

Vereinbarung zur Auftragsverarbeitung

Aktuelle Vertragsfassung ohne archivierten Annahmenachweis

Vertragsparteien

Kunde (Verantwortlicher)	Wird bei der Annahme in der Plattform eingetragen.
Anbieter (Auftragsverarbeiter)	DATENMASSIV GmbH, Zeitblomstraße 31/2, 89073 Ulm
Vertreten durch die Geschäftsführer	Tom Bichay, Toni Thomä, Martin Schubert
Registergericht	Amtsgericht Ulm, HRB 729394

Fassung

Vertragsfassung	2026-10-v4
Prüfsumme des Vertragstextes (SHA-256)	cc4a73e18fc8910d38a53f3e764a84f250b3be9fa7b0c5529289b38f4d62ea23

Fassung 2026-10-v4 vom 20. Oktober 2026

1. Gegenstand und Dauer

1. Die DATENMASSIV GmbH, Zeitblomstraße 31/2, 89073 Ulm (nachfolgend „Anbieter“), verarbeitet bei der Bereitstellung der Plattform Datenmassiv AI personenbezogene Daten im Auftrag des Kunden (nachfolgend „Kunde“). Dieser Vertrag regelt die Rechte und Pflichten der Parteien nach Art. 28 DSGVO für alle Funktionen der Plattform. Er ergänzt die Allgemeinen Geschäftsbedingungen des Anbieters (nachfolgend „Hauptvertrag“).
2. Der Vertrag gilt für die Laufzeit des Hauptvertrags und darüber hinaus, solange der Anbieter Kundendaten verarbeitet, insbesondere bis zum Abschluss der Löschung nach Ziffer 12. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

2. Art, Zweck und Umfang der Verarbeitung

Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1. Der Anbieter verarbeitet Kundendaten ausschließlich zur Erbringung der vereinbarten Leistungen. Er verwendet sie nicht zum Training von KI-Modellen und nicht für eigene Zwecke. Die eingesetzten KI-Modellanbieter verwenden Eingaben nach ihren Bedingungen für die Nutzung ihrer Schnittstellen nicht zum Training ihrer Modelle.

3. Weisungen

1. Der Anbieter verarbeitet Kundendaten nur auf dokumentierte Weisung des Kunden, auch in Bezug auf Übermittlungen in Drittländer, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats dazu verpflichtet. In diesem Fall teilt er dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).
2. Die Weisungen sind in diesem Vertrag festgelegt. Einstellungen, die der Kunde oder seine Nutzer in der Plattform vornehmen, etwa die Wahl der KI-Modelle, die Aufbewahrungsfrist, die Websuche oder das Anbinden von Microsoft 365, gelten als dokumentierte Weisungen. Darüber hinausgehende Einzelweisungen, etwa die Freischaltung von Modellen außerhalb der EU, bedürfen der Textform.
3. Hält der Anbieter eine Weisung für rechtswidrig, informiert er den Kunden unverzüglich. Er darf die Ausführung aussetzen, bis der Kunde sie bestätigt oder ändert.

4. Pflichten des Kunden

Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und seiner Weisungen verantwortlich, insbesondere für eine Rechtsgrundlage, die Information der betroffenen Personen und, beim Embed-Chatbot, für den Datenschutzhinweis auf seiner Website. Er gibt besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO nur ein, soweit dies zulässig ist und er die Risiken bewertet hat. Er informiert den Anbieter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

5. Vertraulichkeit

Der Anbieter gewährleistet, dass sich alle zur Verarbeitung der Kundendaten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Zugriff auf Kundendaten erhalten sie nur, soweit es für die Leistungserbringung, den Support oder die Behebung von Störungen erforderlich ist. Die Pflicht gilt über das Vertragsende hinaus.

6. Sicherheit der Verarbeitung

Der Anbieter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 3 lit. c DSGVO). Die bei Vertragsschluss geltenden Maßnahmen stehen in Anlage 3. Der Anbieter darf sie an den Stand der Technik anpassen, solange das dort festgelegte Schutzniveau nicht unterschritten wird.

7. Unterauftragsverarbeiter

1. Der Kunde erteilt die allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter stehen in Anlage 2.
2. Der Anbieter informiert den Inhaber der Organisation mindestens vier Wochen vor dem Hinzuziehen oder Ersetzen eines Unterauftragsverarbeiters in Textform. Der Kunde kann innerhalb von 14 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Einigen sich die Parteien nicht, kann jede Partei den Hauptvertrag zum Zeitpunkt des geplanten Einsatzes kündigen.
3. Der Anbieter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO), und haftet dem Kunden gegenüber für deren Einhaltung.

