

Wo Ihre Daten liegen und wer das geprüft hat

Zertifikate, Maßnahmen, Verarbeitungsorte und jeder Unterauftragsverarbeiter — alles, was IT, Datenschutz und Einkauf für eine Freigabe brauchen.

Stand: 12. August 2026 · Verantwortliche Stelle: DeutschlandGPT GmbH, Gabriele-Münter-Straße 3, 82110 Germering · info@deutschlandgpt.de

NACHWEISE

Zwei Normen, geprüft von TÜV SÜD

Beide Zertifikate mit Geltungsbereich, Registriernummer und Laufzeit.



ISO/IEC 27001:2022 — Informationssicherheit

Der TÜV hat geprüft, dass wir unsere Daten und Systeme systematisch schützen: Wer darf worauf zugreifen, was passiert bei einem Vorfall, wie wird das kontrolliert. Nicht von uns behauptet, sondern von außen im Audit belegt.

Registriernr. 12 310 66919/03 TMS

Geltungsbereich Entwicklung, Bereitstellung, Betrieb und das Management von KI-unterstützten Plattform- und Softwarelösungen

Laufzeit 13.05.2026 – 17.01.2027

[Zertifikat als PDF »](#) [English version »](#)



DIN EN ISO 9001:2015 — Qualitätsmanagement

Der TÜV hat geprüft, dass unsere Arbeit festen Abläufen folgt: Änderungen werden freigegeben, Fehler erfasst, Verbesserungen nachgehalten. Damit hängt die Qualität nicht daran, wer gerade zuständig ist.

Registriernr. 12 100 66919/02 TMS

Geltungsbereich Entwicklung, Bereitstellung und Vertrieb von KI-gestützten Lösungen

Laufzeit 06.03.2026 – 05.03.2029

[Zertifikat als PDF »](#)

Auf beiden Zertifikaten steht als Inhaberin die Muttergesellschaft (Titanom Group GmbH, auf dem Dokument unter der früheren Firmierung Titanom Technologies GmbH) — das Managementsystem wird gruppenweit als Multi-Site-Zertifizierung geführt. Die DeutschlandGPT GmbH ist darin als Standort namentlich ausgewiesen und vom Geltungsbereich erfasst. Ihr Vertragspartner ist die DeutschlandGPT GmbH.

Dazu: BSI C5 Typ 2 für das Hosting

BSI C5 ist der Prüfkatalog des Bundesamts für Sicherheit in der Informationstechnik für Cloud-Dienste. Ein Wirtschaftsprüfer bestätigt darin, dass die Sicherheitsmaßnahmen nicht nur beschrieben, sondern über einen Zeitraum auch wirksam waren — das ist der Typ 2, den die Open Telekom Cloud hat.

Für sie heißt das: Das Rechenzentrum, in dem Ihre Inhalte liegen, ist von außen geprüft — nicht von der Telekom behauptet und nicht von uns. Das Testat gehört der Telekom, deshalb steht es hier neben unseren Zertifikaten und nicht als eigenes. Den Testatauszug stellen wir auf Anfrage bereit.

ABLAUF

Was mit einer Eingabe passiert

Vier Schritte vom Tastendruck bis zur Antwort im Verlauf.

1. Ihre Eingabe verlässt den Browser verschlüsselt

Übertragung mit TLS 1.3. Bis zu unserer Plattform ist der Inhalt für Dritte nicht lesbar.

2. Sie erreicht unsere Plattform in Deutschland

Anwendung und Datenbank laufen auf der Open Telekom Cloud, betrieben von der T-Systems International GmbH in Deutschland. Dort liegen Verlauf, Dateien und Einstellungen.

3. Das Modell antwortet aus der EU

Für die Antwort geht der Inhalt an den gewählten Modellanbieter — über europäische Unternehmenszugänge, mit Verarbeitung in EU-Rechenzentren.

4. Beim Modellanbieter bleibt nichts

Zero-Data-Retention (ZDR) ist mit allen Modellanbietern vereinbart: keine Speicherung, keine Verwendung zum Training. Die Antwort landet zurück in Ihrem Verlauf, und nur dort.

AUF EINEN BLICK

Die sechs Angaben, die ein Fragebogen zuerst abfragt

Speicherort	Deutschland — Open Telekom Cloud (T-Systems), BSI C5-testiertes Hosting
Verarbeitung	Deutschland und EU. Der Verarbeitungsort ist je Unterauftragsverarbeiter vertraglich festgelegt
Training auf Kundendaten	Findet nicht statt
Auftragsverarbeitung	Vertrag nach Art. 28 DSGVO auf Basis der EU-Standardvertragsklauseln
Mandantentrennung	Logische Trennung aller Konversations-, Datei- und Konfigurationsdaten
Berufsgeheimnisträger	Eigener Betriebsmodus nach § 203 StGB mit eingeschränktem Kreis verpflichteter Unterauftragnehmer

MASSNAHMEN

Technische und organisatorische Maßnahmen

Auszug aus den vertraglich vereinbarten Maßnahmen. Verbindlich ist Anhang III des Auftragsverarbeitungsvertrags.

