Vertrag zur Auftragsverarbeitung

nach Art. 28 DSGVO

Gromai · Fassung 2026-08-1 · Stand: 13. August 2026

Entwurfsfassung — noch nicht anwaltlich geprüft. Vor der Verwendung im Rechtsverkehr bitte prüfen lassen.

Zwischen dem Kunden — nachfolgend „Auftraggeber" — und Finn Burgsmüller, Wuppertal — nachfolgend „Auftragnehmer" — wird der folgende Vertrag über die Verarbeitung personenbezogener Daten im Auftrag geschlossen. Er ergänzt den Hauptvertrag über die Nutzung von Gromai und ist Bestandteil der Allgemeinen Geschäftsbedingungen (§ 12).

§ 1 Gegenstand und Dauer

(1) Dieser Vertrag konkretisiert die Pflichten der Parteien zum Datenschutz, die sich aus der Nutzung von Gromai ergeben. Er gilt für alle Verarbeitungen personenbezogener Daten, die der Auftragnehmer für den Auftraggeber durchführt.

(2) Auftraggeber und Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Kunde. Auftragnehmer und Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO ist Finn Burgsmüller, Wuppertal.

(3) Der Vertrag beginnt mit dem Hauptvertrag über die Nutzung der Software und endet mit ihm. Er kann nicht gesondert gekündigt werden, solange der Hauptvertrag besteht.

(4) Bei Widersprüchen zwischen diesem Vertrag und den Allgemeinen Geschäftsbedingungen geht dieser Vertrag in datenschutzrechtlichen Fragen vor.

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich, um die vertraglich geschuldete Leistung zu erbringen: Bereitstellung der Software, Speicherung und Aufbereitung der vom Auftraggeber hochgeladenen Unterlagen, KI-gestützter Abgleich gegen die vom Auftraggeber hinterlegten Regelwerke sowie Erstellung der Prüfberichte.

(2) Die Verarbeitung umfasst insbesondere das Erheben, Erfassen, Speichern, Auslesen, Verwenden, Übermitteln an die in Anlage 2 genannten Unterauftragsverarbeiter, Einschränken und Löschen.

(3) Die Verarbeitung findet in der Bundesrepublik Deutschland statt. Übermittlungen in Drittländer erfolgen nur im Rahmen der in Anlage 2 aufgeführten Unterauftragsverarbeitung und auf der dort jeweils genannten Grundlage.

(4) Der Auftragnehmer verarbeitet die Daten nicht zu eigenen Zwecken. Insbesondere nutzt er Inhalte des Auftraggebers nicht zum Training von KI-Modellen und gibt sie zu diesem Zweck nicht an Dritte weiter.

§ 3 Datenkategorien und Kreis der Betroffenen

(1) Gegenstand der Verarbeitung sind die in Anlage 3 aufgeführten Datenkategorien und Betroffenenkreise.

(2) Der Auftraggeber bestimmt allein, welche Unterlagen er hochlädt. Er stellt sicher, dass darin keine personenbezogenen Daten besonderer Kategorien im Sinne des Art. 9 DSGVO enthalten sind, sofern dies nicht zuvor gesondert in Textform vereinbart wurde.

§ 4 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Die Nutzung der Software durch den Auftraggeber und seine Nutzer gilt als solche Weisung; darüber hinausgehende Weisungen bedürfen der Textform.

(2) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er ist berechtigt,

die Ausführung auszusetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

(3) Verarbeitet der Auftragnehmer Daten aufgrund einer rechtlichen Verpflichtung, unterrichtet er den Auftraggeber vor der Verarbeitung darüber, sofern das Recht dies nicht verbietet.

§ 5 Vertraulichkeit

(1) Der Auftragnehmer setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterworfen sind. Die Verpflichtung besteht über das Ende der Tätigkeit hinaus fort.

(2) Der Auftragnehmer stellt sicher, dass die zur Verarbeitung befugten Personen über die einschlägigen Datenschutzvorschriften unterrichtet sind und Zugriff nur im erforderlichen Umfang erhalten.

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und hält sie während der Vertragsdauer aufrecht.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie anpassen, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber auf Anfrage mit.

§ 7 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, die in Anlage 2 aufgeführten Unterauftragsverarbeiter einzusetzen.

(2) Der Auftragnehmer kündigt die Hinzuziehung weiterer oder den Austausch bestehender Unterauftragsverarbeiter mindestens vier Wochen vorher in Textform an. Der Auftraggeber kann aus einem wichtigen, datenschutzrechtlich begründeten Anlass innerhalb dieser Frist widersprechen.

(3) Widerspricht der Auftraggeber, kann der Auftragnehmer die betroffene Leistung einstellen oder den Vertrag mit Wirkung zum geplanten Wechsel kündigen. Bereits gezahlte, nicht verbrauchte Entgelte werden anteilig erstattet.