8. Übermittlung in Drittländer

Kundendaten werden grundsätzlich in der Europäischen Union oder dem Europäischen Wirtschaftsraum verarbeitet. Eine Verarbeitung in einem Drittland erfolgt nur, soweit Anlage 2 sie ausweist oder der Kunde sie anweist, etwa durch die Freischaltung von KI-Modellen außerhalb der EU. Übermittlungen in Drittländer erfolgen nur nach Art. 44 ff. DSGVO, insbesondere auf Grundlage eines Angemessenheitsbeschlusses einschließlich des EU-US Data Privacy Framework oder von EU-Standardvertragsklauseln. Modelle außerhalb der EU sind ausgeschaltet. Der Anbieter schaltet sie nur auf Weisung des Kunden frei.

9. Rechte betroffener Personen

Der Anbieter unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen nach Kapitel III DSGVO (Art. 28 Abs. 3 lit. e DSGVO). Dazu stellt er in der Plattform Funktionen zum Export, zur Berichtigung und zur Löschung bereit. Wendet sich eine betroffene Person unmittelbar an den Anbieter, leitet er das Anliegen unverzüglich an den Kunden weiter und beantwortet es nicht selbst, sofern der Kunde ihn nicht anweist.

10. Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Anbieter meldet dem Kunden eine Verletzung des Schutzes von Kundendaten unverzüglich, spätestens innerhalb von 48 Stunden, nachdem sie ihm bekannt geworden ist (Art. 33 Abs. 2 DSGVO). Die Meldung beruht auf den ihm vorliegenden Informationen; weitere Informationen reicht er nach, sobald sie vorliegen.

11. Unterstützung bei den Pflichten nach Art. 32 bis 36 DSGVO

Der Anbieter unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm vorliegenden Informationen bei der Sicherheit der Verarbeitung, bei Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen, bei Datenschutz-Folgenabschätzungen und bei vorherigen Konsultationen der Aufsichtsbehörde (Art. 28 Abs. 3 lit. f DSGVO).

12. Löschung und Rückgabe nach Vertragsende

1. Endet ein Abonnement, bleiben die Kundendaten erhalten, bis der Kunde sie selbst löscht oder in Textform die Löschung seiner Organisation verlangt (Ziffer 14 des Hauptvertrags). Bis dahin kann der Kunde sie über den Organisationsexport und die Funktionen der Plattform abrufen; das ist die Rückgabe im Sinne von Art. 28 Abs. 3 lit. g DSGVO.
2. Verlangt der Kunde die Löschung seiner Organisation, löscht der Anbieter die Kundendaten einschließlich gespeicherter Dateien innerhalb von 30 Tagen, soweit keine Pflicht zur Speicherung nach Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Auf Anfrage bestätigt er die Löschung in Textform.
3. Während der Laufzeit löscht die Plattform Chat-Verläufe und Agenten-Aufträge nach der vom Kunden eingestellten Aufbewahrungsfrist automatisch.
4. Unterlagen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen, darf der Anbieter entsprechend den gesetzlichen Aufbewahrungsfristen auch nach Vertragsende aufbewahren.

13. Nachweise und Kontrollen

Der Anbieter stellt dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Kunden oder einen von ihm beauftragten Prüfer, der zur Verschwiegenheit verpflichtet ist und kein Wettbewerber des Anbieters ist (Art. 28 Abs. 3 lit. h DSGVO). Inspektionen sind mit angemessener Frist, in der Regel zwei Wochen, anzukündigen und finden zu den üblichen Geschäftszeiten statt, ohne den Betrieb unverhältnismäßig zu stören. Die Kosten einer Inspektion trägt der Kunde, es sei denn, sie stellt einen Verstoß des Anbieters gegen diesen Vertrag fest. Der Anbieter darf den Zugang zu Informationen beschränken, soweit Daten anderer Kunden oder Sicherheitsbelange betroffen sind.

