

Ihre Daten bleiben in der EU

So schützt KleserIT Kundendaten: Speicherorte, KI-Werkzeuge, Verträge und Maßnahmen im Überblick

Kurz gesagt: Server und Sicherungen stehen in Deutschland, jede KI-Verarbeitung mit Kundendaten läuft in EU-Rechenzentren, und jeder Dienstleister ist über einen Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO gebunden.

- ✓ **Speicherort Deutschland:** Websites und Dienste laufen in einem Rechenzentrum in Deutschland, Sicherungen ebenfalls und verschlüsselt.
- ✓ **KI-Auslesung nur in der EU:** KInvoice liest Rechnungen mit Google Gemini ausschließlich in EU-Rechenzentren aus, ohne Zwischenspeicher und ohne Training mit Ihren Daten.
- ✓ **Keine Kopien in der Cloud:** Angebote, Rechnungen, Verträge und Kundenunterlagen liegen nicht bei Google Drive, Dropbox oder ähnlichen Diensten.
- ✓ **KI mit Kundendaten nur in der EU:** Für Aufträge mit personenbezogenen Daten nutze ich einen Geschäftszugang in EU-Rechenzentren (AWS Bedrock), ebenfalls ohne Training.
- ✓ **So wenig wie möglich:** Ich verarbeite nur, was der Auftrag braucht, und lösche nach festen Fristen.

Wo Kundendaten liegen

Daten	Ort	Schutz
Websites, Bewertungen, KInvoice-Kontingente	Server von Hostinger, Rechenzentrum in Deutschland	TLS, jeder Dienst einzeln abgeschottet, Zugangsdaten nur auf dem Server
Sicherung des Servers	Hetzner Storage Box, Falkenstein (Deutschland)	vor der Übertragung mit AES-256 verschlüsselt, Hetzner kann nicht mitlesen, höchstens 3 Monate
Angebote, Rechnungen, Verträge, Kundenkartei	Arbeitsrechner	Festplatte verschlüsselt (FileVault), Sicherung AES-256-verschlüsselt bei Hetzner, keine Cloud-Kopie
E-Mail	Hostinger Business-E-Mail	Transport per TLS

Rechnungen und Geschäftsbriefe bewahre ich nach § 147 AO und § 257 HGB zehn bzw. sechs Jahre auf.

KI-Werkzeuge und Kundendaten

Welche Daten eine KI sehen darf, hängt davon ab, über welchen Zugang sie läuft. Dafür gibt es drei getrennte Wege:

KUNDENDATEN IN AUFTRÄGEN

Geschäftszugang AWS Bedrock

WOFÜR

personenbezogene Daten in Aufträgen

VERARBEITUNG

nur EU-Rechenzentren: Frankfurt, Stockholm, Mailand, Spanien, Irland, Paris

VERTRAG

AWS GDPR DPA, kein Training

RECHNUNGSDATEN (KINVOICE)

Google Gemini in Vertex AI, Standort EU

WOFÜR

Auslesen von Rechnungen

VERARBEITUNG

nur Rechenzentren in EU-Mitgliedstaaten, Zwischenspeicher abgeschaltet

VERTRAG

Cloud Data Processing Addendum, kein Training

KEINE KUNDENDATEN

Reguläre KI-Abos

WOFÜR

Programmcode, Texte und Marketing ohne Personenbezug

VERARBEITUNG

beim Anbieter

VERTRAG

Verbrauchertarif, deshalb keine Kundendaten

Beide Geschäftszugänge sind fest auf EU-Standorte eingestellt. Der Bedrock-Zugang sendet zudem keine Nutzungsdaten an Dritte und startet ohne gültigen Geschäftszugang gar nicht, statt auf ein privates Konto auszuweichen.

Meine Dienste im Einzelnen

Website-Betrieb für Kunden. Die Seiten laufen auf dem Server in Deutschland, ohne Cookies, Tracking oder Inhalte externer Anbieter. Zugriffsprotokolle enthalten keine vollständigen IP-Adressen und werden nach 14 Tagen gelöscht. Mit jedem Kunden schließe ich einen AVV; KI-Werkzeuge lesen keine Zugriffsprotokolle von Kundenseiten.

KInvoice (E-Rechnungs-Service). Rechnungen werden nur im Arbeitsspeicher verarbeitet und nie auf einem Datenträger gespeichert. Die KI-Auslesung läuft über Google Gemini am EU-Standort von Vertex AI: Google sagt dort die Verarbeitung ausschließlich in EU-Mitgliedstaaten zu, den Zwischenspeicher habe ich abgeschaltet, ein Training findet nicht statt. Nach dem Versand der Antwort wird die Mail gelöscht, bei Fehlern spätestens nach 30 Tagen. In der Datenbank stehen nur E-Mail-Adresse, Tarif und Zähler.

