EuGPT

MUSTERFASSUNG NACH ART. 28 DSGVO

Auftragsverarbeitungsvertrag

Fassung 1.0 · gültig seit 17.07.2026

> **Muster – noch kein Vertrag:** Ein Vertrag entsteht erst im authentifizierten EuGPT-Compliance-Center nach individuellen Angaben, vollständiger Vorschau und elektronischer Annahme.

Vertrag gemäß Art. 28 DSGVO

Auftragsverarbeitungsvertrag

Referenz WIRD BEIM ABSCHLUSS ERZEUGT · Fassung 1.0 · gültig seit 17.07.2026

Parteien

Verantwortlicher

[Vollständige Firma des Verantwortlichen]
[Vollständige Geschäftsanschrift]
[Land]

vertreten beim elektronischen Abschluss durch [Name], [Funktion], [Geschäftliche E-Mail-Adresse]

Auftragsverarbeiter

intercolo GmbH (EuGPT)
Carl-Goerdeler-Straße 114
60320 Frankfurt am Main, Deutschland

vertreten durch Maxim Gade, Geschäftsführer

Verantwortlicher und Auftragsverarbeiter werden nachfolgend gemeinsam „Parteien“ genannt. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien für Verarbeitungen, die der Auftragsverarbeiter im Rahmen von EuGPT im Auftrag des Verantwortlichen durchführt.

1. Gegenstand, Abgrenzung und Dauer

1. Gegenstand ist die weisungsgebundene Verarbeitung von Kundeninhalten bei der Bereitstellung der ausgewählten EuGPT-Leistungen. Einzelheiten ergeben sich aus Anlage 1.
2. Die Laufzeit entspricht der Laufzeit des Hauptvertrags über EuGPT. Pflichten, die ihrer Natur nach fortbestehen, gelten bis zur vollständigen Rückgabe oder Löschung der Auftragsdaten fort.
3. Nutzerkonto-, Vertrags-, Abrechnungs-, Betrugspräventions- und zwingend erforderliche IT-Sicherheitsdaten, deren Zwecke und Mittel die intercolo GmbH selbst festlegt, sind nicht Gegenstand dieser Auftragsverarbeitung. Für diese Verarbeitung gilt die Datenschutzerklärung von EuGPT.
4. Dieser AVV hat für seinen Regelungsgegenstand Vorrang vor widersprechenden Datenschutzbestimmungen des Hauptvertrags.

2. Weisungen des Verantwortlichen

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich Weisungen zu Drittlandübermittlungen, soweit keine gesetzliche Verarbeitungspflicht besteht.
2. Die Nutzung und Konfiguration der EuGPT-Funktionen, dokumentierte Supportaufträge sowie Weisungen in Textform gelten als Weisungen. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
3. Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtswidrig, informiert er den Verantwortlichen unverzüglich. Er darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.
4. Gesetzlich vorgeschriebene Verarbeitungen werden dem Verantwortlichen vorab mitgeteilt, soweit das Gesetz eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

3. Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, die Zulässigkeit seiner Weisungen sowie die Wahrung der Betroffenenrechte verantwortlich.
2. Er informiert den Auftragsverarbeiter unverzüglich über Fehler, Unregelmäßigkeiten oder besondere Risiken und übermittelt nur solche Daten, deren Verarbeitung für den festgelegten Zweck erforderlich ist.

3. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO und Daten über strafrechtliche Verurteilungen oder Straftaten nach Art. 10 DSGVO dürfen nur bei dokumentierter Rechtsgrundlage und angemessenen zusätzlichen Schutzmaßnahmen verarbeitet werden.

4. Vertraulichkeit und berechtigte Personen

1. Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterworfen sind.
2. Zugriffsrechte werden nach Aufgabenbezug und Need-to-know-Prinzip vergeben und bei Wegfall der Erforderlichkeit entzogen.
3. Die Vertraulichkeitspflichten bestehen nach Beendigung der Tätigkeit und dieses Vertrags fort.

5. Sicherheit der Verarbeitung

1. Der Auftragsverarbeiter setzt die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen ein und gewährleistet ein dem Risiko angemessenes Schutzniveau nach Art. 32 DSGVO.
2. Die Maßnahmen dürfen weiterentwickelt werden, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche nachteilige Änderungen werden dokumentiert.
3. Der Auftragsverarbeiter überprüft die Angemessenheit und Wirksamkeit der Maßnahmen regelmäßig und berücksichtigt dabei Stand der Technik, Implementierungskosten, Art, Umfang, Umstände, Zwecke und Risiken der Verarbeitung.

