CloudPal

CloudPal Whitepaper
Datenschutz und Sicherheit

Die sichere und effiziente Nutzung
von KI-Modellen für den Unternehmensalltag

1. Einleitung

CloudPal ist eine vertrauensvolle Plattform, die mittelständischen Unternehmen einen sicheren und DSGVO-konformen Zugang zu leistungsstarken KI-Sprachmodellen wie ChatGPT, Claude und Gemini ermöglicht. Die Plattform unterstützt Mitarbeitende bei alltäglichen Arbeitsprozessen wie Textgenerierung, -verarbeitung, -analyse, -zusammenfassung, Informationssuche und Prozessoptimierung. Zusätzlich können organisationsspezifische Assistenten für eine effiziente Aufgabenabwicklung erstellt werden.

Wir gewährleisten eine konsequente Datenhaltung in europäischen Rechenzentren und implementieren umfassende technische sowie organisatorische Schutzmaßnahmen. Durch die kontinuierliche Überwachung eines externen Datenschutzbeauftragten wird der vollumfängliche Schutz der Rechte und Freiheiten der Betroffenen sichergestellt.

Wir verstehen uns als ganzheitlicher Vertrauenspartner für Unternehmen, die KI verantwortungsvoll einsetzen möchten, und bieten mit diesem Whitepaper einen Überblick über Datenverarbeitung, DSGVO-Compliance, beteiligte Subdienstleister und die implementierten Datenschutzmaßnahmen.

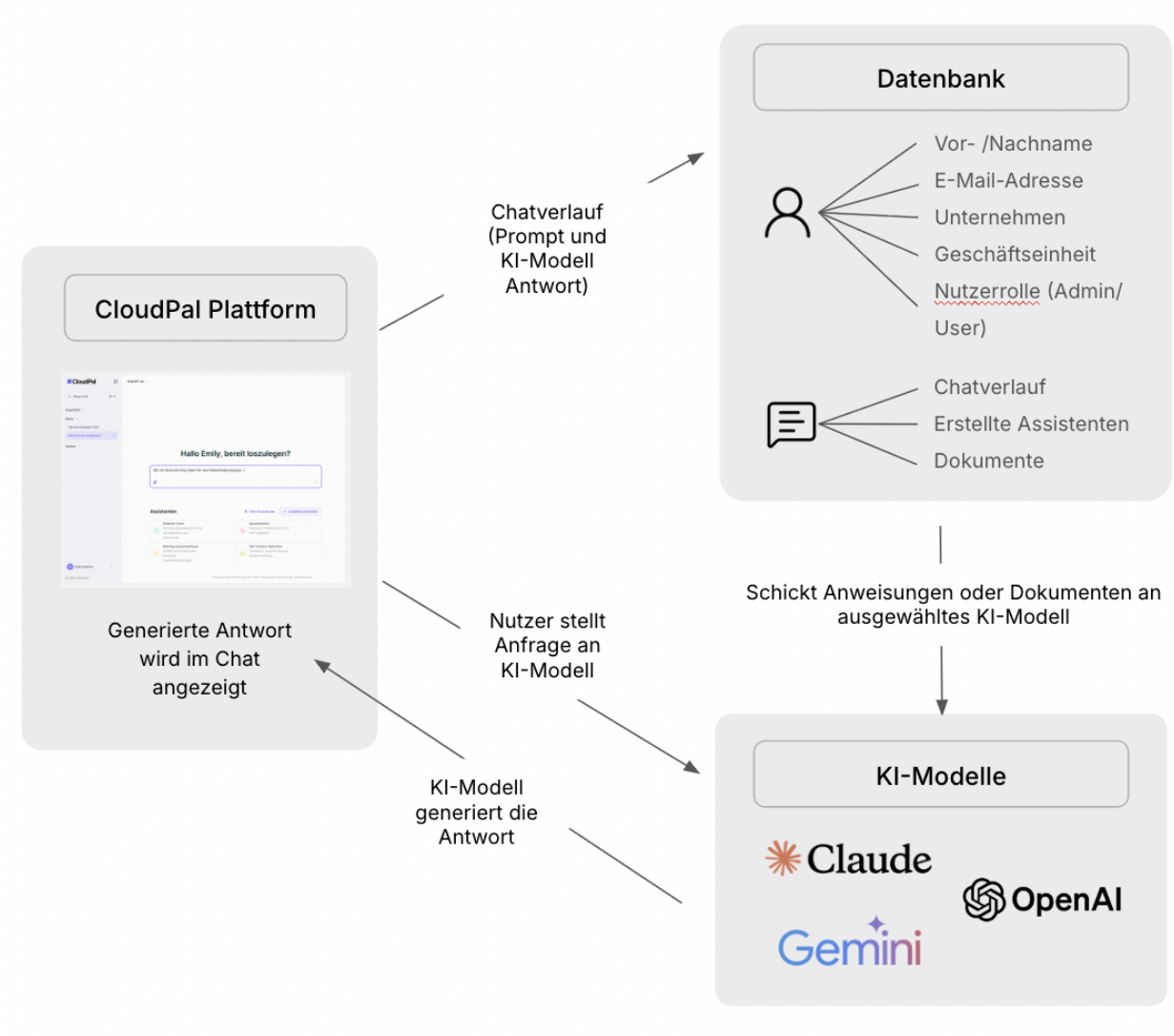
2. Welche Daten verarbeitet werden und warum

