



Sicherer Einsatz von ChatGPT im Behördenumfeld



Cloudera & SVA, 12.09.2023

Webinar Behördenspiegel

Agenda

- Einführung KI und Anwendungen
Giscard Venn, SVA
- Grundlagen ChatGPT
Stefan Kammer, SVA
- Fragen & Antworten

- Open Source Sprachmodell in der Cloudera Datenplattform
Friedel Rothkötter, Jürgen Bienzeisler, Cloudera
- Fragen & Antworten
- Vorgehensmodell
Giscard Venn, SVA
- Fragen & Antworten

Vorstellung

/ SVA GmbH Kurzprofil

Deutsches Unternehmen seit 1998,
Inhabergeführter
System-Integrator

Geschäftsführung



PHILIPP ALEXANDER



SVEN EICHELBAUM

+ 1,55 Mrd. € Umsatz in 2022
+ 7.000 Kunden
+ 180 Partner

Mitarbeiter

2.900

2023

1.300

2020

1.000

2019



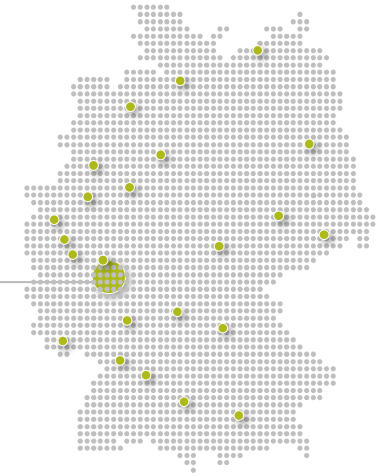
1N73LL1G3NC3
15 7H3 4B1L17Y
70 4D4P7
70 CH4NG3.