6. Unterstützung und Betroffenenrechte

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung durch geeignete Maßnahmen bei der Erfüllung von Betroffenenrechten.
2. Anfragen betroffener Personen, die erkennbar den Verantwortlichen betreffen, werden ohne inhaltliche Bearbeitung unverzüglich weitergeleitet, sofern keine abweichende Weisung besteht.
3. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der verfügbaren Informationen bei der Einhaltung der Art. 32 bis 36 DSGVO, insbesondere bei Sicherheitsbewertungen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

7. Datenschutzverletzungen

1. Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Auftragsdaten unverzüglich nach Bekanntwerden an den vereinbarten Datenschutzkontakt.
2. Die Erstmeldung enthält die zu diesem Zeitpunkt verfügbaren Angaben zu Art und Umfang, betroffenen Daten und Personen, wahrscheinlichen Folgen, ergriffenen oder vorgeschlagenen Maßnahmen sowie einen Kontakt für Rückfragen. Fehlende Angaben werden ohne unangemessene Verzögerung nachgereicht.
3. Der Auftragsverarbeiter trifft angemessene Sofortmaßnahmen zur Eindämmung und unterstützt den Verantwortlichen bei dessen gesetzlichen Melde- und Informationspflichten.

8. Unterauftragsverarbeiter

1. Der Verantwortliche erteilt die allgemeine schriftliche Genehmigung zum Einsatz der in Anlage 3 genannten Unterauftragsverarbeiter.
2. Beabsichtigte Hinzufügungen oder Ersetzungen werden grundsätzlich mindestens 30 Tage vor Einsatz an die für den Vertrag hinterlegte geschäftliche E-Mail-Adresse mitgeteilt. Der Verantwortliche kann innerhalb von 14 Tagen aus berechtigten datenschutzrechtlichen Gründen widersprechen. Die Parteien suchen eine zumutbare Alternative; ist diese nicht möglich, bleiben gesetzliche und vertragliche Beendigungsrechte unberührt.
3. Der Auftragsverarbeiter legt dem Unterauftragsverarbeiter durch Vertrag im Wesentlichen dieselben Datenschutzpflichten auf. Er bleibt gegenüber dem Verantwortlichen für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich.
4. Reine Nebenleistungen ohne Zugriff auf Auftragsdaten gelten nicht als Unterauftragsverarbeitung. Eigenständig Verantwortliche, insbesondere bei bestimmten Zahlungs- oder gesetzlichen Prüfprozessen, werden in der Datenschutzerklärung gesondert ausgewiesen.

9. Drittlandübermittlungen

1. Eine Verarbeitung außerhalb der EU/des EWR erfolgt nur auf dokumentierte Weisung und bei Vorliegen der Voraussetzungen des Kapitels V DSGVO.
2. Bei der Betriebsart „Self-Hosted Deutschland“ werden keine optionalen externen KI-Provider für Kundeninhalte eingesetzt. Bei ausdrücklich gewählter externer Betriebsart gelten nur die in Anlage 3 dokumentierten und vertraglich freigegebenen Provider.
3. Soweit ein Drittlandtransfer stattfindet, dokumentiert der Auftragsverarbeiter den verwendeten Transfermechanismus und unterstützt bei erforderlichen Transferbewertungen.

10. Nachweise, Audits und Aufsicht

1. Der Auftragsverarbeiter stellt alle Informationen zur Verfügung, die zum Nachweis der Pflichten nach Art. 28 DSGVO erforderlich sind, und ermöglicht angemessene Audits einschließlich Inspektionen.
2. Audits sollen zunächst anhand aktueller Dokumentationen, Prüfberichte oder geeigneter Nachweise erfolgen. Vor-Ort-Prüfungen werden mit angemessener Frist, während üblicher Geschäftszeiten und unter Schutz von Betriebsgeheimnissen sowie Daten anderer Kunden durchgeführt; dringende anlassbezogene Prüfungen bleiben möglich.
3. Der Verantwortliche kann einen fachkundigen, unabhängigen und zur Vertraulichkeit verpflichteten Prüfer beauftragen. Gesetzliche Befugnisse der Aufsichtsbehörden bleiben unberührt.

11. Rückgabe und Löschung

1. Nach Beendigung der Leistungen löscht oder gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle Auftragsdaten zurück und löscht vorhandene Kopien, soweit keine gesetzliche Aufbewahrungspflicht besteht.
2. Daten in Sicherungen werden im Rahmen des regulären, dokumentierten Überschreibzyklus gelöscht und bis dahin vor weiterer produktiver Verarbeitung geschützt.
3. Der Abschluss- und Integritätsnachweis dieses AVV wird für die Dauer gesetzlicher vertraglicher Nachweis- und Aufbewahrungspflichten gespeichert; er enthält keine Kundeninhalte.

12. Schlussbestimmungen

1. Änderungen dieses Vertrags einschließlich der Anlagen bedürfen der Textform. Der elektronische Abschluss erfüllt Art. 28 Abs. 9 DSGVO.
2. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die Bestimmung durch eine wirksame Regelung, die dem datenschutzrechtlichen Zweck möglichst nahekommt.
3. Im Übrigen gelten Haftung, Gerichtsstand und anwendbares Recht des Hauptvertrags, soweit zwingendes Datenschutzrecht nicht entgegensteht.

Anlage 1 – Beschreibung der Verarbeitung

Gegenstand und Zweck Bereitstellung der ausgewählten EuGPT-Funktionen zur weisungsgebundenen KI-Verarbeitung.

Dauer Dauer des Hauptvertrags zuzüglich technisch erforderlicher Lösch- und Rückgabephase.

