC)

Anlage 3: Sicherheitsmaßnahmen

Der Anbieter hat folgende technische und organisatorische Maßnahmen zum Schutz der Kundendaten implementiert:

1. Vertraulichkeit

1.1 Zutrittskontrolle

Die Infrastruktur des Anbieters wird vollständig über Cloud-Dienste betrieben. Physische Server werden nicht selbst betrieben. Die eingesetzten Cloud-Anbieter (Supabase, Vercel, AWS, Azure, Google Cloud) verfügen über zertifizierte Rechenzentren mit entsprechenden Zutrittskontrollen.

1.2 Zugangskontrolle

Maßnahmen zum Schutz vor unbefugter Systemnutzung:

- Passwortrichtlinie: Mindestens 8 Zeichen, Großbuchstaben, Kleinbuchstaben, Zahl und Sonderzeichen erforderlich
- Automatische Session-Sperrung nach Inaktivität
- Verschlüsselte Übertragung aller Anmeldedaten (TLS/HTTPS)
- Verwaltung von Benutzerberechtigungen über die Plattform

1.3 Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass Berechtigte nur auf die ihnen zugewiesenen Daten zugreifen:

- Rollenbasiertes Berechtigungskonzept (Owner, Admin, User)
- Logische Mandantentrennung in der Datenbank
- Protokollierung von Zugriffen (Logs werden nach 90 Tagen anonymisiert)
- Prinzip der minimalen Rechtevergabe

1.4 Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung von Daten:

- Strikte logische Mandantentrennung innerhalb der Datenbank

- Trennung von Entwicklungs-, Test- und Produktivsystemen
- Differenziertes Berechtigungskonzept

2. Integrität

2.1 Weitergabekontrolle

Maßnahmen zum Schutz bei der Datenübertragung:

- TLS/HTTPS-Verschlüsselung für alle Verbindungen
- Verschlüsselte API-Kommunikation mit KI-Anbietern
- Keine unverschlüsselte Übertragung von Kundendaten

2.2 Eingabekontrolle

Maßnahmen zur Nachvollziehbarkeit von Dateneingaben:

- Protokollierung von Eingaben, Änderungen und Löschungen
- Zuordnung von Aktionen zu Benutzerkonten
- Logs werden nach 90 Tagen anonymisiert

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen zum Schutz gegen Datenverlust:

- Hosting auf professionellen Cloud-Infrastrukturen (Supabase, Vercel, AWS, Azure, Google Cloud)
- Tägliche Backups der Datenbank
- Redundante Systemauslegung durch Cloud-Anbieter
- Verschlüsselung der Datenbank (Supabase)

4. Verfahren zur regelmäßigen Überprüfung

4.1 Datenschutz-Management

- Regelmäßige Überprüfung der Datenschutzmaßnahmen
- Schulung der Mitarbeiter zum Datenschutz
- Prozesse zur Bearbeitung von Betroffenenanfragen implementiert

- Kontakt für Datenschutzanfragen: support@corporatellm.de

4.2 Incident-Response

- Unverzügliche Information des Kunden bei Sicherheitsvorfällen
- Dokumentation von Sicherheitsvorfällen
- Klare Verantwortlichkeiten für die Bearbeitung von Vorfällen