Capgemini

Information und Technik
Nordrhein-Westfalen

OC3 Case Study

Confidential AI im öffentlichen Sektor

Wie IT.NRW LLMs sicher und skalierbar einsetzt

Vortragende

Arne Schömann
GenAI Lead

Information und Technik
Nordrhein-Westfalen

Maximilian Kälbert
Data & AI Public Sector Lead

Capgemini

Vorstellung NRW.Genius

Generative Künstliche Intelligenz ist die Schlüsseltechnologie, um langfristig die Handlungsfähigkeit im öffentlichen Sektor zu erhalten

Der **demografische Wandel** führt zu unbesetzten Stellen und Wissensverlust in der Verwaltung.

Neue Technologien und die Befähigung der Beschäftigten sichern ihre **Handlungsfähigkeit**.

Generative KI unterstützt zahlreiche Handlungsfelder im öffentlichen Sektor.

33% **Senkung des Fachkräftemangels in der öffentlichen Verwaltung**

50% **Verkürzung der Bearbeitungszeiten um bis zu 50%**

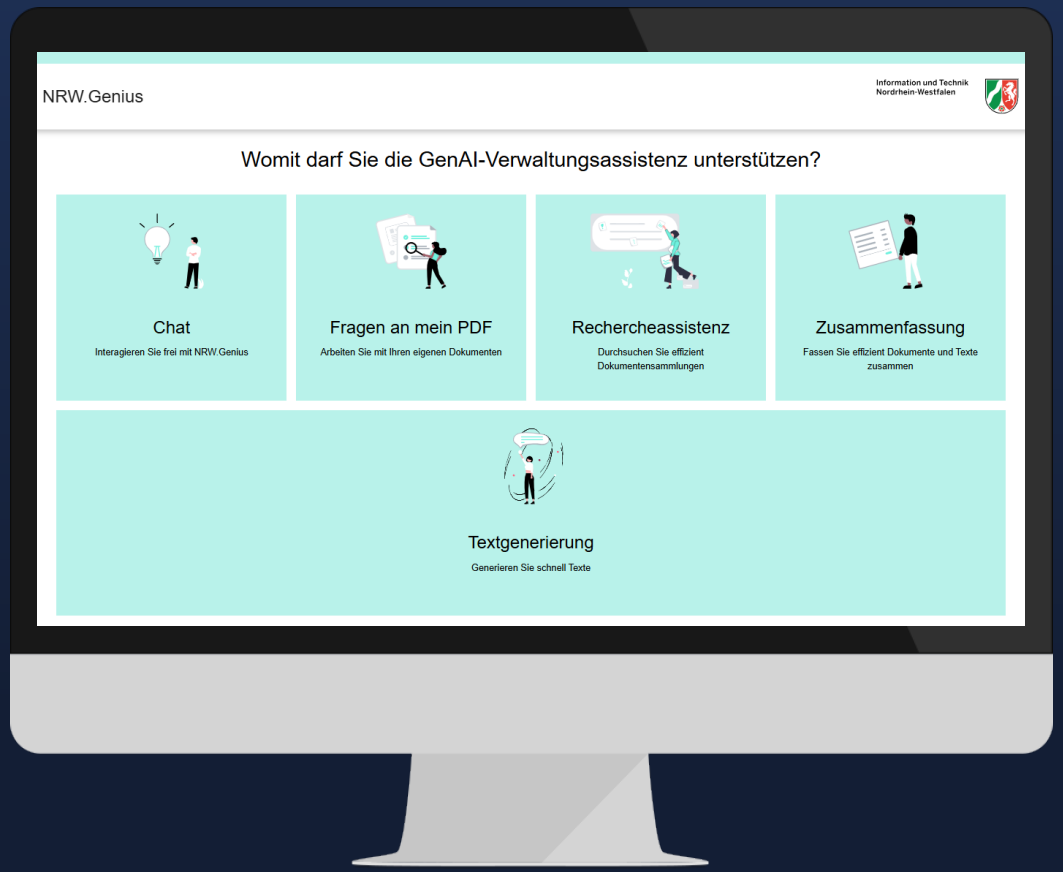
55% **Automatisierbarkeit von 55% aller Aufgaben, die Fachwissen erfordern**

Die **Potenziale** von **KI** können nur durch eine **ganzheitliche Transformation** gehoben werden.

Künstliche Intelligenz (KI) ist ein Sammelbegriff für unterschiedliche Technologien, während *generative KI* Inhalte verstehen und neue erzeugen (generieren) kann.