(4) Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf ein Schutzniveau, das diesem Vertrag entspricht, und haftet für deren Verhalten wie für eigenes.

§ 8 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber im erforderlichen Umfang bei der Erfüllung von Anträgen betroffener Personen nach Art. 15 bis 22 DSGVO. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er das Anliegen unverzüglich an den Auftraggeber weiter und antwortet nicht selbst.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und bei vorherigen Konsultationen nach Art. 36 DSGVO, soweit die dafür erforderlichen Informationen nur ihm vorliegen.

(3) Die Software stellt dem Auftraggeber einen Datenexport im JSON-Format bereit, mit dem sich Auskunfts- und Übertragbarkeitsansprüche selbst erfüllen lassen.

§ 9 Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, in Textform.

(2) Die Meldung enthält, soweit bekannt, eine Beschreibung des Vorfalls, die betroffenen Datenkategorien, die ungefähre Zahl der Betroffenen, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Gegenmaßnahmen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei dessen Melde- und Benachrichtigungspflichten

nach Art. 33 und 34 DSGVO. Meldungen an die Aufsichtsbehörde nimmt der Auftraggeber vor.

§ 10 Löschung und Rückgabe

(1) Nach Beendigung des Hauptvertrags kann der Auftraggeber seine Daten noch 30 Tage lang über die Exportfunktion abrufen.

(2) Nach Ablauf dieser Frist löscht der Auftragnehmer die im Auftrag verarbeiteten personenbezogenen Daten einschließlich hochgeladener Unterlagen und erzeugter Prüfberichte, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

(3) Von der Löschung ausgenommen sind Daten, die der Auftragnehmer als eigener Verantwortlicher zum Nachweis des Vertragsschlusses und der erteilten Zustimmungen benötigt, sowie Buchhaltungsunterlagen im Rahmen der handels- und steuerrechtlichen Aufbewahrungsfristen.

(4) Auf Anfrage bestätigt der Auftragnehmer die Löschung in Textform.

§ 11 Nachweise und Kontrollen

(1) Der Auftragnehmer weist die Einhaltung der Pflichten aus diesem Vertrag auf Anfrage nach, insbesondere durch Auskünfte, die Beschreibung der Maßnahmen nach Anlage 1 sowie vorliegende Zertifikate, Prüfberichte oder Auftragsverarbeitungsverträge seiner Unterauftragsverarbeiter.

(2) Reichen diese Nachweise im Einzelfall nicht aus, kann der Auftraggeber eine Prüfung vor Ort durchführen oder durch einen zur Verschwiegenheit verpflichteten, nicht mit dem Auftragnehmer im Wettbewerb stehenden Prüfer durchführen lassen. Die Prüfung wird mit angemessener Frist, zu üblichen Geschäftszeiten und ohne vermeidbare Betriebsstörung angekündigt.

(3) Der Auftraggeber trägt die Kosten einer Prüfung vor Ort, es sei denn, sie deckt einen erheblichen Verstoß des Auftragnehmers auf.

§ 12 Haftung und Schlussbestimmungen

(1) Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses.

(3) Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.

(4) Fragen zu diesem Vertrag beantwortet der Auftragnehmer unter datenschutz@gromai.de.

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

Schutzziel	Beschreibung
Vertraulichkeit — Zutrittskontrolle	Die Anwendung läuft auf einem angemieteten Server der netcup GmbH im Rechenzentrum Nürnberg. Der physische Zutritt wird durch den Hoster kontrolliert; ein eigener Serverraum besteht nicht.
Vertraulichkeit — Zugangskontrolle	Anmeldung ausschließlich über den Identitätsdienst Clerk mit individuellen Konten. Der Verwaltungsbereich ist zusätzlich durch ein zweites, separat gehashtes Passwort geschützt und nach fünf Fehlversuchen für fünf Minuten gesperrt. Die Selbstregistrierung ist während des Erprobungsbetriebs geschlossen.
Vertraulichkeit — Zugriffskontrolle	Rollenbasierte Rechte je Organisation. Jede Datenabfrage ist auf die Organisation des anfragenden Nutzers eingegrenzt; hochgeladene Dateien liegen in privaten Objektspeicher-Buckets und sind nur über kurzlebige, signierte URLs hinter einer Berechtigungsprüfung erreichbar.
Vertraulichkeit — Trennungskontrolle	Mandantentrennung auf Datenbankebene über die Organisationszugehörigkeit. Erprobungs- und Produktivumgebung nutzen getrennte Datenbanken und getrennte Objektspeicher-Buckets.
Integrität — Weitergabekontrolle	Sämtlicher Datenverkehr ausschließlich über TLS mit automatisch erneuerten Zertifikaten. HTTP Strict Transport Security und eine Content Security Policy sind serverseitig gesetzt. Datenbank, Objektspeicher und der Extraktionsdienst sind an die lokale Schnittstelle gebunden und aus dem Internet nicht erreichbar.
Integrität — Eingabekontrolle	Sicherheitsrelevante Vorgänge werden mit Zeitpunkt, handelndem Konto und Organisation in einem Prüfprotokoll erfasst. Erteilte Zustimmungen werden unveränderlich mit Fassung und Zeitpunkt protokolliert.
Verfügbarkeit und Belastbarkeit	Reverse-Proxy mit automatischer Zertifikatserneuerung; Veröffentlichungen bauen das neue Abbild vollständig, bevor der laufende Dienst getauscht wird, sodass ein fehlgeschlagener Build den Betrieb nicht unterbricht. Eine bestimmte Verfügbarkeitsquote wird nicht zugesagt.
Verfahren zur Überprüfung und Bewertung	Statische Codeprüfung und automatisierte Tests laufen vor jeder Veröffentlichung. Zugangsdaten liegen ausschließlich in Umgebungsvariablen und nicht in der Versionsverwaltung. Die Maßnahmen werden bei wesentlichen Änderungen der Verarbeitung überprüft.
Auftragskontrolle	Mit allen in Anlage 2 genannten Unterauftragsverarbeitern bestehen Verträge nach Art. 28 DSGVO; für Übermittlungen in Drittländer liegen die dort genannten Garantien vor.