573PH3N H4WK1NG

SecurITy
Trust Seal
www.trustseal.de/lemig
made
in
Germany



27
Standorte



Darum vertrauen uns unsere Kunden



Fachliche Stärke

1.600+ Consultants
Interdisziplinäre Zusammenarbeit
Zertifiziert & kompetent



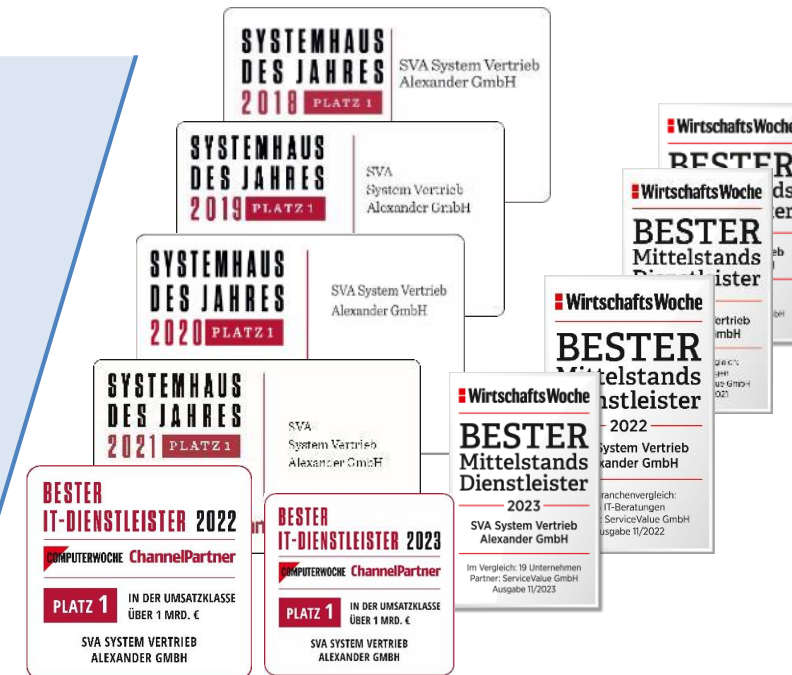
Partnerschaftliche Zusammenarbeit

Hohe Mitarbeiterzufriedenheit ↑
Große Loyalität ↑
Sehr hohe Projektqualität ↑



Planungs- und Investitionssicherheit

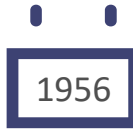
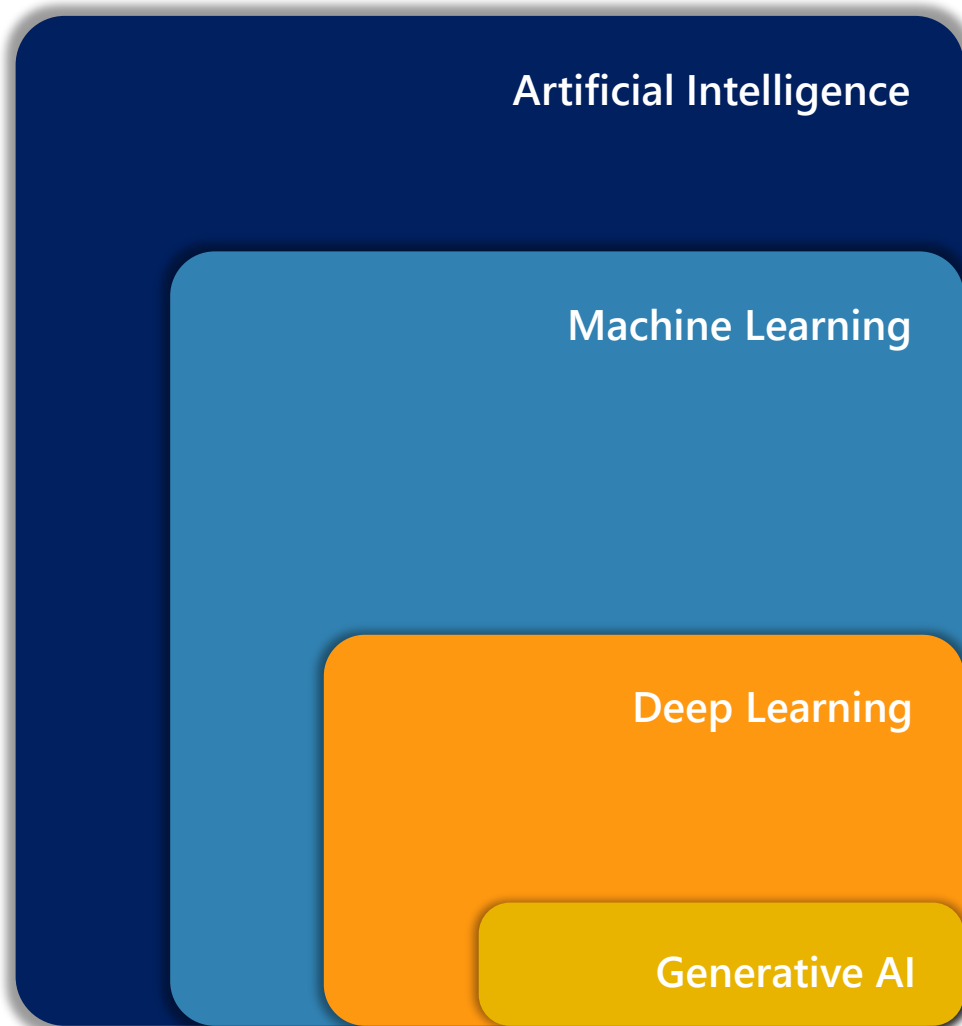
Wachstumsorientierte und
gleichzeitig konservative
Führung durch die Inhaber