Infrastruktur

- Betrieb auf BSI C5-testierter Open Telekom Cloud (T-Systems), Rechenzentren in Deutschland
- Physische Sicherungsmaßnahmen beim Hostinganbieter
- Firewall und Netzwerksegmentierung
- Tägliche Datenbanksicherungen, 14 Tage Vorhaltung, verschlüsselt gespeichert

Zugang und Berechtigungen

- Zwei-Faktor-Authentifizierung
- Rollenbasiertes Berechtigungskonzept, Zugriff nur für befugte Personen
- Strenge Passwort-Richtlinien und Clean-Desk-Policy
- Protokollierung von Zugriffen und Änderungen

Daten und Übertragung

- Übertragung mit TLS 1.3, Verschlüsselung im Ruhezustand (AES), Zugangsdaten zusätzlich anwendungsseitig verschlüsselt
- Logische Trennung der Daten je Kundenorganisation
- Export Ihrer Inhalte jederzeit möglich — die Voraussetzung dafür, dass ein Anbieterwechsel offen bleibt
- Datenschutzfreundliche Voreinstellungen nach Art. 25 Abs. 2 DSGVO

KI-spezifisch

- Keine Nutzung von Kundendaten zum Training von KI-Modellen
- Freischaltung der Modelle und Anbieter je Organisation steuerbar
- Betriebsmodus für Berufsgeheimnisträger nach § 203 StGB
- Anbieterunabhängig: Ausweichsteuerung über mehrere Modellanbieter

Organisation

- Informationssicherheits-Managementsystem nach ISO/IEC 27001
- Qualitätsmanagement nach ISO 9001
- Externer Datenschutzbeauftragter
- Regelmäßige Schulungen und Datenschutz-Richtlinien

Betrieb und Notfall

- Incident-Response mit Notfallteam, Meldewegen und Eskalationsprozessen
- Dokumentiertes Datensicherungs-, Wiederherstellungs- und Notfallkonzept
- Öffentliche Statusseite mit Verfügbarkeitshistorie
- Responsible-Disclosure-Programm für Sicherheitsforschende

UNTERAUFTRAGSVERARBEITER

Wen wir einsetzen

Alle Unterauftragsverarbeiter mit Gegenstand und Verarbeitungsort. Identisch mit Anhang IV des Auftragsverarbeitungsvertrags.

Unterauftragsverarbeiter	Gegenstand	Ort	§ 203-Modus
T-Systems International GmbH	Betrieb von KI-Modellen und Speicherung persistenter Daten	DE	Ja
Hetzner Online GmbH	Betrieb von KI-Modellen und Speicherung persistenter Daten	DE	Nein
IONOS SE	Betrieb von KI-Modellen	EU	Nein
Microsoft Ireland Operations Limited (Azure)	Betrieb von KI-Modellen	EU	Ja
Amazon Web Services EMEA SARL (AWS)	Betrieb von KI-Modellen	EU	Ja
Google Cloud EMEA Limited	Betrieb von KI-Modellen	EU	Ja
Mistral AI SAS	Betrieb von KI-Modellen	EU	Nein
OpenAI Ireland Ltd	Betrieb von KI-Modellen	EU	Nein
Linkup Technologies SAS	Websuche-Funktion (Search API)	EU (Frankreich)	Ja
Functional Software, Inc. (Sentry)	Sammlung von Fehlermeldungen (Error- und Crash-Reporting)	EU (Verarbeitung im EU-Rechenzentrum); Unternehmenssitz USA	Ja (ohne Nutzerinhalte)

Verpflichtungsnachweis für Berufsgeheimnisträger

Im Berufsgeheimnisträger-Modus sind nur Unterauftragnehmer erreichbar, die eine Verschwiegenheitsverpflichtung nach § 203 Abs. 4 S. 2 StGB übernommen haben — mit Beleg, nicht als Behauptung.

