LAND KÄRNTEN

KI & PRÜFHANDLUNGEN

KI-gestützte Prüfhandlungen

Von KärntenGPT zum kontrollierten hybriden Prüfmodell

Lokale Datensouveränität bleibt die Basis. Externe Modellleistung kommt nur nach Anonymisierung hinzu.

Mag. Christian Inzko · CIO / CDO
Amt der Kärntner Landesregierung · 5. Oktober 2026

IN DREI STUFEN

1 **KärntenGPT**
Sensible Originaldaten bleiben im Land.

2 **Anonymisierung**
Nur freigegebene, hinreichend anonymisierte Prüfdaten verlassen die Schutzzone.

3 **Externe Modelle**
Komplexes Reasoning dort nutzen, wo lokale Modelle nicht genügen.

Human-in-the-loop
Die Verantwortung bleibt beim Prüfer.

Warum Kärnten eine eigene KI-Plattform aufgebaut hat

KI nutzen, ohne die Kontrolle über sensible Verwaltungsdaten abzugeben.

01

Sicherheit & Datenschutz

Personal-, Förder-, Gesundheits- oder Verfahrensdaten sollen unsere Infrastruktur nicht ungeprüft verlassen.

02

Datensouveränität

Modelle, Datenhaltung, Protokollierung und Zugriffe bleiben unter Kontrolle des Landes.

03

Verwaltungswissen

Antworten sollen auf unseren Regelwerken, Dokumenten und Fachprozessen beruhen – nicht nur auf allgemeinem Internetwissen.

04

Gestaltbarkeit

Use Cases und Agenten können an Kärntner Prozesse angepasst und wiederverwendet werden.

UNSERE STRATEGISCHE ENTSCHEIDUNG

Sensible Originaldaten zuerst lokal verarbeiten. Cloudlösungen nur dort einsetzen, wo sie einen klaren fachlichen Mehrwert bringen – und nur unter definierten Schutzbedingungen.