14. Haftung

Für die Haftung der Parteien untereinander gilt Ziffer 13 des Hauptvertrags. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

15. Schlussbestimmungen

1. Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag in allen Fragen des Datenschutzes vor. Im Übrigen gelten die Bestimmungen des Hauptvertrags, insbesondere zu anwendbarem Recht und Gerichtsstand.
2. Eine neue Fassung dieses Vertrags wird wirksam, wenn der Kunde sie in der Plattform annimmt. Bis dahin gilt die zuletzt angenommene Fassung.
3. Sollte eine Bestimmung unwirksam sein, bleiben die übrigen Bestimmungen wirksam.

Anlage 1: Art und Zweck der Verarbeitung, Datenarten, betroffene Personen

Gegenstand der Verarbeitung ist die Bereitstellung der Plattform mit den folgenden Funktionen. Daten werden jeweils nur verarbeitet, soweit der Kunde die Funktion nutzt.

Funktion	Art und Zweck
AI Chat	Beantwortung von Eingaben der Nutzer durch KI-Sprachmodelle, Speicherung der Chat-Verläufe, optionale Websuche.
Wissensdatenbanken	Speicherung, Texterkennung, Zerlegung und Indexierung (Embeddings) hochgeladener oder importierter Dokumente sowie Suche darin.

Dokument-Chat	Fragen und Antworten zu einzelnen hochgeladenen Dokumenten.
Agenten und Orchestrator	Ausführung von Aufgaben durch KI-Agenten mit Werkzeugen (Suche in Wissensdatenbanken, Websuche, Datenanalyse in einer isolierten Umgebung, Erstellung von Dateien), Speicherung von Aufträgen, Zwischenschritten und Ergebnissen.
Workflows	Automatisierte, vom Kunden konfigurierte Abläufe mit KI-Schritten, Freigaben und Benachrichtigungen.
Transkription	Umwandlung von Audioaufnahmen in Text einschließlich Sprechertrennung sowie KI-gestützte Zusammenfassung.
Embed-Chatbots	Beantwortung von Fragen der Website-Besucher des Kunden auf dessen Website, optional Erfassung von Kontaktanfragen und Abfrage freier Termine eines Kalenders.
Microsoft-365-Anbindung	Abruf von Dateien und Inhalten aus dem Microsoft-365-Mandanten des Kunden im Rahmen der Berechtigungen des jeweiligen Nutzers, um Fragen dazu zu beantworten.
Verwaltung	Anmeldung, Verwaltung von Mitgliedern, Rollen und Einstellungen, Versand von System-E-Mails, Protokollierung sicherheitsrelevanter Vorgänge, Fehlerüberwachung.

Arten personenbezogener Daten

- Nutzerstammdaten: Name, E-Mail-Adresse, Rolle, Organisationszugehörigkeit
- Inhaltsdaten: Eingaben, hochgeladene und importierte Dokumente, KI-Antworten, erzeugte Dateien und Ergebnisse von Agenten und Workflows
- Audioaufnahmen, Transkripte und Zusammenfassungen von Gesprächen
- Konfigurationsdaten: Vorlagen, Agenten-, Workflow- und Chatbot-Einstellungen, soweit sie personenbezogene Daten enthalten
- Integrationsdaten: Dateien und Inhalte aus Microsoft 365 sowie Termine eines angebundenen Kalenders
- Daten von Website-Besuchern: Chat-Nachrichten, pseudonyme Sitzungskennung, Zeitstempel, Sprache und freiwillig angegebene Kontaktdaten
- Nutzungs- und Protokolldaten: Zeitstempel, Verbrauch, IP-Adresse in Sicherheitsprotokollen, technische Fehlerkontexte

Kategorien betroffener Personen

- Beschäftigte und sonstige Nutzer des Kunden, die Zugang zur Plattform erhalten
- Kontakte und sonstige Dritte, deren Daten der Kunde über Eingaben, Dokumente, Workflows oder Integrationen einbringt, etwa Kunden, Interessenten, Lieferanten, Geschäftspartner und Bewerber
- Teilnehmende an transkribierten Gesprächen
- Website-Besucher des Kunden, die einen Embed-Chatbot nutzen

Anlage 2: Unterauftragsverarbeiter

Stets eingesetzt:

Unternehmen, Sitz	Zweck	Ort der Verarbeitung
Supabase, Inc., USA	Datenbank, Anmeldung und Dateispeicher	EU (Frankfurt)
Vercel Inc., USA	Betrieb der Anwendung	EU (Frankfurt)
Upstash, Inc., USA	Ablaufsteuerung länger laufender Vorgänge	EU (Frankfurt)