/ SVA Lösungsportfolio auf einen Blick

 <p>DATACENTER INFRASTRUCTURE 450*</p> <ul style="list-style-type: none">Storage- & Server-SystemeIP-Netzwerk-InfrastrukturSoftware Defined Data Center/ContainerCloud & AutomationHyperconverged	 <p>MAINFRAME 60*</p> <ul style="list-style-type: none">Services/ConsultingzHostingzBusiness ServicesIBM System z HardwareManaged Services	 <p>END USER COMPUTING 250*</p> <ul style="list-style-type: none">Application & Desktop (CAD/E) VirtualizationVirtual Workspace & MobilityApplication, Information & Device ManagementUnified Endpoint Management	 <p>BIG DATA ANALYTICS & IOT 300 Consultants</p> <ul style="list-style-type: none">Data Science & AIOperational & Security AnalyticsBusiness IntelligenceInternet of ThingsData EngineeringManaged Big Data	 <p>SAP 50*</p> <ul style="list-style-type: none">SAP TechnologieSAP Solution ManagerSAP AnalyticsSAP SecuritySAP Lizenzmanagement
 <p>BUSINESS CONTINUITY 120*</p> <ul style="list-style-type: none">ArchivierungBackup und RecoveryDisaster RecoveryHigh AvailabilityNotfallplanung	 <p>DIGITAL PROCESS SOLUTIONS 120*</p> <ul style="list-style-type: none">Enterprise Service ManagementEnterprise Asset ManagementEngineering Lifecycle ManagementProcess Digitization & Automation<ul style="list-style-type: none">Intelligent Document Processing (IDP)Robotic Process Automation (RPA)	 <p>CYBER SECURITY 100*</p> <ul style="list-style-type: none">Information Security & Compliance ConsultingIT-Security-Architektur & -IntegrationPenetration TestingIT Security Managed ServicesSecurity Incident Response	 <p>AGILE IT & SOFTWARE DEVELOPMENT 120*</p> <ul style="list-style-type: none">DevOps & Agile KulturSoftware-EntwicklungInfrastructure as Code & Configurations ManagementCICD Pipeline/ToolchainContainer-Plattformen & Cloud Management	