LOCAL FIRST

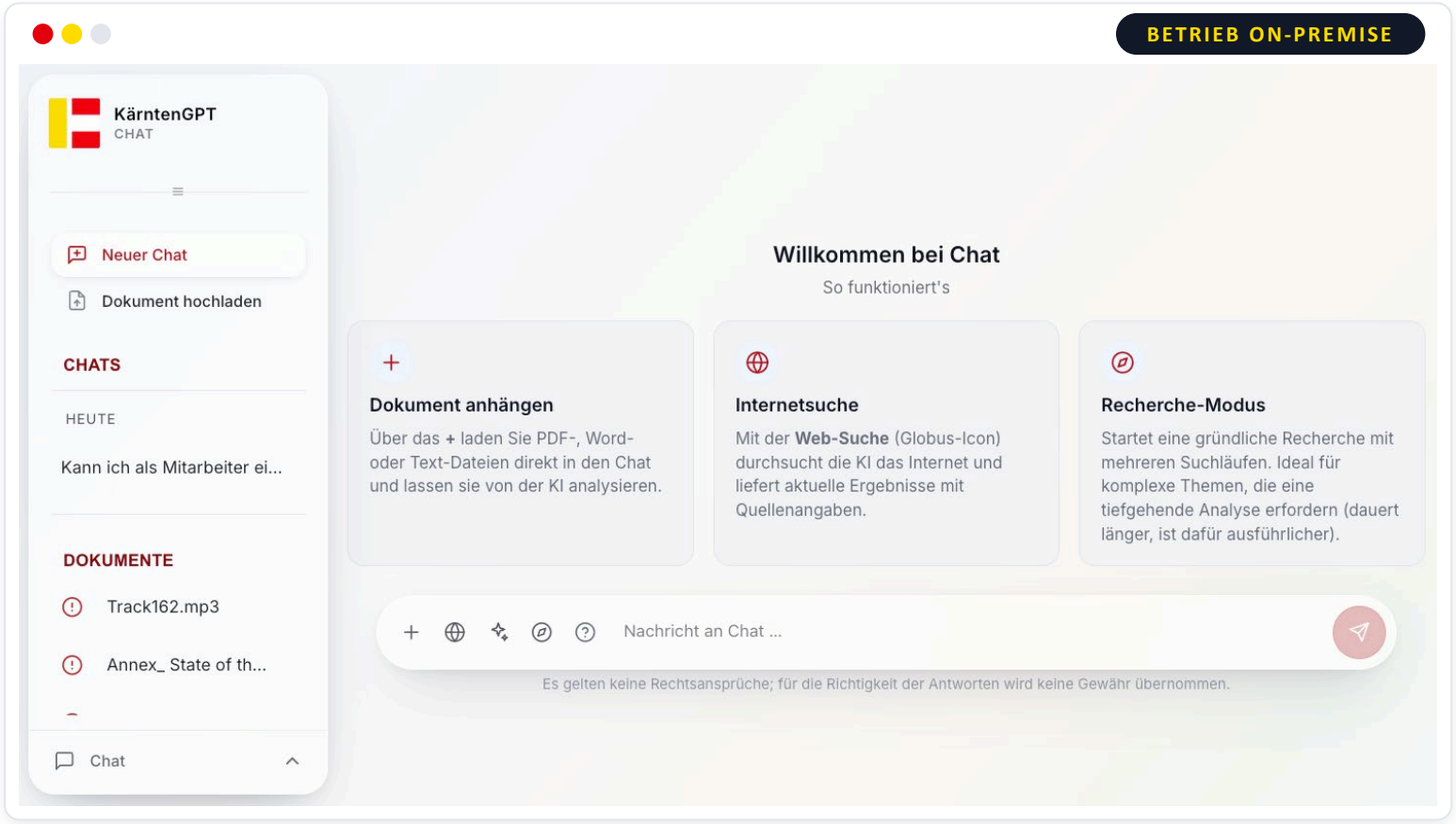
DATENSOUVERÄN

USE-CASE-GETRIEBEN

MENSCH ENTSCHEIDET

Unser interner Assistent – Bedienung wie ChatGPT, Betrieb On-Premise

Für Mitarbeiter:innen entsteht ein vertrauter Zugang zu generativer KI, ohne sensible Inhalte ins öffentliche Internet zu übertragen.



01

Ein gemeinsamer Einstieg

Chat, Dokumente und Fachwissen über eine einheitliche Oberfläche.

02

Daten bleiben intern

Die Verarbeitung sensibler Inhalte erfolgt innerhalb unserer Schutzzone.

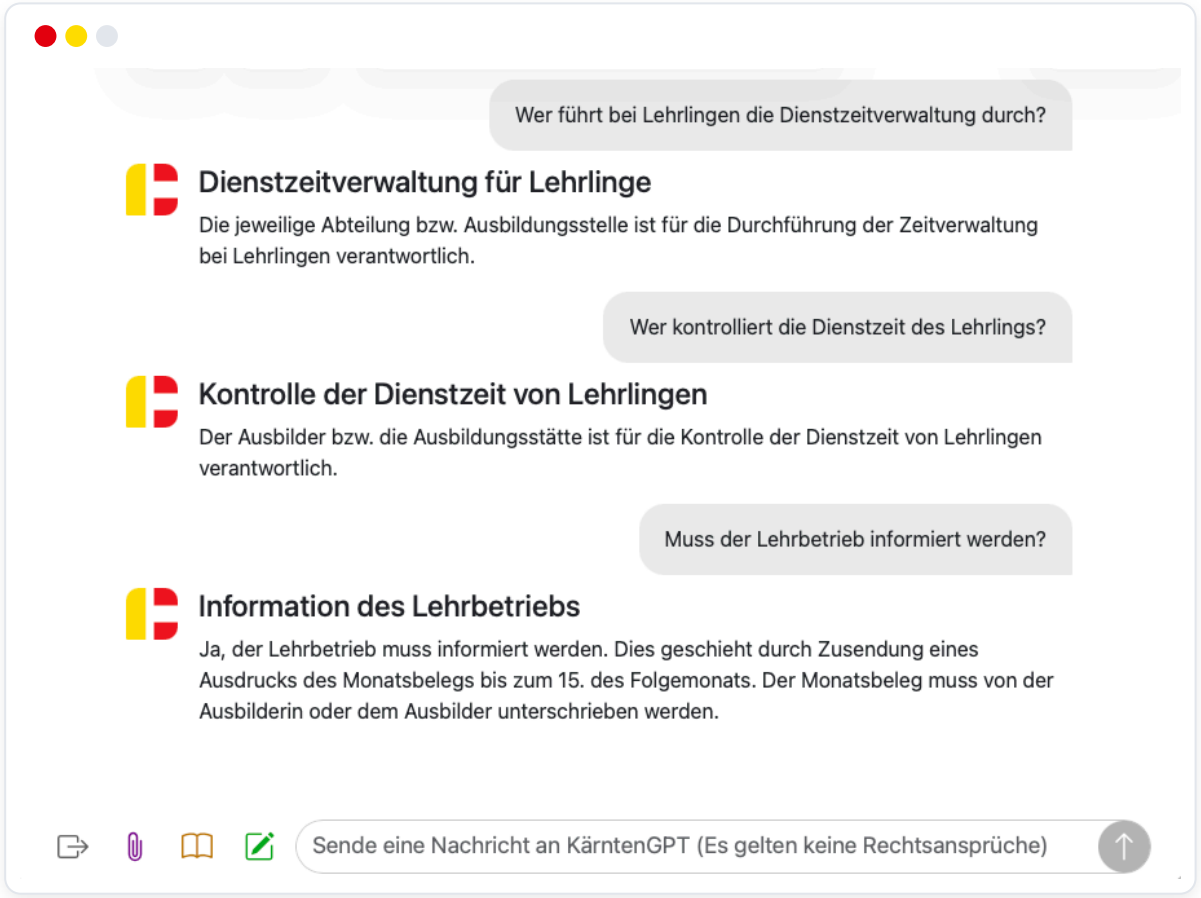
03

Plattform statt Einzeltool

Auf derselben Basis entstehen Assistenten, Dokumentverarbeitung und Agenten.