Unterauftragnehmer / Rolle	Form der Verpflichtung	Beleg
T-Systems International GmbH (Open Telekom Cloud) Betrieb der Plattform, Speicherung persistenter Daten (DE)	Ausdrücklich in den Ergänzenden Bedingungen zur AVV: Wahrung der Vertraulichkeit nach § 203 StGB, Verpflichtung des Personals auf den Geheimnisschutz nach § 203 StGB und das Sozialgeheimnis nach § 35 SGB I.	AVV, Stand April 2025
Microsoft Ireland Operations Ltd. (Azure) Betrieb von KI-Modellen (EU)	Professional Secrecy Amendment als Bestandteil des Microsoft Customer Agreement, wirksam seit Beginn der Belieferung.	MCA inkl. German Data Secrecy Amendment
Amazon Web Services EMEA SARL Betrieb von KI-Modellen (EU)	Gesondertes Professional Secrecy Addendum zum AWS Customer Agreement, beidseitig unterzeichnet — Personalverpflichtung und Weitergabe an Subunternehmer eingeschlossen.	Addendum, wirksam 10.02.2026
Google Cloud EMEA Limited Betrieb von KI-Modellen (EU)	Gesondertes Professional Secrecy Agreement, beidseitig unterzeichnet.	Agreement, vollzogen 25.06.2026
Linkup Technologies SAS Websuche (EU); Übermittlung der Suchanfrage, keine Speicherung	Gesondertes Professional Secrecy Agreement, beidseitig unterzeichnet; Verpflichtung des Personals und Weitergabe an Subunternehmer in Textform eingeschlossen.	Agreement vom 17.08.2026
Functional Software, Inc. (Sentry) Fehler-Monitoring (EU-Rechenzentrum), ohne Nutzerinhalte	Gesonderte Verpflichtung nicht erforderlich, da dem Dienst keine fremden Geheimnisse offenbart werden — geregelt über den Auftragsverarbeitungsvertrag.	AVV / DPA

STEUERUNG

Was Ihre IT selbst in der Hand hat

Anmeldung über Ihr Firmenkonto

Single Sign-On über SAML und OIDC, Nutzerverwaltung automatisch über SCIM. Wer das Unternehmen verlässt, verliert den Zugang mit dem Firmenkonto — ohne dass jemand daran denken muss.

Rollen und Freigaben je Bereich

Welche Modelle, Funktionen und Datenquellen eine Gruppe benutzen darf, legt eine administrative Person fest. Die Personalabteilung braucht andere Freigaben als der Vertrieb.

Protokolle für den Nachweis

Aufgezeichnet wird, wer wann welche Funktion benutzt hat. Das ist mitbestimmungspflichtig (§ 87 BetrVG) — der Betriebsrat gehört deshalb früh an den Tisch, nicht nach der Auswahl.

Löschfristen nach Ihrer Vorgabe

Wie lange Chatverläufe und Dateien bleiben, stellt eine administrative Person selbst ein — pro Bereich, nicht pauschal. Ohne einstellbare Frist gibt es keine Datenminimierung, nur ein Archiv.

GRENZEN

Was wir nicht behaupten

Kein Medizinprodukt, keine Rechtsberatung

Die Plattform erzeugt Entwürfe. Fachliche Prüfung, Freigabe und Verantwortung für das Ergebnis bleiben bei der Person, die es verwendet — bei Diagnosen, Bescheiden und Verträgen ohne Ausnahme.

Kein Betrieb im eigenen Rechenzentrum

Wir betreiben die Plattform als Dienst auf der Open Telekom Cloud. Wer On-Premises braucht, braucht ein anderes Modell — sagen Sie es im Gespräch, dann ordnen wir ehrlich ein.

UNTERLAGEN

Alles für die Freigabe

Die Dokumente, die eine Datenschutz- oder Einkaufsprüfung anfordert.

Auftragsverarbeitung (AVV)

Der Vertrag nach Art. 28 DSGVO, samt technischen und organisatorischen Maßnahmen (Anhang III) und der vollständigen Liste der Unterauftragsverarbeiter (Anhang IV).

www.deutschlandgpt.de/auftragsverarbeitung

Nutzungsbedingungen

Allgemeine Bedingungen (Teil A) und die Besonderen Bedingungen für Berufsgeheimnisträger nach § 203 StGB (Teil B) mit Anlage 1 und 2.

www.deutschlandgpt.de/agb

Datenschutzerklärung

Verarbeitungszwecke, Rechtsgrundlagen, Empfänger und die Rechte der betroffenen Personen.

www.deutschlandgpt.de/datenschutz

Responsible Disclosure

Meldewege für Sicherheitslücken, der Geltungsbereich und die Safe-Harbor-Zusicherung für Meldungen in gutem Glauben.

www.deutschlandgpt.de/responsible-disclosure

Ergänzungsvereinbarung DORA

Nachtrag nach Art. 30 der Verordnung (EU) 2022/2554 für Kunden aus dem Finanzsektor, einbezogen über Ziff. 1.4 der Nutzungsbedingungen — inklusive der Angaben für Ihr Informationsregister (EUID, Registerdaten, Verarbeitungsorte).

www.deutschlandgpt.de/downloads/dora-nachtrag.pdf

Verpflichtungsnachweis § 203 StGB

Für jeden im Berufsgeheimnisträger-Modus eingesetzten Unterauftragnehmer die Form der Verpflichtung und den Beleg dazu.

www.deutschlandgpt.de/downloads/nachweis-203-unterauftragnehmer-2026-09-03.pdf