CloudPal verarbeitet personenbezogene Daten ausschließlich im erforderlichen Umfang für den ordnungsgemäßen Betrieb der Plattform und für die Bereitstellung der KI-Funktionen.

Unser Grundsatz: Wir verwenden Ihre Daten niemals für eigene Analysezwecke, zur Softwareoptimierung oder zu Trainingszwecken, Ihre Informationen bleiben ausschließlich Ihrem bestimmungsgemäßen Gebrauch vorbehalten.

- **Stammdaten:** Vor- und Nachname, geschäftliche E-Mail Adresse, Unternehmen, Geschäftseinheit → für die Benutzerverwaltung und Authentifizierung.
- **Nutzungsdaten:** IP-Adresse, Zeitstempel, Tokenverbrauch, HTTP-Status → für Sicherheit, Abrechnung und Betrieb.
- **Inhaltsdaten:** Texteingaben (Prompts), Chatverläufe, hochgeladene Dokumente → können von Nutzer*innen selbst gelöscht werden.
- **Assistenten-Daten:** Inhalte und Einstellungen selbst erstellter Assistenten → Speicherung zur Wiederverwendung.

Übersicht des Datenflusses bei CloudPal



3. DSGVO-Konformität

CloudPal wurde konsequent nach den Prinzipien von Privacy by Design & Default entwickelt und gewährleistet vollumfängliche DSGVO-Compliance.

Rechtliche Grundlagen

Die Datenverarbeitung erfolgt auf Basis von:

- Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung)
- Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse)

Datenschutzprinzipien

- Datenminimierung: Ausschließliche Speicherung der für den Betrieb unbedingt erforderlichen Daten.
- Transparenz: Umfassende Information der Nutzer*innen über sämtliche Datenverarbeitungsprozesse bereits bei der Registrierung sowie kontinuierlich innerhalb der Anwendung.
- Vollständige Umsetzung aller Betroffenenrechte:
    - Auskunftsrecht (Art. 15 DSGVO)
    - Recht auf Berichtigung (Art. 16 DSGVO)
    - Recht auf Löschung (Art. 17 DSGVO)
    - Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
    - Widerspruchsrecht (Art. 21 DSGVO)

Datenschutzbeauftragte/r

CloudPal wird durch eine/n externe/n Datenschutzbeauftragte/n kontinuierlich begleitet und auditiert.

Kontakt: dsb@freshcompliance.de, Nilufar Shahla, Fresh Compliance GmbH, Schönhauser Allee 43a, 10435 Berlin

4. Subdienstleister

Die Datenverarbeitung erfolgt ausschließlich in der EU-Region bei folgenden Anbietern:

Anbieter	Dienst / Zweck	Region
Amazon Web Services (AWS)	Hosting Backend, Datenbank (Aurora), Dateispeicherung (S3), Logs (CloudWatch), Container-Infrastruktur	Frankfurt (eu-central-1)
Microsoft Azure OpenAI	Bereitstellung von GPT-4-Inferenz via API	Europa (Germany West Central / EU)

Amazon Bedrock (Claude)	Bereitstellung von Claude-Inferenz via API	Frankfurt (eu-central-1)
Google Cloud (Gemini)	Bereitstellung von Gemini-Inferenz via API	Europa (EU)

Mit allen Subdienstleistern bestehen Auftragsverarbeitungsverträge (AVV) inkl. Standardvertragsklauseln (SCCs).

5. Speicherung, Sicherheit & Löschung

Speicherung

- Stammdaten, Chat-Verläufe (Prompts inkl. KI-Antwort) und Assistenten werden nach neuesten Sicherheitsstandards in der AWS-Infrastruktur Frankfurt (Aurora, S3) gespeichert.
- System-Logs und Protokolle werden über AWS CloudWatch Frankfurt verwaltet.

