

AVV

Auftragsverarbeitungsvertrag (Art. 28 DSGVO) zur Verarbeitung der Workspace-Inhalte deines Teams.

Stand: 2026-08-01 · Version 2026-08 · Änderungsprotokoll

Präambel

Dieser Auftragsverarbeitungsvertrag (AVV) konkretisiert die Verpflichtungen der Parteien nach Art. 28 Abs. 3 DSGVO im Zusammenhang mit der Verarbeitung personenbezogener Daten durch die **Kracht Media GmbH** (Betreiberin von Gorilia, nachfolgend „Auftragsverarbeiter“) im Auftrag des jeweiligen Team-Accounts (nachfolgend „Verantwortlicher“ oder „Kunde“).

Er gilt für jeden Gorilia-Team-Account, sobald du ihn in den Team-Einstellungen per Klick-Akzeptanz bestätigst — der Zeitpunkt und die akzeptierte Version werden dabei protokolliert. Bis zur Bestätigung gelten die allgemeinen Regelungen der Nutzungsbedingungen zur Auftragsverarbeitung entsprechend.

Relevant wird dieser AVV insbesondere, sobald ein Team-Account Inhalte verarbeitet, die personenbezogene Daten Dritter enthalten können (z. B. Chat-Inhalte mit Kundendaten). Für Verarbeitungen, bei denen Gorilia selbst Verantwortlicher ist (Konto-, Sicherheits- und Abrechnungsdaten), gilt stattdessen die Datenschutzerklärung.

1. Gegenstand, Dauer und Zweck der Verarbeitung

Gegenstand, Dauer, Art und Zweck der Verarbeitung sowie die betroffenen Datenkategorien und Personengruppen ergeben sich aus **Anlage 1** zu diesem AVV.

Die Verarbeitung erfolgt ausschließlich zur Erbringung der Plattformleistung (KI-Chat-Workspace) für die Dauer des zwischen den Parteien bestehenden Nutzungsvertrags.

2. Pflichten des Auftragsverarbeiters (Art. 28 Abs. 3 DSGVO)

a) Verarbeitung nur auf dokumentierte Weisung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen — einschließlich in Bezug auf Übermittlungen an ein Drittland oder eine internationale Organisation —, sofern er nicht durch das Recht der Europäischen Union oder der



Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen Grundes des öffentlichen Interesses verbietet. Die Konfiguration und Bedienung der Plattform durch den Verantwortlichen (z. B. Modellauswahl, Team-Einladungen, Speicherung von Chat-Inhalten) gilt als dokumentierte Weisung im Sinne dieser Bestimmung.

b) Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

c) Sicherheit der Verarbeitung (Art. 32 DSGVO)

Der Auftragsverarbeiter ergreift alle nach Art. 32 DSGVO erforderlichen Maßnahmen. Die konkret umgesetzten technischen und organisatorischen Maßnahmen sind in **Anlage 3** beschrieben.

d) Weitere Auftragsverarbeiter (Unterauftragsverarbeiter)

Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter (Unterauftragsverarbeiter). Die aktuelle Liste der eingesetzten Unterauftragsverarbeiter ist in **Anlage 2** geregelt und öffentlich unter gorilia.ai/subprozessoren einsehbar.

Über beabsichtigte Änderungen (Hinzufügung oder Ersetzung von Unterauftragsverarbeitern) informiert der Auftragsverarbeiter den Kontoinhaber mindestens **30 Tage im Voraus** per E-Mail. Der Verantwortliche kann der Änderung innerhalb dieser Frist aus nachvollziehbaren, datenschutzrechtlichen Gründen widersprechen; im Fall eines berechtigten Widerspruchs, den die Parteien nicht einvernehmlich lösen können, steht dem Verantwortlichen ein außerordentliches Kündigungsrecht für den betroffenen Teil der Leistung zu. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Änderung als akzeptiert.

Ist die kurzfristige Hinzuziehung eines Unterauftragsverarbeiters aus technischen oder betrieblichen Gründen unaufschiebbar (z. B. zur Aufrechterhaltung der Sicherheit oder Verfügbarkeit der Plattform), informiert der Auftragsverarbeiter unverzüglich nachträglich; das Widerspruchsrecht bleibt davon unberührt.

Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments zur Einhaltung von Datenschutzpflichten, die denen dieses AVV entsprechen.

e) Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen, soweit dies möglich ist, bei der Erfüllung von dessen Pflicht Anträge auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen



Person zu beantworten. Der Verantwortliche kann Auskunft und Export der Team-Workspace-Inhalte über die Selbstbedienungsfunktion in den Konto- bzw. Team-Einstellungen selbst vornehmen (siehe [Datenportabilität](#)).

f) Unterstützung bei Sicherheit, Meldepflichten und Datenschutz-Folgenabschätzung

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

Bei Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten (Art. 33 DSGVO), die Daten betrifft, die der Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet, informiert der Auftragsverarbeiter den Verantwortlichen **unverzüglich, spätestens innerhalb von 48 Stunden** nach Bekanntwerden, unter der beim Team-Account hinterlegten E-Mail-Adresse des Kontoinhabers.

g) Löschung oder Rückgabe nach Vertragsende

Nach Beendigung der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Beides steht dem Verantwortlichen jederzeit als Selbstbedienung zur Verfügung: die **Rückgabe** über die Exportfunktion in den Team-Einstellungen, die **Löschung** über die Löschung einzelner Inhalte bzw. des Team-Accounts. Der Auftragsverarbeiter löscht die Daten darüber hinaus auf Weisung des Verantwortlichen. Eine automatische Löschung allein aufgrund des Vertragsendes findet nicht statt — die Daten bleiben abrufbar, solange der Account besteht. Einzelheiten zum Export und zu den Löschwegen enthält das Kapitel „Wechsel und Vertragsende“ der [Datenportabilitätsseite](#).

h) Nachweis- und Kontrollpflichten

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen — einschließlich Vor-Ort-Überprüfungen —, die vom Verantwortlichen oder einem anderen von ihm beauftragten Prüfer durchgeführt werden. Ein Audit ist mit angemessener Vorlaufzeit (mindestens 30 Tage) schriftlich anzukündigen, auf die Dauer eines Arbeitstags pro Kalenderjahr zu beschränken und unterliegt einer Vertraulichkeitsvereinbarung. Der Auftragsverarbeiter kann statt eines eigenen Audits aussagekräftige Nachweise (z. B. Zusammenfassungen einschlägiger Nachweise Dritter) vorlegen, wenn diese die Einhaltung der Pflichten aus diesem AVV hinreichend belegen.

3. Weisungsrecht



Der Verantwortliche hat das Recht, dem Auftragsverarbeiter jederzeit Weisungen zu Art, Umfang und Verfahren der Verarbeitung zu erteilen. Weisungen erfolgen grundsätzlich über die Bedienoberfläche der Plattform oder in Textform (z. B. per E-Mail an admin@kracht.at).

Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies dem Verantwortlichen unverzüglich mit und ist berechtigt, die Ausführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung auszusetzen.

4. Haftung

Für Schäden, die aus einer Verletzung dieses AVV oder der Bestimmungen der DSGVO durch eine der Parteien entstehen, gelten die gesetzlichen Haftungsregelungen sowie ergänzend die Haftungsregelungen der [Nutzungsbedingungen](#).

5. Schlussbestimmungen

Es gilt österreichisches Recht. Sollten einzelne Bestimmungen dieses AVV unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Im Fall von Widersprüchen zwischen diesem AVV und den Nutzungsbedingungen geht dieser AVV im Hinblick auf Fragen der Verarbeitung personenbezogener Daten vor.

Anlage 1 — Verarbeitungsübersicht

Feld	Angabe
Gegenstand der Verarbeitung	Workspace-Inhalte des Team-Accounts: Chat-Threads und -Nachrichten, Projekte und Projekthinhalte, hochgeladene Dateien und daraus abgeleitete Texterkennung (OCR), sowie in den Team-Speicher (Memory) geschriebene KI-Erinnerungen.
Dauer der Verarbeitung	Für die Dauer des Nutzungsvertrags und darüber hinaus, solange der Team-Account besteht; Löschung durch den Verantwortlichen selbst (einzelne Inhalte oder Kontolöschung) bzw. auf dessen Weisung, siehe Datenportabilitätsseite .
Art und Zweck der Verarbeitung	Bereitstellung eines KI-gestützten Chat-Workspace: Speicherung und Anzeige von Chat-Inhalten, Weiterleitung an das vom Nutzer gewählte KI-Sprachmodell zur Answererzeugung, automatische Titel-Generierung, Dokumenten-Texterkennung, persistente KI-Erinnerungen sowie die dafür technisch notwendige Zwischenspeicherung (z. B. Stream-Zwischenpuffer beim Chat-Reconnect).
Kategorien betroffener Personen	Mitglieder des Team-Accounts sowie Dritte, deren personenbezogene Daten Nutzer im Rahmen von Chat-Eingaben, Dateien oder Projekthinhalten eigenverantwortlich verarbeiten.
Kategorien personenbezogener Daten	Freitext-Inhalte (Chat-Prompts und KI-Antworten, Dateiinhalte, Memory-Einträge) beliebiger Kategorie, abhängig davon, was Nutzer eingeben — 

	potenziell auch besondere Kategorien personenbezogener Daten (Art. 9 DSGVO), ohne inhaltliche Prüfung oder Filterung durch den Auftragsverarbeiter.
Empfänger / Unterauftragsverarbeiter	Siehe Anlage 2 und die öffentliche <u>Subprozessorenliste</u> .