Allgemeine KI wird erst durch internes Wissen verwaltungstauglich

Regelwerke, Leitfäden und Fachdokumente werden kontrolliert eingebunden – ohne sie ins öffentliche Internet zu übertragen.



1

Fachquelle auswählen

Nur freigegebene interne Dokumente und Regelwerke werden in den Wissensraum übernommen.

2

Kontext gezielt liefern

KärntenGPT zieht zur Frage passende Textstellen heran und stellt sie dem Modell als Kontext bereit.

3

Antwort nachvollziehbar machen

Die Antwort basiert auf dem internen Wissensbestand – nicht auf unkontrollierter Recherche.

BEISPIEL

Personalfragen zu Dienstzeitregelungen

Das Modell beantwortet konkrete Fragen auf Basis hinterlegter Regelwerke und bleibt innerhalb der internen Plattform.

Beispiel: FAQ-Editor für Mitarbeiter

Mitarbeiter können fachspezifisches Wissen selbst mittels Fragen und Antworten in die lokale KI einbringen.

SO ENTSTEHT EIN EINTRAG

Frage & Antwort erfassen

Beide Felder sind Pflicht.

Einordnen

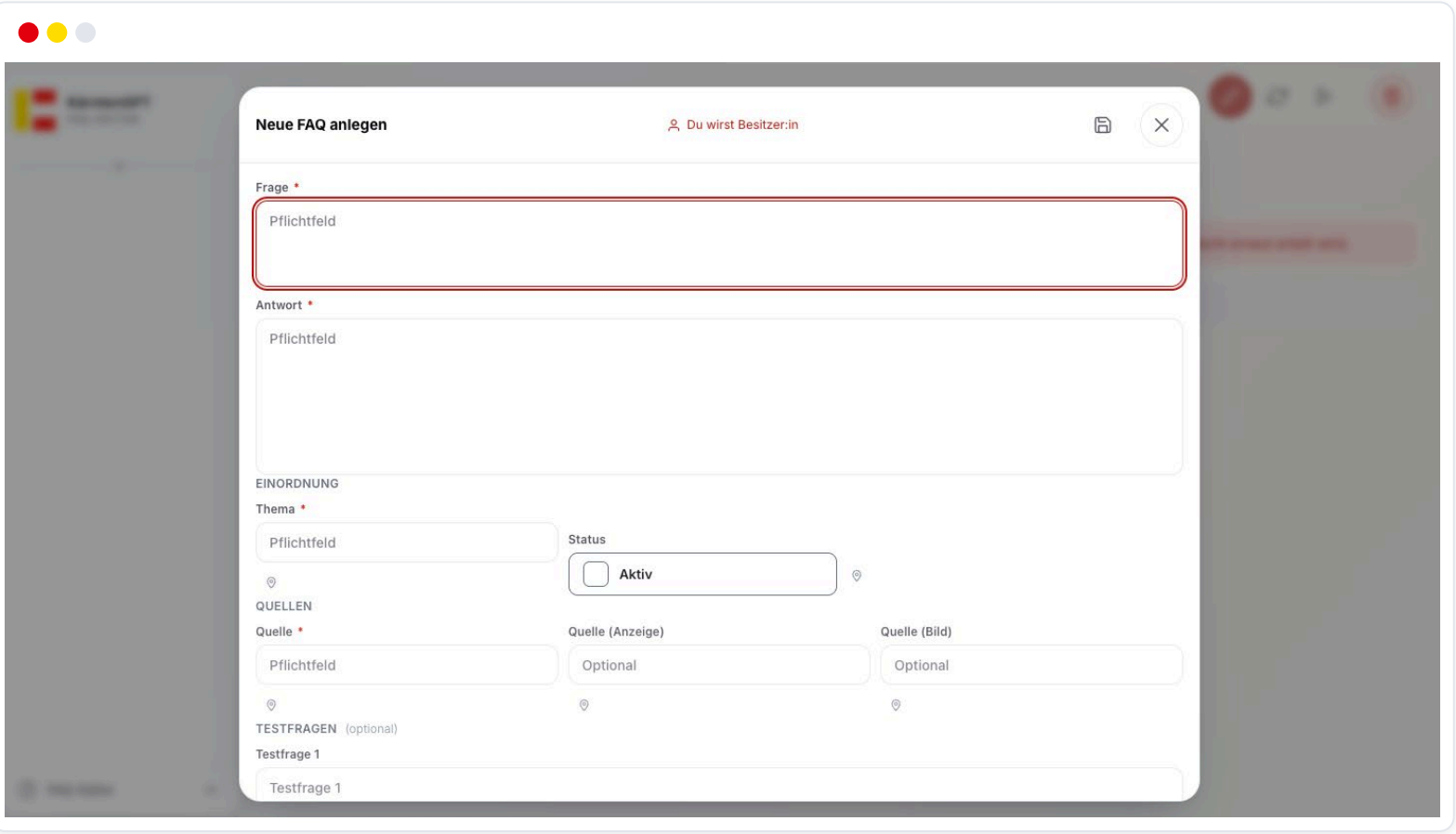
Thema und Status festlegen.