Sicherheitsmaßnahmen (TOMs)

Wir setzen folgende technische und organisatorische Sicherheitsmaßnahmen ein:

Verschlüsselung & Datenübertragung

- Sichere Übertragung: Alle Daten werden mit TLS 1.2+ verschlüsselt übertragen
- Höchster Schutzstandard für die Kommunikation zwischen Ihrem Browser und unseren Servern

Zugriffskontrolle & Datentrennung

- Rollenbasierte Zugänge: Klare Berechtigungsstufen (SuperAdmin, Admin, Nutzer)
- Strikte Kundentrennung: Multi-Tenant-Architektur mit vollständiger logischer Isolation der Kundendaten
- Umgebungstrennung: Komplette Separierung von Entwicklungs- und Produktivsystemen

Überwachung & Kontrolle

- Vollständige Nachverfolgung: Lückenlose Protokollierung aller Systemzugriffe
- Automatische Sicherheit: Regelmäßige Credential-Rotation und kontinuierliche Systemüberwachung
- Professionelle Audits: Regelmäßige Security-Überprüfungen durch interne Teams

Datensicherung & Verfügbarkeit

- Tägliche EU-Backups: Automatisierte Sicherungen ausschließlich innerhalb der Europäischen Union

Löschkonzept

- Manuelle Löschung: Nutzer können jederzeit ihre hochgeladenen Dokumente, Assistenten und Chat-Verläufe eigenständig löschen.
- Automatische Löschung: Administratoren können festlegen, dass Chat-Verläufe aller Benutzer automatisch nach 7, 30, 90 oder 365 Tagen gelöscht werden.
- Vertragsende: Bei Beendigung unseres Vertrags werden alle Daten gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

6. Drittlandübermittlungen

CloudPal verarbeitet alle Daten ausschließlich in europäischen Rechenzentren und führt grundsätzlich keine absichtlichen Übermittlungen personenbezogener Daten in Drittländer durch. In seltenen Einzelfällen kann jedoch ein technischer Zugriff durch Administratoren aus Drittländern wie den USA erforderlich werden, beispielsweise wenn AWS- oder Microsoft-Experten Supportleistungen erbringen müssen.

Alle Drittanbieter unterliegen strikten Auftragsverarbeitungsverträgen und den europäischen Standardvertragsklauseln, die internationale Datenübermittlungen umfassend regulieren. Darüber hinaus ist bei allen verwendeten KI-Modellen die "No Training"-Option aktiviert, wodurch sichergestellt wird, dass Kundendaten niemals in das Training oder die Weiterentwicklung der Modelle einfließen.

7. Fazit

CloudPal bietet Unternehmen die Möglichkeit, leistungsstarke KI-Modelle sicher und DSGVO-konform zu nutzen. Als vertrauensvolle Plattform verbinden wir innovative

KI-Modelle mit höchsten europäischen Datenschutzstandards und schaffen so eine sichere Umgebung für den professionellen Einsatz künstlicher Intelligenz.

Unser ganzheitlicher Ansatz basiert auf der konsequenten Datenhaltung in europäischen Rechenzentren, umfassenden technischen und organisatorischen Schutzmaßnahmen sowie der kontinuierlichen Überwachung durch unseren externen Datenschutzbeauftragten.

Durch die Kombination aus konsequenter, europäischer Datenhaltung, umfassenden technischen und organisatorischen Schutzmaßnahmen sowie der kontinuierlichen Überwachung durch unseren externen Datenschutzbeauftragten gewährleisten wir, dass die Rechte und Freiheiten der Betroffenen umfassend geschützt sind.

CloudPal versteht sich nicht nur als Produktivitätsplattform, sondern auch als Vertrauenspartner für Unternehmen, die KI verantwortungsvoll einsetzen möchten.

8. Fragen & Kontakt

Bei Fragen zum Datenschutz steht Ihnen unsere Datenschutzbeauftragte Nilufar Shahla gerne zur Verfügung:

dsb@freshcompliance.de, Fresh Compliance GmbH, Schönhauser Allee 43a, 10435 Berlin

Datenschutz-Whitepaper
CloudPal Plattform - Vertrauen durch Datenschutz
Stand: 04.09.2025
Verantwortlich: Pico Ventures GmbH, Novalisstr. 12, 10115 Berlin - info@cloudpal.ai