/ Historie der KI



Künstliche Intelligenz



Machine Learning

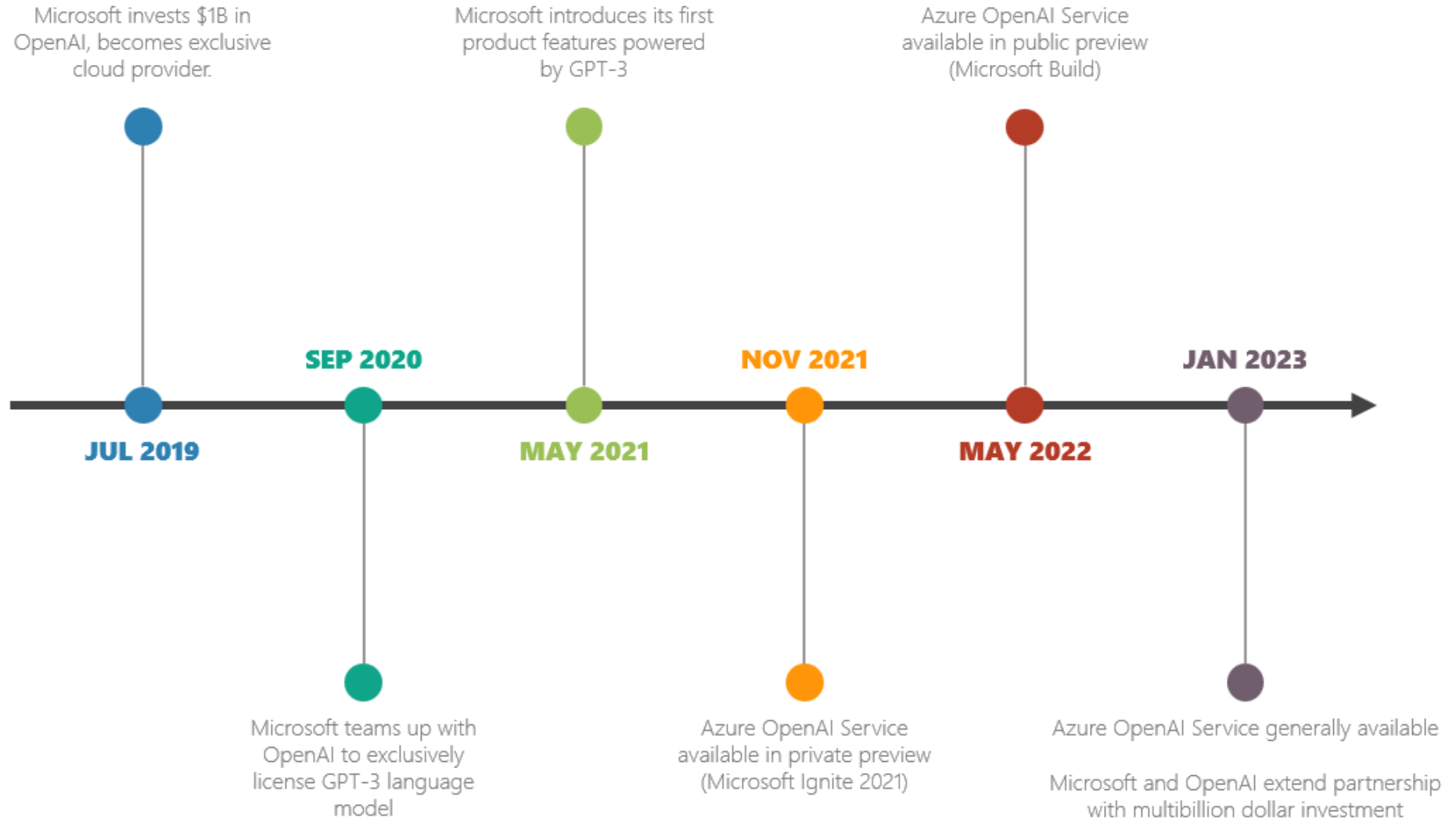


Deep Learning



Generative AI

/ Historie von ChatGPT (Generative Pre-trained Transformer)



/ Nutzung von ChatGPT

Microsoft Bing CHAT English Anmelden

Ist ein sicherer Einsatz von ChatGPT im Behördenumfeld möglich?

- ✓ Suchen nach: „sicherer Einsatz ChatGPT Behörden“
- ✓ Antworten für Sie werden generiert...

Ein sicherer Einsatz von ChatGPT im Behördenumfeld ist möglich, aber erfordert einige Vorsichtsmaßnahmen und **Richtlinien**. Es gibt datenschutzrechtliche und IT-sicherheitstechnische Aspekte, die beachtet werden müssen. Zum Beispiel sollte ChatGPT nur auf Daten zugreifen, die frei von sensiblen Informationen sind ¹ und die Nutzer sollten sich der Risiken bewusst sein, die mit der Generierung von Inhalten verbunden sind ². Es gibt auch einige Empfehlungen für die rechtssichere Nutzung von ChatGPT, die von Experten vorgeschlagen werden ³. Sind Sie an diesen Empfehlungen interessiert?

Weitere Informationen: [1. lawpilots.com](#) [2. it-recht-kanzlei.de](#) [3. legal-tech-verzeichnis.de](#) 2 von 4 ●

/ „AI Act“ der Europäischen Union

Microsoft Bing SUCHEN English 3

- ✓ Suchen nach: „why is AI regulation needed“
- ✓ Antworten für Sie werden generiert...

Eine Regulierung ist erforderlich, um sicherzustellen, dass KI-Systeme vertrauenswürdig sind und dieses Vertrauen nicht ausnutzen. KI stellt eine besondere Herausforderung dar, weil die Entwickler nicht genau wissen können, wie sich KI-Systeme verhalten werden. Außerdem können KI-Systeme Entscheidungen treffen, die einen erheblichen Einfluss auf unser Leben haben, z.B. in den Bereichen Bildung, Gesundheit oder Sicherheit ^{1 2 3 4 5}.

Haben Sie noch weitere Fragen zum Thema KI-Regulierung?

Weitere Informationen: [1. theconversation.com](#) [2. en.wikipedia.org](#) [+3 mehr](#) 2 von 4 ●

/ Nicht die Technologie stellt ein Risiko dar

Microsoft Bing SUCHEN CHAT English Anmelden 3

Wer könnte denn das Vertrauen ausnutzen?

- ✓ Suchen nach: „who can exploit trust in AI“
- ✓ Antworten für Sie werden generiert...