Quelle angeben

Pflichtangabe – Anzeige und Bild optional.

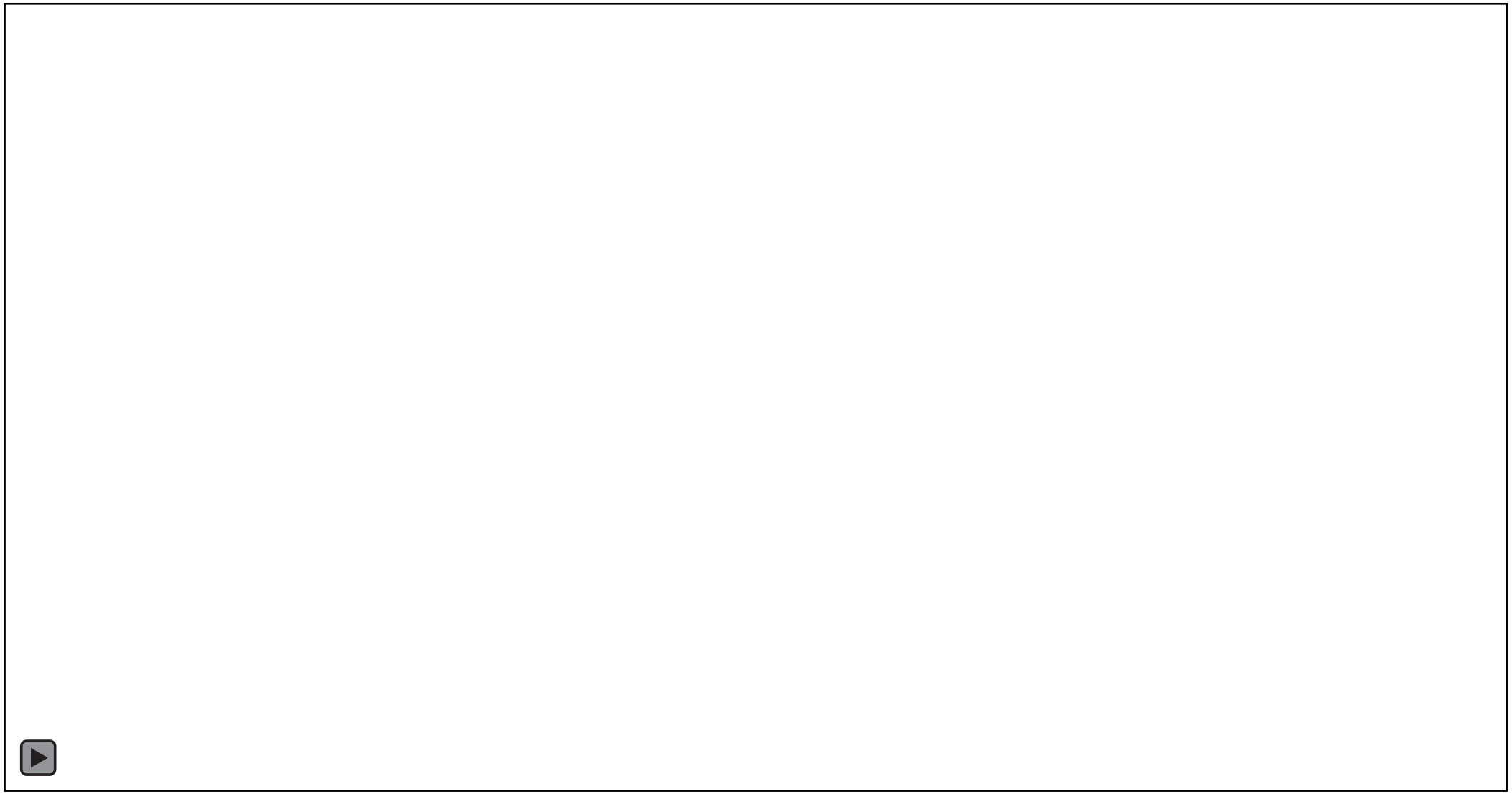
Testfragen

Optional ergänzbar.



KärntenGPT – Fragen nach individuellem Wissen

Bedienung wie bei ChatGPT und Co. mit Ausgabe von individuellem Wissen



Was wir mit lokalen Modellen gelernt haben

KärntenGPT ist die richtige Basis – aber „lokal“ ist kein Selbstzweck und keine Garantie für maximale Modellleistung.