Functional Software, Inc. (Sentry), USA	Fehlerüberwachung	EU (Deutschland)
Microsoft Ireland Operations Limited, Irland	KI-Modelle und Transkription (Azure)	EU
Amazon Web Services EMEA SARL, Luxemburg	KI-Modelle (Amazon Bedrock), Versand von System-E-Mails (Amazon SES)	EU
Google Cloud EMEA Limited, Irland	KI-Modelle (Vertex AI)	EU

Nur eingesetzt, wenn der Kunde die jeweilige Funktion nutzt oder freischaltet:

Unternehmen, Sitz	Zweck	Ort der Verarbeitung
Daytona Platforms, Inc., USA	Datenanalyse durch Agenten in isolierten Umgebungen	EU (Frankfurt)
Linkup Technologies SAS, Frankreich	Websuche	EU
SideGuide Technologies, Inc. (Firecrawl), USA	Import öffentlicher Webseiten in Wissensdatenbanken	USA
Google LLC, USA	Kalenderabfrage für Embed-Chatbots	USA
Vercel Inc., USA (AI Gateway)	Freigeschaltete KI-Modelle außerhalb der EU	USA und weitere Drittländer
Microsoft Ireland Operations Limited, Amazon Web Services EMEA SARL, Google Cloud EMEA Limited	Freigeschaltete KI-Modelle mit globaler Bereitstellung	Weltweit, einschließlich USA

Von Anbietern, die der Kunde selbst anbindet, etwa sein Microsoft-365-Mandant, ruft die Plattform Daten in seinem Auftrag ab. Diese Anbieter sind Vertragspartner des Kunden und keine Unterauftragsverarbeiter des Anbieters. Ebenfalls nicht erfasst sind Verarbeitungen, für die der Anbieter selbst verantwortlich ist, etwa die Abrechnung über Stripe und die Reichweitenmessung der öffentlichen Website.

Anlage 3: Technische und organisatorische Maßnahmen

Vertraulichkeit

- Mandantentrennung in der Datenbank durch zeilenbasierte Zugriffsregeln (Row Level Security); jede Organisation sieht nur ihre eigenen Daten.
- Abgestuftes Rollen- und Rechtekonzept je Organisation mit serverseitiger Prüfung jeder Anfrage.
- Anmeldung über persönliche, zeitlich begrenzte Anmelde-Links.
- Zugangsdaten für Integrationen werden mit AES-256-GCM unter einem eigenen Schlüssel je Organisation verschlüsselt gespeichert.
- Embed-Chatbots nur auf freigegebenen Domains, Besucher werden über pseudonyme Sitzungskennungen geführt.
- Datenanalyse durch Agenten in isolierten, kurzlebigen Umgebungen ohne Netzwerkzugriff.

Integrität

- Verschlüsselte Übertragung aller Verbindungen über TLS.
- Protokollierung sicherheitsrelevanter Vorgänge wie Rollenänderungen und Vertragsannahmen in einem Sicherheitsprotokoll.
- Begrenzung der Anfragerate gegen Missbrauch und automatisierte Angriffe.

Verfügbarkeit und Belastbarkeit

- Betrieb bei Infrastrukturanbietern nach Anlage 2 mit Verschlüsselung ruhender Daten.
- Länger laufende Vorgänge über eine dauerhafte Ablaufsteuerung, die nach Störungen wiederaufsetzt.
- Fehlerüberwachung, die standardmäßig keine personenbezogenen Daten erfasst.

Datenschutz durch Voreinstellung

- KI-Modelle außerhalb der EU sind ausgeschaltet; der Anbieter schaltet sie nur auf Weisung des Kunden frei.
- Kein Training von KI-Modellen mit Kundendaten.
- Einstellbare Aufbewahrungsfrist mit automatischer Löschung; Löschung einer Organisation einschließlich aller gespeicherten Dateien.
- Selbstständiger Export der Organisationsdaten als JSON-Datei (Art. 20 DSGVO).

Organisation

- Verpflichtung aller Beschäftigten auf Vertraulichkeit.
- Zugriff auf Kundendaten nur, soweit für Betrieb und Support erforderlich.
- Auswahl und vertragliche Bindung der Unterauftragsverarbeiter nach Art. 28 Abs. 4 DSGVO.