

Vertrauliche Arbeit. Nachvollziehbare Datenwege.

Für Kanzleipartner, IT und Datenschutz: die AnwaltGPT-Verarbeitung, die beschriebenen Schutzmaßnahmen und die Entscheidungen für Ihren Einsatz im Überblick.

Hosting im Europäischen Wirtschaftsraum (EWR)

AnwaltGPT wird auf Infrastruktur im EWR gehostet. Die konkrete Modellwahl und aktivierte Integrationen bestimmen, welche Dienste an einer Anfrage beteiligt sind.

01 Eingabe & ausgewählter Kontext

Web-App, Office Add-ins und weitere Zugänge übermitteln die für die gewählte Funktion benötigten Fragen, Textauszüge oder Dateien an die Plattform. Die Plattform prüft den Zugriff und führt Auftrag und Kontext zusammen.

02 Pseudonymisierung vor dem nachgelagerten Modell

Der eigene Pseudonymisierungsdienst kann erkannte personenbezogene Angaben durch konsistente Platzhalter ersetzen. Er wird nach Betreiberangabe bei Hetzner in Nürnberg betrieben. Die Funktion ist optional oder durch Kanzleivorgaben gesteuert.

03 Modellverarbeitung & Ergebnis

Je nach gewähltem Modell erfolgt die Verarbeitung über Azure, Bedrock oder Eigenbetrieb. Das Ergebnis fließt über die Plattform zurück zur Oberfläche. Bei deaktivierter Pseudonymisierung wird der ausgewählte Kontext ohne diesen Ersetzungsschritt weitergegeben.

Welche Daten sieht die Schutzschicht?

Die Plattform und der Pseudonymisierungsdienst erhalten den ursprünglichen Kontext. Die Ersetzung erfolgt vor der Weitergabe an das nachgelagerte KI-Modell. Sie ist keine Zusage einer vollständigen Anonymisierung.

[Datenfluss interaktiv erkunden → anwaltgpt.de/sicherheit](https://anwaltgpt.de/sicherheit)

Schutz durch Technik. Verantwortung im Betrieb.

Die bereitgestellten Sicherheitsrichtlinien beschreiben ein Informationssicherheits-Managementsystem mit Zuständigkeiten, technischen und organisatorischen Maßnahmen sowie regelmäßigen Überprüfungen.

Zugriff & Berechtigungen

Personengebundene Konten, minimale Rechtevergabe und klar begrenzte administrative Zugriffe. Die Richtlinien sehen zusätzliche Absicherung privilegierter Konten und die regelmäßige Prüfung ihrer Berechtigungen vor.

Verschlüsselung

Verschlüsselte Übertragung und Speicherung schützen Inhalte. Schlüsselverwaltung, zugelassene Verfahren und der Umgang mit Zugangsdaten werden in den Sicherheitsrichtlinien geregelt.

Entwicklung & Änderungen

Dokumentierte Änderungen, Code-Reviews und eine Trennung von Entwicklungs- und Betriebsaufgaben gehören zum beschriebenen Vorgehen. Schwachstellen und Sicherheitsaktualisierungen werden systematisch bearbeitet.

Betrieb & Wiederanlauf

Systemhärtung, Monitoring und Backup-Regelungen sollen Verfügbarkeit und Wiederherstellung unterstützen. Für Störungen sind Wiederanlaufverfahren und Zuständigkeiten vorgesehen.

Vertraulichkeit & Dienstleister

Verschwiegenheitsverpflichtungen, Lieferantenbewertung und vertragliche Regelungen bilden den organisatorischen Rahmen. Ein externer Datenschutz- und Informationssicherheitsbeauftragter unterstützt die Kontrolle.

Vorfälle & Verbesserung

Definierte Meldewege, Bewertung und Bearbeitung von Sicherheitsvorfällen sowie regelmäßige Überprüfungen dienen der kontinuierlichen Verbesserung. Kundenbezogene Verfahren werden vertraglich konkretisiert.

Arbeitsdaten und Trainingsnutzung sind verschiedene Fragen.

Arbeitsinhalte wie Akten, Dokumente und Verläufe können auf der Plattform gespeichert werden; technische Ereignisse und Nutzungsdaten werden getrennt betrachtet. Die beschriebene Standardkonfiguration sieht keine Nutzung von Mandatsdaten zum Modelltraining vor. Speicher- und Löschregeln richten sich nach Datenart, Funktion und Vereinbarung.

Cowork. Bewusst verbinden.

Bei Cowork liegen Dateien und Arbeitsbereich auf Ihrem Gerät. Ob der benötigte Kontext für eine Modellanfrage übertragen wird, hängt vom gewählten Modellzugang ab.

AnwaltGPT als Provider

Anfragen laufen mit Ihrem AnwaltGPT-Zugang und Kontingent über die Plattform. Der benötigte Kontext wird an die Plattform übermittelt; die gewählte Modellverarbeitung und anwendbare Kanzleivorgaben bestimmen die weiteren Schritte.

Eigener Provider

Ein eigener API-Schlüssel oder ein unterstütztes Abonnement ermöglicht einen anderen Modellzugang. Der Provider erhält die benötigten Anfrageinhalte. Es gelten die gewählte Konfiguration und die dafür vereinbarten Bedingungen.

Lokales Modell

Ein lokal eingerichtetes Modell, etwa über Ollama, kann die Modellanfrage auf dem Gerät verarbeiten. Optionaler Web-Abgleich, Plugins und MCP-Dienste sind davon getrennt: Aktivierte Verbindungen können zusätzliche Datenflüsse auslösen.

Dienste und Rollen: Azure, Bedrock und Eigenbetrieb beschreiben Modellwege; Hetzner ist für den Pseudonymisierungsdienst genannt. Die vollständige vertragliche Unterauftragsverarbeiterliste erhalten Sie mit den aktuellen Vertragsunterlagen.

Unterlagen für Ihre konkrete Kanzlei

Für die vertragliche Einordnung benötigen Sie den aktuellen AVV einschließlich Verarbeitungsbeschreibung, technischen und organisatorischen Maßnahmen und Unterauftragsverarbeiterliste sowie die passende Verschwiegenheitsvereinbarung. Maßgeblich sind die für Ihren Einsatz vereinbarten Fassungen.

[Vertragsunterlagen anfordern: info@mind-verse.de](mailto:info@mind-verse.de)

Grundlagen & Dokumentenstand

Produktbeschreibung und Betreiberangaben (08.09.2026), Mindverse General Information Security Guideline v1.0 und MindVerse ISMS Policies v1.1. Dieser Überblick erläutert die dokumentierte Organisation und Produktwege; konkrete Leistungen und Verarbeitung werden in den Vertragsunterlagen festgelegt.