Stärken lokaler Modelle

- **Datenschutz**
  Originaldaten können intern verarbeitet werden.
- **Fachwissen**
  RAG und interne Quellen sind kontrollierbar.
- **Integration**
  Direkte Anbindung an interne Prozesse und Systeme.
- **Kostenkontrolle**
  Keine nutzungsabhängige Cloud-Logik für jeden Standardfall.

vs.

Grenzen bei anspruchsvollen Aufgaben

- **Komplexes Reasoning**
  Mehrstufige Prüfketten sind für kleine lokale Modelle schwieriger.
- **Langer Kontext**
  Viele Verträge, Belege und Zeitreihen gleichzeitig belasten Kontext und Qualität.
- **Multimodalität**
  Tabellen, Scans und heterogene Dokumente erfordern starke Modelle.
- **Stabilität strukturierter Outputs**
  Für Prüfprozesse sind robuste, konsistente Ergebnisse besonders wichtig.

KONSEQUENZ **KärntenGPT bleibt die sichere Schaltstelle – externe Modelle ergänzen gezielt.**

Was KärntenGPT gekostet hat

2023 extern gestartet – danach Know-how und Weiterentwicklung bewusst ins Land geholt.

GESAMTINVESTITION in 3 Jahren

ca. € 140.000

Entwicklung + Hardware – ohne laufende interne Personalkosten



€ 50.000
Erstentwicklung extern (2023)

€ 90.000
On-Premise KI-Cluster (Hardware)

ON-PREMISE KI-CLUSTER 4 Server · 4 NVIDIA-GPUs · 2 Mac Pro

Hardware **ca. € 90.000**

HP GPU Server 1
2× NVIDIA GPU · 48 GB

HP GPU Server 2
2× NVIDIA GPU · 96 GB

KärntenGPT
Cluster Runtime

Mac Pro Server 1
198 GB Gesamtspeicher

Mac Pro Server 2
198 GB Gesamtspeicher

Alle vier Systeme arbeiten als gemeinsamer Compute-Cluster. Workloads können zwischen GPU-Servern und Mac-Pro-Knoten verteilt werden.

2023 · Extern gestartet
Grundaufbau von KärntenGPT durch eine externe Firma.

Danach · Know-how ins Land
Übernahme durch eigene, neu aufgenommene Mitarbeiter.

Heute · Eigenbetrieb
Betrieb, Integration und Weiterentwicklung erfolgen intern.

STRATEGIE

Initial extern beschleunigen – Know-how, Betrieb und Infrastruktur dauerhaft selbst beherrschen.

Warum Use-Cases des Rechnungshofs besonders anspruchsvoll sind

Die KI muss nicht nur lesen – sie muss Informationen über mehrere Quellen hinweg in Beziehung setzen.

01

Viele Quellen

Vertrag, Bestellung, Rechnung, Leistungsnachweis, Genehmigungen, Korrespondenz und Zeitdaten müssen gemeinsam betrachtet werden.

02

Viele Regeln

Tagessätze, Zuschläge, Obergrenzen, Fristen, Leistungszeiträume und formale Pflichtangaben wirken parallel.

03

Viele Beziehungen

Eine Abweichung wird oft erst sichtbar, wenn mehrere Belege, Perioden oder Personen miteinander verglichen werden.

04

Hohe Nachvollziehbarkeit

Jeder Prüfhinweis muss auf konkrete Daten oder Dokumentstellen zurückführbar sein – keine Black-Box-Entscheidung.

WAS DIE KI LEISTEN SOLL

Dokumente strukturieren

Abweichungen erkennen

Zeitreihen vergleichen

ZIEL

Prüfer:innen verbringen mehr Zeit mit Bewertung – und weniger Zeit mit Suchen, Sortieren und Vergleichen.