Quelle:
https://www.mckinsey.de/news/presse/2024-07-15-genai-and-talent-in-public-sector

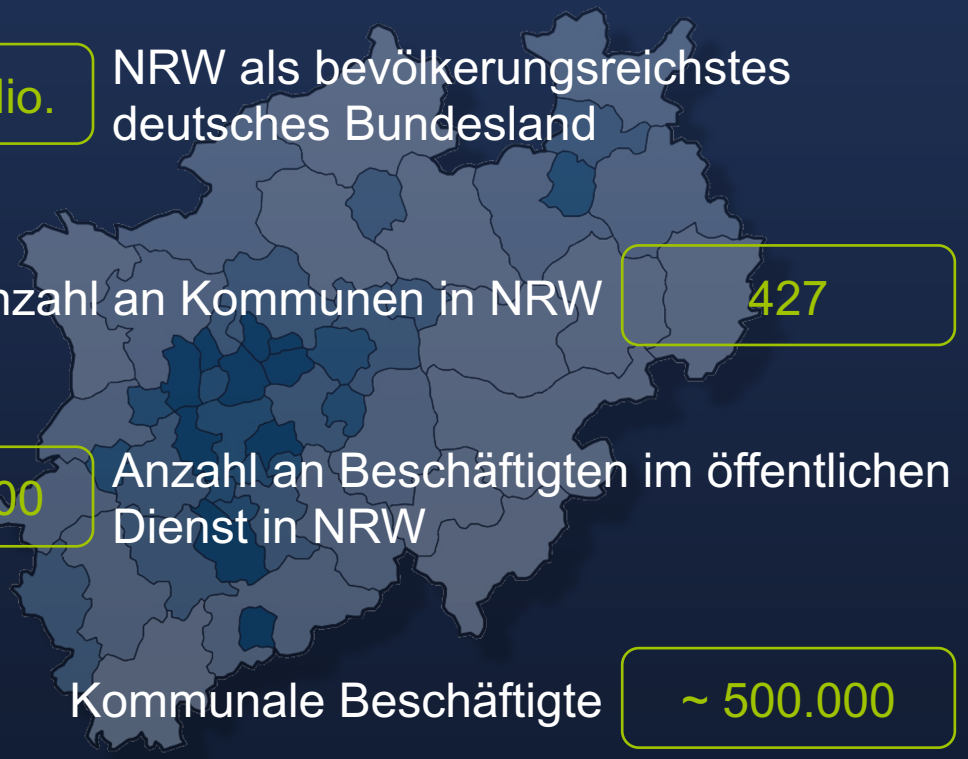
NRW.Genius ist ein gemeinschaftlicher Weg zum Einsatz von KI in der Verwaltung, getrieben aus dem Digitalisierungsministerium NRW



- Effiziente und nutzendenfreundliche Verwaltung
- Rechtssicherer Umgang mit generativer KI
- Beschleunigung von zeitraubenden Verwaltungstätigkeiten
- Kompetenzaufbau für Zukunftsfähigkeit
- Aufbau skalierbarer & hybrider Architektur

Die Größe der Verwaltung in NRW erfordert eine Lösung, die sowohl skalierbar als auch sicher ist

ca. 18 Mio. NRW als bevölkerungsreichstes deutsches Bundesland



Anzahl an Kommunen in NRW **427**

~ 300.000 Anzahl an Beschäftigten im öffentlichen Dienst in NRW

Kommunale Beschäftigte **~ 500.000**

Es bedarf einer Lösung, die kostenoptimiert in die Tiefe und Breite skalierbar ist

Besonderheiten von Daten & Dokumenten in der öffentlichen Verwaltung

- Viele textbasierte Dokumente
- Viele interne Daten
- Viele personenbezogene Daten
- Viele als Verschlusssachen (VS) gekennzeichnete Dokumente

Es bedarf einer Lösung, die eine sichere Datenverarbeitung gewährleistet

Um diese Bedarfe zu decken, müssen wir das Vertrauen in die Nutzung von Cloud stärken

Herausforderungen für die sichere Skalierung von KI in der Verwaltung

Begrenzte Kapazitäten für KI in NRW Rechenzentren

Beschaffung neuer GPU-Hardware ist langwierig und kostenintensiv

Inkompatibilität zwischen Netzen innerhalb der Verwaltung

Die Nutzung einer **sicheren Cloud** ist unerlässlich für die Skalierung.

Confidential Computing bietet hierfür einen vielversprechenden Ansatz

NRW.Genius – Confidential Computing im Chat

NRW.Genius

Information und Technik Nordrhein-Westfalen

Womit darf Sie die GenAI-Verwaltungsassistenz unterstützen?