Anlage 2 — Unterauftragsverarbeiter

Die jeweils aktuelle Liste der eingesetzten Unterauftragsverarbeiter, einschließlich Rechtsträger, Sitz, Zweck, verarbeiteter Datenkategorien, Ort der Verarbeitung und Transfermechanismus, wird öffentlich und fortlaufend aktuell unter gorilia.ai/subprozessoren geführt. Diese Anlage nimmt auf diese Liste Bezug, anstatt sie statisch zu wiederholen, damit sie jederzeit den tatsächlichen Stand widerspiegelt.

Änderungsmechanismus (siehe auch Pflicht d) oben):

- Allgemeine Genehmigung des Verantwortlichen zur Hinzuziehung weiterer Unterauftragsverarbeiter.
- Vorabinformation per E-Mail an den Kontoinhaber mindestens 30 Tage vor Wirksamwerden einer Änderung.
- Widerspruchsrecht des Verantwortlichen aus nachvollziehbaren datenschutzrechtlichen Gründen innerhalb dieser Frist, mit außerordentlichem Kündigungsrecht bei ungelöstem Widerspruch.
- Ausnahme für unaufschiebbare, sicherheits- oder betriebsnotwendige Hinzuziehungen: unverzügliche nachträgliche Information, Widerspruchsrecht bleibt bestehen.

Anlage 3 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Diese Anlage listet ausschließlich Maßnahmen, die tatsächlich umgesetzt und verifiziert sind — keine geplanten oder unverifizierten Maßnahmen.

A. Vertraulichkeit und Zugriffskontrolle

- **Mandantentrennung auf Datenbankebene (Row-Level Security):** jede Datenbankabfrage wird serverseitig durch Postgres-RLS-Richtlinien auf den jeweils berechtigten Account beschränkt — ein struktureller Schutz gegen Cross-Tenant-Zugriff, nicht nur eine Anwendungsprüfung.
- **Spaltenscharfe Rechtevergabe (Column-Level Grants):** besonders sensible Tabellenspalten sind zusätzlich zur RLS auf Spaltenebene berechtigt, sodass selbst berechtigte Rollen nur genau die Spalten schreiben können, die für ihre Funktion vorgesehen sind.



- **Zwei-Faktor-Authentifizierung (TOTP):** Nutzerkonten können durch einen zeitbasierten Einmalpasswort-Faktor zusätzlich abgesichert werden.
- **Prinzip der geringsten Rechte bei Backend-Diensten:** interne Server-Rollen (Service-Rollen) sind auf die für ihre jeweilige Funktion notwendigen Berechtigungen beschränkt, nicht pauschal privilegiert.

B. Integrität und Übertragungssicherheit

- **Transportverschlüsselung (TLS):** sämtliche Datenübertragung zwischen Client, Plattform und den eingesetzten Unterauftragsverarbeitern erfolgt verschlüsselt.

C. Verschlüsselung

- **Verschlüsselung im Ruhezustand:** Daten werden bei der eingesetzten Datenbank- und Storage-Infrastruktur (Supabase) verschlüsselt gespeichert.

D. Vertraulichkeit gegenüber KI-Modellanbietern

- **Kein Training auf Kundeneinhalten:** die eingesetzten KI-Modellanbieter werden vertraglich bzw. über deren API-Bedingungen so eingebunden, dass Chat-Inhalte nicht zum Training ihrer Modelle verwendet werden — Details und Ausnahmen je Anbieter siehe [Subprozessorenliste](#).
- **Private Speicherung, signierte Zugriffs-URLs:** hochgeladene Dateien liegen in einem nicht öffentlich zugänglichen Speicherbereich; der Zugriff erfolgt ausschließlich über zeitlich begrenzte, signierte URLs.

E. Verfahren zur regelmäßigen Überprüfung

- **Fehler- und Sicherheitsmonitoring ohne Klardaten-Übertragung:** technisches Monitoring (Fehlerüberwachung) ist so konfiguriert, dass keine vollständigen Chat-Inhalte oder unnötige personenbezogene Daten in Fehlerberichte gelangen (Datenbereinigung vor Übermittlung).

Der Auftragsverarbeiter kann diese Maßnahmen im Zeitverlauf aktualisieren oder anpassen, sofern das dadurch erreichte Schutzniveau insgesamt nicht gemindert wird.