Wo KärntenGPT allein an Grenzen stoßen kann

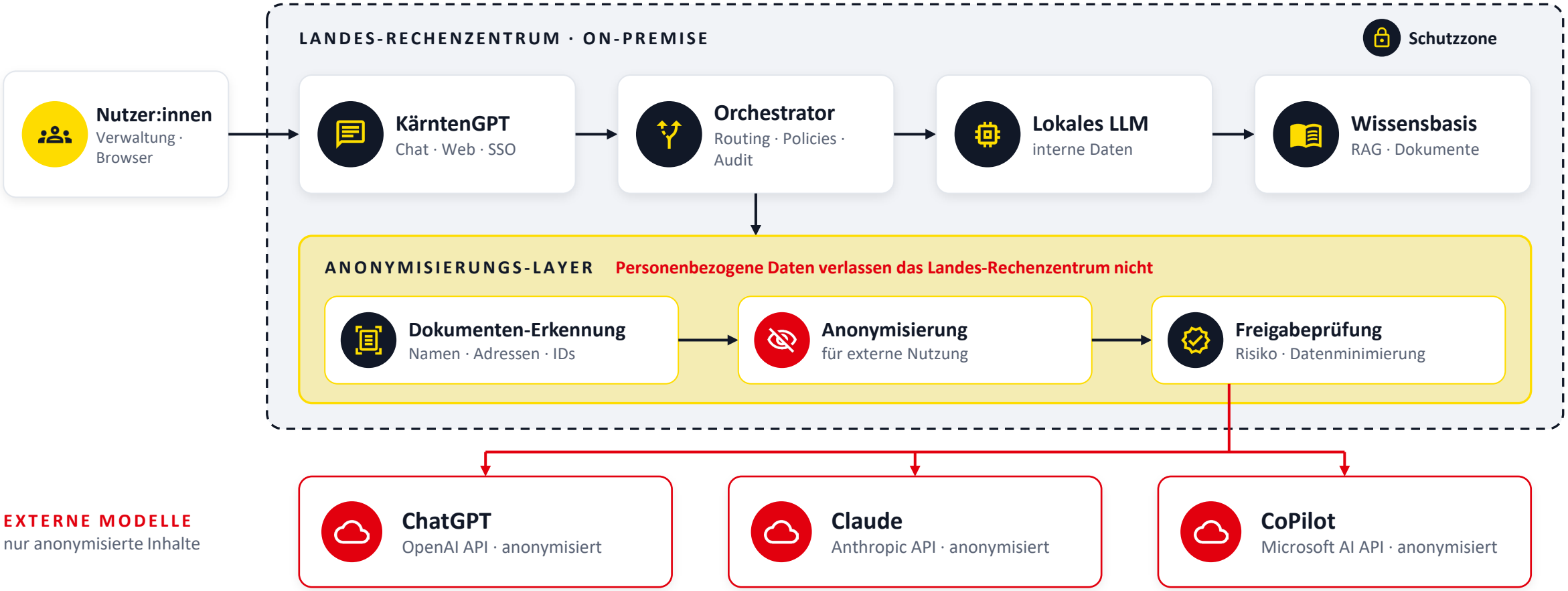
Nicht jeder Prüfteil braucht ein externes Modell. Aber einige Aufgaben profitieren deutlich von größerer Modellleistung.

AUFGABE	KÄRNTENGPT LOKAL	GROSSES EXTERNES MODELL	ROUTING
Dokumentklassifikation & Extraktion	●●● **sehr gut**	●●○ gut	**lokal bevorzugen**
Interne Wissensabfrage / RAG	●●● **sehr gut**	●●○ gut	**lokal bevorzugen**
Mehrere lange Verträge + Rechnungen gleichzeitig	●○○ begrenzt	●●● **sehr gut**	**extern erwägen**
Komplexe fachliche Begründung / Reasoning	●●○ gut	●●● **sehr gut**	**extern erwägen**
Unstrukturierte Tabellen / Scans / Mischformate	●●○ gut	●●● **sehr gut**	**extern erwägen**
Ausreißer- und Musteranalyse mit viel Kontext	●●○ gut	●●● **sehr gut**	**extern erwägen**

SICHERHEIT **KärntenGPT orchestriert die Modellwahl. Das externe Modell erhält niemals direkten Zugriff auf Elektronischen Akt, SAP oder Originalbelege.**

KärntenGPT 3.0 – die sichere KI-Drehscheibe des Landes

Lokale Datensouveränität bleibt die Basis. Externe Spitzenmodelle werden nur kontrolliert und ausschließlich mit anonymisierten Inhalten zugeschaltet.



Anonymisierung ≠ Pseudonymisierung

Beide reduzieren Personenbezug – aber mit unterschiedlichen Folgen für Analyse und Re-Identifizierbarkeit.

Anonymisierung

Personenbezug wird so entfernt, dass eine Re-Identifizierung mit vertretbaren Mitteln nicht mehr möglich ist.

BEISPIEL

„[PERSON] hat 18 Überstunden.“

Die Person ist nicht mehr über mehrere Belege hinweg verknüpfbar.

≠

Pseudonymisierung

Direkte Identifikatoren werden durch ein Pseudonym ersetzt. Die Zuordnung bleibt über separat geschützte Zusatzinformationen möglich.

BEISPIEL

„PERSON_017 hat 18 Überstunden.“

Querbezüge über mehrere Belege bleiben erhalten – ohne den Namen zu übertragen.

FAUSTREGEL

- Identität analytisch irrelevant → **anonymisieren**
- Querbezüge erforderlich → **pseudonymisieren**

Ein Datensatz – drei Datenschutzstufen

Gleicher fachlicher Inhalt, aber unterschiedlicher Personenbezug.

ORIGINAL · INTERN

Name	**Anna Berger**
Pers.-Nr.	**4711**
Abteilung	**IT-Betrieb**
Rechnung	**RE-2026-0831**
Leistung	**31.08. · 1 PT**

→ **maximale Analysefreiheit intern**

ANONYMISIERT

Name	**[ENTFERNT]**
Pers.-Nr.	**[ENTFERNT]**
Abteilung	**IT-Betrieb**
Rechnung	**RE-2026-0831**
Leistung	**31.08. · 1 PT**

→ **geringstes Re-Identifikationsrisiko**

PSEUDONYMISIERT

Name	**PERSON_017**
Pers.-Nr.	**ID_017**
Abteilung	**IT-Betrieb**
Rechnung	**RE-2026-0831**
Leistung	**31.08. · 1 PT**

→ **Bezüge bleiben prüfbar**

KI erkennt auffällige Überstundenmuster in einer Gemeinde

Die KI markiert Auffälligkeiten – der Prüfer klärt Kontext, Genehmigung und sachliche Begründung.