Chat

Interagieren Sie frei mit NRW.Genius

Fragen an mein PDF

Arbeiten Sie mit Ihren eigenen Dokumenten

Rechercheassistenz

Durchsuchen Sie effizient Dokumentensammlungen

Zusammenfassung

Fassen Sie effizient Dokumente und Texte zusammen

Textgenerierung

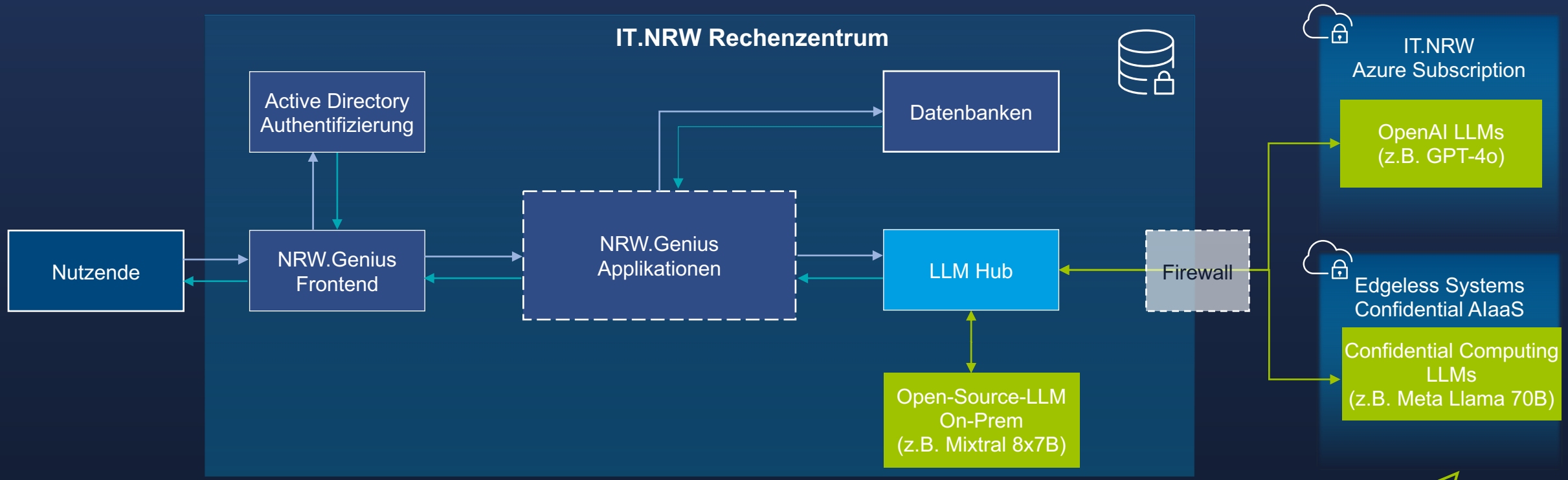
Generieren Sie schnell Texte

Im Rahmen der Teststellung steht Ihnen NRW.Genius werktags von 7:00 - 17:00 Uhr zur Verfügung.

Ausloggen

Hybride Architektur & Data Governance

Eine hybride Plattform-Architektur ermöglicht sichere Skalierung unter Wahrung der digitalen Souveränität.



Hinweis: Dies ist eine vereinfachte Darstellung der Architektur, um die wichtigsten Komponenten und deren Zusammenspiel aufzuzeigen.

Anwendungsfall-abhängige Entscheidung über die Umsetzung erfolgt in **Abstimmung mit IT-Sicherheit & Datenschutz**.

Confidential Computing ist ein weiterer Vertrauensanker als technische Maßnahme zum Schutz der Daten.

Strukturierte Data Governance ermöglicht die passende Auswahl des Verarbeitungsortes

Datenklassifizierung

- Einstufung in Datenkategorie*
  - 1: Privat- und Dienst-, Betriebs- und Geschäftsgeheimnisse gemäß StGB
  - 2: Personenbezogene Daten DSGVO
  - 3: Verschlusssachen gemäß VSA
  - 4: Sonstige Daten
- Einstufung des Schutzbedarfs von personenbezogenen Daten
  - A – Normaler Schutzbedarf
  - B – Erhöhter Schutzbedarf
  - C – Hoher Schutzbedarf