Leistungsbereiche EuGPT Web-Chat und Chat-Verläufe; EuGPT API und API-Zugangsdaten; Custom GPTs, Assistenten und Systemanweisungen; Datei-Uploads, Projekte und Wissensquellen

Datenkategorien Identifikations- und Kontaktdaten, die in Kundeninhalte eingegeben werden; Prompts, Eingaben, Antworten und Chat-Inhalte; Hochgeladene Dateien und daraus extrahierte Inhalte; Vom Verantwortlichen übermittelte technische IDs und Metadaten.

Betroffene Personen Beschäftigte und Bewerber des Verantwortlichen; Kunden, Interessenten und Ansprechpartner; Lieferanten, Dienstleister und Geschäftspartner; Weitere Personen, deren Daten der Verantwortliche eingibt.

Art.-9-Daten Nach Angabe des Verantwortlichen nicht planmäßig vorgesehen.

Art.-10-Daten Nach Angabe des Verantwortlichen nicht planmäßig vorgesehen.

Betriebsart Self-Hosted Deutschland; keine optionalen externen KI-Provider für Kundeninhalte.

Training Keine Nutzung von Kundeninhalten zum Training eigener Self-Hosted-Modelle.

Löschung Nach Weisung, durch Produktfunktionen oder nach Vertragsende gemäß Ziffer 11 und den dokumentierten Löschfristen.

Anlage 2 – Technische und organisatorische Maßnahmen

Zutrittskontrolle

Unbefugten physischen Zutritt zu Verarbeitungssystemen verhindern.

- Betrieb der Kerninfrastruktur in deutschen Rechenzentrumsumgebungen mit geregeltem Zutritt
- Zutrittsberechtigungen nach Aufgabenbezug und Need-to-know-Prinzip
- Dokumentierte Vergabe und Entziehung physischer Berechtigungen

Zugangs- und Authentisierungskontrolle

Unbefugte Nutzung von Systemen und Konten verhindern.

- Personenbezogene Benutzerkonten und rollenbasierte administrative Berechtigungen
- Sichere Passwort-Hashes und geschützte, zeitlich begrenzte Sitzungen
- Begrenzung administrativer Zugänge auf autorisierte Beschäftigte
- Protokollierung sicherheitsrelevanter administrativer Vorgänge

Zugriffs- und Mandantentrennung

Sicherstellen, dass Daten nur im Rahmen der jeweiligen Berechtigung verarbeitet werden.

- Anwendungsseitige Prüfung von Eigentümerschaft und Berechtigungen
- Trennung von Benutzer-, Chat-, Projekt- und API-Daten anhand der jeweiligen Kontozuordnung
- Gesonderte Administratorrolle mit protokollierten Administrationsvorgängen
- Server- und Modellzugriffe nach Freigabe und Zugriffstyp

Übertragungs- und Weitergabekontrolle

Daten bei Übertragung schützen und Empfänger nachvollziehbar begrenzen.

- Verschlüsselte HTTPS-Verbindungen im Produktivbetrieb
- Verschlüsselte Speicherung externer Provider-Zugangsdaten in der Anwendung
- Dokumentierte Auswahl und Freigabe externer KI-Provider
- Keine Nutzung von Kundeneingaben zum Training eigener Self-Hosted-Modelle

Eingabe- und Protokollkontrolle

Wesentliche Änderungen und administrative Zugriffe nachvollziehbar machen.

- Audit-Protokoll für administrative Tätigkeiten
- Nutzungs- und Accounting-Datensätze mit Benutzer-, Modell- und Zeitbezug
- Begrenzte Aufbewahrung technischer Protokolle nach festgelegtem Löschkonzept

Verfügbarkeit und Wiederherstellung

Verfügbarkeit und zeitnahe Wiederherstellbarkeit personenbezogener Daten unterstützen.

- Betriebsmonitoring für Plattform- und Inferenzkomponenten
- Regelmäßige Datensicherungen nach internem Sicherungskonzept
- Dokumentierte Behandlung technischer Störungen und Sicherheitsvorfälle
- Wiederherstellungsverfahren für relevante Plattformdaten

Datenschutzfreundliche Organisation

Datenschutzanforderungen über den gesamten Verarbeitungszyklus berücksichtigen.

- Vertraulichkeitsverpflichtung für berechtigte Beschäftigte
- Weisungsgebundene Verarbeitung und definierte Datenschutzkontakte
- Verfahren für Auskunft, Berichtigung, Export und Löschung
- Prüfung von Unterauftragsverarbeitern vor deren Einsatz
- Regelmäßige Überprüfung der Angemessenheit der Maßnahmen

Anlage 3 – Genehmigte Unterauftragsverarbeiter

intercolo GmbH

Carl-Goerdeler-Straße 114, 60320 Frankfurt am Main, Deutschland

Leistung: Rechenzentrums- und Serverbetrieb für Web-Frontend, Datenbank- und Inferenzkomponenten

Daten: Konto-, Vertrags-, Nutzungs- und Inhaltsdaten, soweit sie in der Plattform gespeichert werden

Verarbeitungsort: Frankfurt am Main, Deutschland

Drittland: Kein Drittlandtransfer vorgesehen

Status: Eingesetzt