DATENGRUNDLAGE

- 36 Monate Zeitreihe
- Soll- und Ist-Stunden
- Überstunden & Zeitausgleich
- genehmigt / nicht genehmigt
- Abteilung & Beschäftigungsausmaß

vor externer KI pseudonymisiert

LLM
Musteranalyse

AUTOMATISCHE AUSREISSER-ERKENNUNG

HOCH	**MA-017** kontinuierlicher Anstieg		**+186 %**
HOCH	**MA-042** dauerhaft hohes Niveau		**Ø 29 h**
MITTEL	**MA-031** sprunghafter Peak		**47 h**
POSITIV	**MA-056** konsequenter Abbau		**–62 %**

Prüfhinweis – kein automatischer Vorwurf oder Entscheid. Verläufe illustrativ.

Warum wir lokal UND extern brauchen

Routing nach Schutzbedarf, Datenstatus und Analysekomplexität.

ROUTING

KärntenGPT orchestriert die Modellwahl

	EINSATZFALL	MODELL	DATENSTATUS	BETRIEB
A	**Sensible Standardfälle und Verarbeitung mit Originaldaten**	KärntenGPT / internes LLM	Originaldaten & sensible Unterlagen	On-Premise
B	**Zeitreihen, Querbezüge und dokumentübergreifende Muster**	Externes LLM + Pseudonymisierung	Pseudonyme statt direkter Identifikatoren	Cloud / API
C	**Anspruchsvolle Fachanalyse, wenn Identität keine Rolle spielt (Verträge)**	Externes LLM + Anonymisierung	Kein sinnvoller Personenbezug mehr	Cloud / API

PRINZIP **Kontrolliertes Routing: lokal, wo möglich – externe Modellleistung dort, wo sie fachlich Mehrwert bringt.**

Was für einen revisionssicheren KI-Prüfprozess notwendig ist

Technik allein reicht nicht. Entscheidend sind Freigaben, Protokollierung, Quellenbezug und klare Verantwortlichkeiten.

1 DATEN → 2 MODELL → 3 ERGEBNIS

Datenfreigabe

Welche Daten dürfen lokal verarbeitet werden? Welche dürfen – anonymisiert – extern genutzt werden?

Modellrouting

Für jeden Prüfschritt ist festgelegt, welches Modell genutzt werden darf und warum.

Quellenbezug

Jeder relevante KI-Hinweis muss auf Datenpunkte oder Dokumentstellen zurückführen.

Anonymisierungsregeln

Automatisierte Erkennung plus definierte Schwellenwerte und Stichprobenkontrollen.

Prompt- & Versionsmanagement

Prüfregeln, Prompts und Modellversionen müssen dokumentiert und nachvollziehbar sein.

Human-in-the-loop

Keine autonome Zahlungs-, Personal- oder Rechtsentscheidung durch das Modell.

ZIELBILD **KI als nachvollziehbarer Prüfassistent – nicht als autonome Entscheidungsinstanz.**

PRAXIS

Ein Beispiel aus der Praxis

Vom pseudonymisierten Überstundendatensatz zum nachvollziehbaren Prüfbefund

LIVE-DEMO / DETAILANALYSE

ABLAUF

1 **Daten**
pseudonymisiert

2 **Hinweis**
Muster & Ausreißer

3 **Entscheid**
durch Prüfer:in

Ausgangsdatei – Beispiel Lohndaten

ORIGINALDATEN · INTERN

Direkte Identifikatoren wie Name, Geburtsdatum, SV-Nummer und Adresse sind noch enthalten.