Anlage 2 — Unterauftragsverarbeiter

Dienstleister	Leistung, Zweck und Grundlage
netcup GmbH (Deutschland)	Server und Rechenzentrum Nürnberg — Hosting der Anwendung, der PostgreSQL-Datenbank und des selbst betriebenen Objektspeichers. Grundlage: Verarbeitung ausschließlich in Deutschland.
Clerk, Inc. (USA)	Clerk (Authentifizierung und Organisationsverwaltung) — Anmeldung, Sitzungsverwaltung, Einladungen. Grundlage: EU-Standardvertragsklauseln.

Mistral AI SAS (Frankreich)	Mistral-API (mistral-large-latest) — Unabhängige Zweitprüfung in Phase 3 — nur was Claude und Mistral beide finden, gilt ohne weitere Instanz als Befund. Grundlage: Verarbeitung in der EU.
Anthropic, PBC (USA)	Claude-API (u. a. claude-haiku-4-5, claude-sonnet-4-6) — Kategorisierung, Regelwerks-Zuordnung, Vorwärtsprüfung und Berichterstellung. Grundlage: EU-US Data Privacy Framework. Anthropic speichert API-Inhalte standardmäßig kurzzeitig zu Missbrauchsschutz-Zwecken zwischen.
Google LLC (USA)	Gemini-API (gemini-2.5-pro) — Dritte Instanz (Tiebreaker), wenn Claude und Mistral sich widersprechen — übermittelt werden nur die strittigen Textstellen samt Regelwerks-Auszügen. Grundlage: EU-US Data Privacy Framework.
OpenAI, L.L.C. (USA)	Embedding-API (text-embedding-3-small) — Vektor-Indexierung von Regelwerken für die Semantiksuche. Grundlage: EU-US Data Privacy Framework.

Anlage 3 — Datenkategorien und Kreis der Betroffenen

Datenkategorien

Kategorie	Beschreibung
Kontaktdaten der Nutzer	Name, E-Mail-Adresse, Profilbild, optional Titel und Telefonnummer sowie Rolle innerhalb der Organisation.
Nutzungsdaten	Anmeldezeitpunkte, Sitzungskennungen, durchgeführte Prüfläufe, Verbrauch von Kontingenten, Prüfprotokoll-Einträge.
Inhaltsdaten	Hochgeladene Projektunterlagen und Regelwerke, daraus extrahierte Texte, erzeugte Befunde und Prüfberichte, Kommentare und Freigabeentscheidungen. Personenbezug entsteht hier nur, soweit die Unterlagen des Auftraggebers solche Daten enthalten.
Vertrags- und Abrechnungsdaten	Organisationsname und Anschrift, Umsatzsteuer-Identifikationsnummer, Tarif, Zahlungsart und letzte vier Stellen des Zahlungsmittels. Vollständige Zahlungsdaten verarbeitet ausschließlich der Zahlungsdienstleister.

Kreis der betroffenen Personen

Personenkreis	Beschreibung
Beschäftigte des Auftraggebers	Nutzerinnen und Nutzer, die für den Auftraggeber mit der Software arbeiten.
Von eingeladenen Personen	Externe Beteiligte, die der Auftraggeber in seine Organisation oder in einzelne Projekte einlädt.
In Unterlagen benannte Personen	Personen, die in den hochgeladenen Projektunterlagen genannt sind — etwa Planverfasser, Prüfsachverständige, Ansprechpartner von Auftraggebern oder ausführenden Firmen.