

## Verzeichnis der Unterauftragsverarbeiter

EmpowerGPT zieht eine begrenzte Anzahl von Unterauftragsverarbeitern für die Bereitstellung von Infrastruktur, KI-Funktionalitäten, Analytik und Sicherheit heran. Sämtliche Unterauftragsverarbeiter sind so konfiguriert, dass die Datenresidenz in der EU, die DSGVO-Konformität sowie eine minimale Offenlegung von Daten gegenüber externen Stellen gewährleistet sind.

### Liste der Unterauftragsverarbeiter

Unterauftragsverarbeiter	Kategorie	Zweck	Datenkategorien	Verarbeitungsort	Schutzmaßnahmen
<b>Microsoft Azure</b>	Infrastruktur	Kerninfrastruktur, Rechenleistung, Speicher, Netzwerk (AKS, Blob Storage, PostgreSQL, VNet)	Eingabeaufforderungen, Dokumente, Embeddings, Metadaten, Protokolle	Germany West Central	<ul style="list-style-type: none"> <li>Ausschließlich private Endpunkte</li> <li>Verschlüsselung im Ruhezustand und während der Übertragung</li> <li>Strikte EU-Datenresidenz</li> </ul>
<b>Azure OpenAI</b>	KI / ML	LLM-Inferenz und Embeddings (primäre KI-Ebene)	Eingabeaufforderungen, Vervollständigungen, Embeddings	EU-Datenzone	<ul style="list-style-type: none"> <li>Keine Datenspeicherung (Missbrauchs-Monitoring unter genehmigter Ausnahmeregelung deaktiviert)</li> <li>Keine Speicherung von Eingabeaufforderungen/Vervollständigungen</li> <li>Keine regionsübergreifende Verarbeitung</li> </ul>
<b>Google Cloud AI (Gemini + Claude über GCP)</b>	KI / ML	Gemini-Modelle (Google) sowie Claude-Modelle über GCP-Integration	Eingabeaufforderungen, Antworten, Kontextdaten	Ausschließlich EU-Region (konfigurierte Bereitstellung)	<ul style="list-style-type: none"> <li>Verarbeitung auf EU-basierte GCP-Regionen beschränkt</li> <li>Keine regionsübergreifende Übertragung (gemäß Konfiguration)</li> <li>Datenschutzkontrollen auf Unternehmensniveau über GCP</li> </ul>

Unterauftragsverarbeiter	Kategorie	Zweck	Datenkategorien	Verarbeitungsort	Schutzmaßnahmen
<b>Azure Speech Service</b>	Sprache	Sprache-zu-Text-Transkription	Audioeingabe, Transkriptionsergebnisse	EU-konforme Azure-Region	<ul style="list-style-type: none"> <li>• EU-konforme Verarbeitung</li> </ul>
<b>E2B</b>	Code-Ausführung	Sichere, in einer Sandbox isolierte Code-Ausführung (Code-Interpreter)	Von Nutzern übermittelter Code, Ausführungsergebnisse, temporäre Laufzeitdaten	Vom Anbieter verwaltete Infrastruktur	<ul style="list-style-type: none"> <li>• Isolierte, kurzlebige Ausführungsumgebungen</li> </ul>
<b>Cloudflare</b>	Edge / Sicherheit	DNS, CDN, WAF, DDoS-Schutz	IP-Adresse, Anfrage-Metadaten	Globales Edge-Netzwerk	<ul style="list-style-type: none"> <li>• Vollständig DSGVO-konforme Konfiguration</li> </ul>
<b>PostHog</b>	Analytik	Produkt- und Nutzungsanalytik	Ereignisdaten, Nutzungs-Metadaten	EU (konfigurierte Bereitstellung)	<ul style="list-style-type: none"> <li>• Vollständig DSGVO-konforme Konfiguration</li> <li>• Minimale Erhebung personenbezogener Daten</li> <li>• Keine Erfassung von KI-Eingabeaufforderungen oder sensiblen Inhalten</li> </ul>

## Selbst gehostete Komponenten (keine Unterauftragsverarbeiter)

Die folgenden Komponenten werden intern innerhalb der EmpowerGPT-Infrastruktur gehostet. Sie sind innerhalb der Microsoft Azure-Umgebung (AKS) bereitgestellt, laufen auf den eigenen Servern von EmpowerGPT und übermitteln keinerlei Daten an die ursprünglichen Software-Hersteller.

Komponente	Hinweise
<b>Keycloak</b>	Bereitgestellt innerhalb von Microsoft Azure (AKS). Wird auf den eigenen Servern von EmpowerGPT betrieben. Es werden keine Daten an die ursprünglichen Software-Hersteller übermittelt.
<b>Grafana</b>	
<b>Prometheus</b>	
<b>Grafana Loki</b>	

## Datenresidenz und -übertragungen

Grundsatz: Sämtliche Kundendaten werden innerhalb der EU verarbeitet, sofern nicht ausdrücklich etwas anderes für dedizierte Unternehmensbereitstellungen konfiguriert wurde.

Komponente	Verarbeitungsregion
<b>Primäre Infrastruktur (Azure)</b>	Germany West Central
<b>Azure OpenAI</b>	EU-Datenzone
<b>Google Cloud AI (Gemini + Claude)</b>	EU-Region
<b>Azure Speech Service</b>	EU-Region
<b>PostHog</b>	EU-Region

## Datenaufbewahrung und -löschung

Speicherart	Aufbewahrungsfrist / Details
<b>Blob Storage</b>	Vorläufige Löschung („Soft Delete“): 95 Tage · Versionierung aktiviert
<b>PostgreSQL-Sicherungen</b>	35 Tage
<b>Protokolle</b>	90 Tage
<b>Metriken</b>	10 Tage
<b>Löschfunktionen</b>	Löschung auf Anfrage über interne Dienste · Mandanten-Löschung (Multi-Tenant) · Vollständige Stilllegung der Infrastruktur (dedizierte Umgebungen)

## Änderungsmanagement

EmpowerGPT aktualisiert dieses Verzeichnis vor der Inbetriebnahme neuer Unterauftragsverarbeiter. Die Kunden werden gemäß den vertraglichen Verpflichtungen über wesentliche Änderungen unterrichtet.

*Bei Fragen zu diesem Verzeichnis wenden Sie sich bitte an [contact@empowergpt.ai](mailto:contact@empowergpt.ai)*