PERSNR	NACHN	VORNA	TITEL	GESCH	GBDAT	SVNR	FAMST	ANZKD	STAAN	STRAS
Personalnummer	Nachname	Vorname	Titel	Geschlecht	Geburtsdatum	Sozialvers.-Nr.	Familienstand	Anz. Kinder	Staatsangehörigkeit	Straße
00010001	Schuh	Luca	Dr.	1	23.07.1975	9053230775	02	2	AT	Am Kanal 159/20
00010006	Barbieri	Andrea	Dr.	2	26.06.1983	5036260683	01	0	AT	Mühlweg 103
00010010	Prasser	Katharina	Mag.	2	25.06.1987	7132250687	02	1	AT	Buchenweg 209/21
00010015	Willegger	Markus	Prof.	1	02.05.1965	6564020565	02	2	AT	St. Veiter Straße 27/38
00010019	Grill	Gudrun	Mag.	2	22.04.1992	7421220492	01	0	AT	Am Bach 173
00010024	Steinberger	Oezge	BEd	2	10.07.1999	2772100799	04	1	IT	Burggasse 45/9
00010029	Lang	Sofia		2	17.05.1978	9077170578	01	2	AT	Kastanienallee 214/19
00010033	Hollersbacher	Luana	BSc	2	30.04.1973	8866300473	01	0	HR	Wörthersee-Straße 35
00010038	Tomic	Hans		1	03.07.1979	5960030779	01	1	AT	Hangweg 2
00010039	Aktas	Sibel		2	24.06.1966	3102240666	02	1	AT	Tannenweg 30
00010043	Preiml	Biljana		2	05.09.1997	6663050997	01	0	AT	Talstraße 125
00010048	Grbic	Ana	Dipl.-Ing.(FH)	2	21.12.1979	2953211279	01	2	HR	Hauptplatz 87
00010050	Kroell	Valentina		2	20.04.1981	7789200481	01	2	SI	Hangweg 143
00010052	Kljajić	Erwin	MBA	1	09.03.1976	1644090376	01	0	HR	Rosentaler Straße 104

PRAXISBEISPIEL · LIVE-DEMO

Anonymisierungs- / Pseudonymisierungsprozess

Schritt 1 · Daten werden vor der externen Analyse pseudonymisiert.

ABLAUF

1 **Daten**
pseudonymisiert

2 **Analyse**
Muster & Ausreißer

3 **Entscheid**
durch Prüfer:in

Anonymisierungs- / Pseudonymisierungsprozess

PRAXISBEISPIEL · LIVE-DEMO

Das Ergebnis …

Schritt 1 · Der pseudonymisierte Datensatz

ABLAUF

1 **Daten**
pseudonymisiert

2 **Analyse**
Muster & Ausreißer

3 **Entscheid**
durch Prüfer:in

Anonymisierungs- / Pseudonymisierungsprozess



PRAXISBEISPIEL · LIVE-DEMO

KI-Analyse

Schritt 2 · Muster & Ausreißer erkennen

ABLAUF

1 **Daten**
pseudonymisiert

2 **Analyse**
Muster & Ausreißer

3 **Entscheid**
durch Prüfer:in

KI-Analyse

KI-Analyse

Was KI nicht automatisch löst

Gute KI-Prüfung braucht Datenqualität, Quellenbezug und klare Eskalationsregeln.

RISIKO		KONTROLLE
Halluzinationen	Ein Modell kann plausible, aber unbelegte Aussagen erzeugen.	**Nur Quellenbezug und strukturierte Befunde akzeptieren.**
Unvollständige Daten	Fehlende Nachträge oder Genehmigungen können zu falschen Schlussfolgerungen führen.	**Fehlende Unterlagen ausdrücklich als Unsicherheit markieren.**
Mehrdeutige Verträge	Juristisch offene Klauseln sind nicht rein technisch entscheidbar.	**Eskalation an Fach- oder Rechtsprüfung.**
Pseudonym-Leakage	Zu viele Kontextmerkmale können indirekte Re-Identifizierung ermöglichen.	**Datenminimierung, Schwellenwerte und Freigaberegeln vor externer Nutzung.**

Was wir durch das hybride Modell gewinnen

Die Architektur verbindet die Stärken lokaler Datenverarbeitung mit der Leistungsfähigkeit großer Modelle – ohne den Datenschutzgrundsatz aufzugeben.

Weniger manuelle Arbeit

Belege und Daten werden automatisiert zusammengeführt, strukturiert und vorgeprüft.

Höhere Vollständigkeit

Regeln und Vergleichsmuster werden systematisch auf alle relevanten Positionen angewendet.

Risiken früher sichtbar

Preis-, Mengen-, Zeit- oder Genehmigungsabweichungen werden gezielt priorisiert.

Bessere Nachvollziehbarkeit

Prüfhinweise kommen strukturiert, begründet und mit Quellenbezug zurück.

DER ZENTRALE MEHRWERT

Nicht „mehr KI“, sondern besseres Routing: einfache und sensible Aufgaben lokal, komplexe Analyse extern – aber nur auf anonymisierten Daten.

FAZIT

Kontrolliertes Routing statt „nur lokal“ oder „nur Cloud“.

1

KärntenGPT bleibt die Basis

Originaldaten, internes Wissen, Orchestrierung und Protokollierung bleiben in unserer Infrastruktur.

2

Externe Modelle ergänzen gezielt

Wir nutzen sie dort, wo komplexes Reasoning und große Kontextfenster einen messbaren Mehrwert bringen.

3

Extern bedeutet: anonymisiert

Keine personenbezogenen Original- oder Pseudonymdaten verlassen die Schutzzone.

4

Der Mensch entscheidet

KI priorisiert, erklärt und unterstützt – die Prüfverantwortung bleibt bei der Prüferin oder beim Prüfer.

Vielen Dank für Ihre Aufmerksamkeit

Mag. Christian Inzko · CIO / CDO
Amt der Kärntner Landesregierung