Bewertungen und Referenzen. Grundlage ist Ihre Einwilligung, jederzeit widerrufbar. Die IP-Adresse wird nur als Prüfsumme höchstens eine Stunde im Arbeitsspeicher gehalten. Fotos werden ohne Metadaten neu gespeichert; nicht freigegebene Bewertungen lösche ich nach 90 Tagen.

Dienstleister und Verträge

Dienstleister	Aufgabe	Ort der Verarbeitung	Vertrag
Hostinger International Ltd.	Server, E-Mail	Deutschland	AVV
Hetzner Online GmbH	verschlüsselte Datensicherung	Deutschland	AVV
Amazon Web Services EMEA SARL	KI über Bedrock für Aufträge mit Kundendaten	nur EU-Rechenzentren	AWS GDPR DPA
Google Ireland Limited	Gemini in Vertex AI für KInvoice	nur EU-Rechenzentren (Vertex AI, Standort EU)	Cloud Data Processing Addendum, Zwischenspeicher abgeschaltet
Stripe Payments Europe, Ltd.	Online-Zahlungen	Irland	Vereinbarung zur Datenverarbeitung von Stripe
PNL Fintech B.V. (Finom)	Geschäftskonto, Überweisungen	Niederlande	Bank, eigene Verantwortung
GitHub	Quellcode in privaten Repositories	USA	keine Kundendaten
UptimeRobot	prüft, ob öffentliche Seiten erreichbar sind	Anbieter in Tschechien	keine Personendaten

Technische und organisatorische Maßnahmen

Die Maßnahmen nach Art. 32 DSGVO sind eingerichtet und werden geprüft, zuletzt am 27.10.2026.

- **Verschlüsselung:** TLS für alle Seiten und Mails, Festplatte des Arbeitsrechners mit FileVault, Sicherungen mit AES-256 vor der Übertragung.
- **Abschottung:** Jeder Dienst läuft mit eigenen, minimalen Rechten; fremde Word-Dateien werden in einem Wegwerf-Prozess ohne Netz und ohne Zugangsdaten umgewandelt.
- **Schutz vor Angriffen:** strenge Sicherheits-Header (CSP, HSTS), Prüfung eingehender Anhänge auf Schadcode, Mengenbegrenzungen gegen Missbrauch.
- **Zugangsdaten:** nur auf dem Server bzw. im Schlüsselbund, nie im Quellcode; der Code wird regelmäßig auf versehentlich enthaltene Schlüssel geprüft.
- **Zugriff:** AWS-Hauptkonto mit Zwei-Faktor-Anmeldung, für die KI ein eigener Benutzer, der nur Modelle aufrufen darf, mit Kostenwarnung.
- **Verfügbarkeit:** tägliche Sicherung mit Fehleralarm, wöchentliche Prüfung der Sicherung, Wiederherstellung am 27.10.2026 erfolgreich getestet, externe Überwachung der Erreichbarkeit.
- **Löschung:** feste Fristen je Datenart, Sicherungen werden nach höchstens drei Monaten überschrieben.

Wenn Sie EU-Datenschutz mit AVV verlangen

- 1 Wir schließen einen AVV nach Art. 28 DSGVO mit Anlagen zu Maßnahmen und Unterauftragsverarbeitern.
- 2 Wir legen fest, welche Ihrer Daten eine KI überhaupt sehen darf, zum Beispiel keine Zugriffsprotokolle Ihrer Website.
- 3 Personenbezogene Daten verarbeite ich mit KI ausschließlich über den Geschäftszugang bei AWS Bedrock in EU-Rechenzentren.
- 4 Ich trage AWS als Unterauftragsverarbeiter in Ihren AVV und in meine Datenschutzerklärung ein.
- 5 Nach Auftragsende gebe ich Ihre Daten zurück oder lösche sie, soweit keine Aufbewahrungspflicht besteht.

Offen benannt

Diese Punkte nenne ich ausdrücklich, damit Sie sie selbst bewerten können:

- **US-Konzerne als Dienstleister:** Google und AWS gehören zu US-Konzernen. Beide verarbeiten Ihre Daten bei mir ausschließlich in EU-Rechenzentren; für den Ausnahmefall eines Zugriffs aus Drittländern, etwa durch den Support, gelten das EU-US Data Privacy Framework und EU-Standardvertragsklauseln.
- **Missbrauchserkennung:** Google darf Anfragen ausschließlich zur Erkennung von Missbrauch protokollieren; ein Training mit den Daten findet nicht statt.
- **Programmcode und Texte ohne Personenbezug** entwickle ich auch mit regulären KI-Abos. Personenbezogene Kundendaten gelangen dort nicht hinein.

Fragen, Auskunft oder Löschung: **kontakt@kieserit.io** · Datenschutzerklärung: **kieserit.io/datenschutz**
Fabian Kieser

KleserIT · Eduard-Vogel-Straße 76 · 64839 Münster (Hessen)