*Mindeststandard des BSI zur Nutzung externer Cloud-Dienste 2.1

Freigaben

- Empfohlene Konsultation von
  - IT-Sicherheitsbeauftragte
  - Datenschutzbeauftragte
  - Geheimschutzbeauftragte

Datenquellen

- Formulieren von Prompts
- Hochladen von Dokumenten
- Zugriff auf angebundene Datenbanksysteme

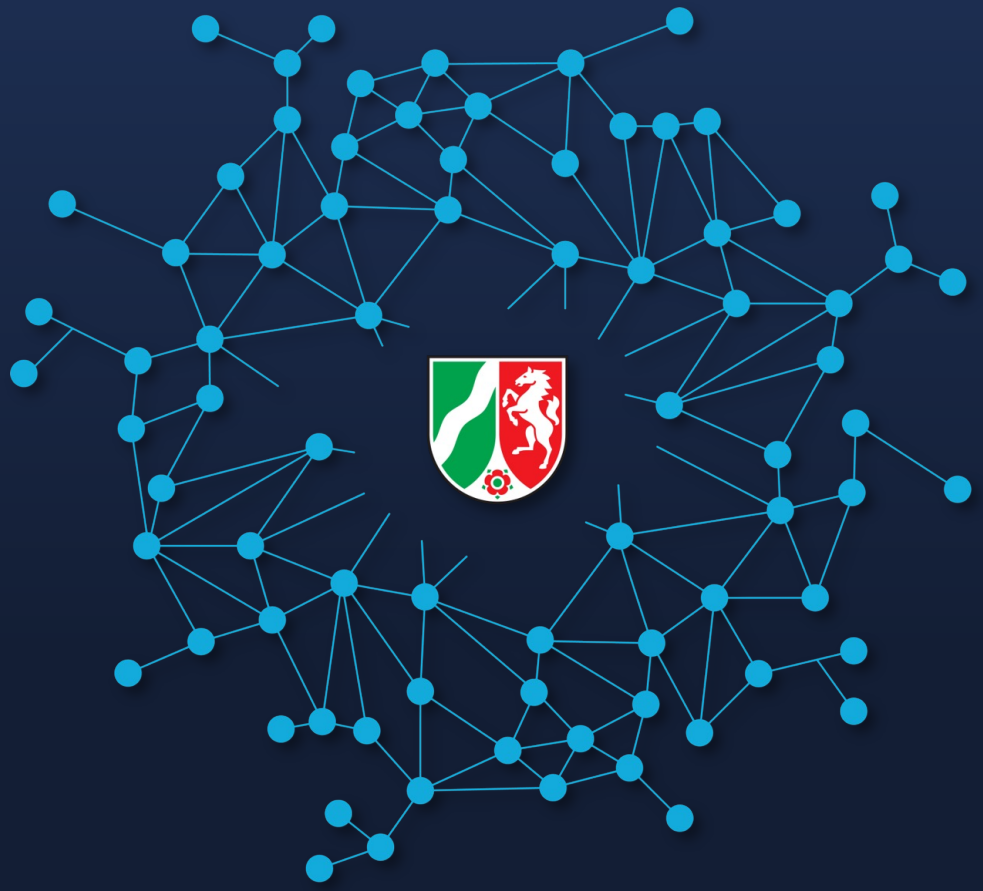
Mechanismen / Vertrauensanker

- Regelbasierte Entscheidungen
- Veränderung der Daten durch
  - Anonymisierung oder Pseudonymisierung
- KI-basierte Daten Klassifikation

Mit dem Betrieb in der Cloud & On-Premise ermöglichen wir den passenden Datenverarbeitungsort für verschiedene Anliegen

Beispiele

(Prompt) & Datenquelle	(Fragen an PDF) "Tarifspiegel 2024"	(Generierung) einer Antwort auf eine Bürgeranfrage	(Übersetzen) eines Verfassungsschutzberichts zur *Jungen Alternative*
Datenkategorie (BSI)	Kategorie 4: Sonstige Daten	Kategorie 2: Personenbezogene Daten gemäß DSGVO	Kategorie 3: Verschlusssache gemäß VSA
Schutzbedarf (personenbezogener Daten)	Kein Schutzbedarf	A – Normaler Schutzbedarf	B – Erhöhter Schutzbedarf
	Einbeziehen von IT-Sicherheits- und Datenschutzbeauftragten		
Möglicher Verarbeitungsort	Public Cloud	Confidential Computing in der Public Cloud	IT.NRW Rechenzentrum



Kontakt

Arne Schömann
arne.schoemann@it.nrw.de

Maximilian Kälbert
maximilian.kaelbert@capgemini.com