Das Vertrauen in KI kann von verschiedenen **Akteuren ausgenutzt** werden, die KI-Systeme entwickeln, vermarkten oder nutzen. Zum Beispiel können sie die Nutzer über die Funktionsweise, die Ziele oder die Grenzen der KI-Systeme täuschen oder irreführen. Sie können auch die Daten, die von den KI-Systemen gesammelt oder verarbeitet werden, missbrauchen oder manipulieren. Oder sie können die Verantwortung für die Folgen der KI-Entscheidungen vermeiden oder abschieben ^{1 2 3}.

Wie stehen Sie zu dem Thema Vertrauen in KI?

Weitere Informationen: [1. link.springer.com](#) [2. emerald.com](#) [3. nist.gov](#) 3 von 4

INTELLIGENCE
IS THE ABILITY
TO ADAPT
TO CHANGE.

1N73LL1G3NC3
15 7H3 4B1L17Y
70 4D4P7
70 CH4NG3.

573PH3N H4WK1NG

Deutsches Unternehmen seit 1998,
Inhabergeführter
System-Integrator



PHILIPP ALEXANDER



SVEN EICHELBAUM

Geschäftsführung

+ 1,55 Mrd. € Umsatz in 2022
+ 7.000 Kunden
+ 180 Partner

STEPHEN HAWKING

2023

1.300

2020

1.000

2019

SecurITy
made
in
Germany



27
Standorte



Darum vertrauen uns unsere Kunden



Fachliche Stärke

1.600+ Consultants
Interdisziplinäre Zusammenarbeit
Zertifiziert & kompetent



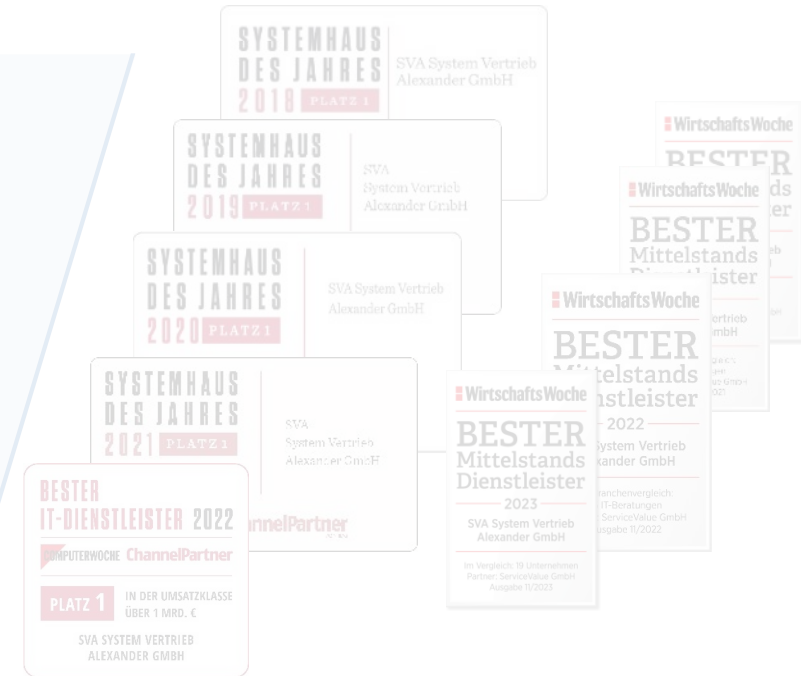
Partnerschaftliche Zusammenarbeit

Hohe Mitarbeiterzufriedenheit ↑
Große Loyalität ↑
Sehr hohe Projektqualität ↑



Planungs- und Investitionssicherheit

Wachstumsorientierte und
gleichzeitig konservative
Führung durch die Inhaber



Agenda

- Einführung KI und Anwendungen
Giscard Venn, SVA
- Grundlagen ChatGPT
Stefan Kammer, SVA
- Fragen & Antworten

- Open Source Sprachmodell in der Cloudera Datenplattform
Friedel Rothkötter, Jürgen Bienzeisler, Cloudera
- Fragen & Antworten
- Vorgehensmodell
Giscard Venn, SVA
- Fragen & Antworten

Grundlagen

/ ChatGPT

... ist eine Künstliche Intelligenz (KI)

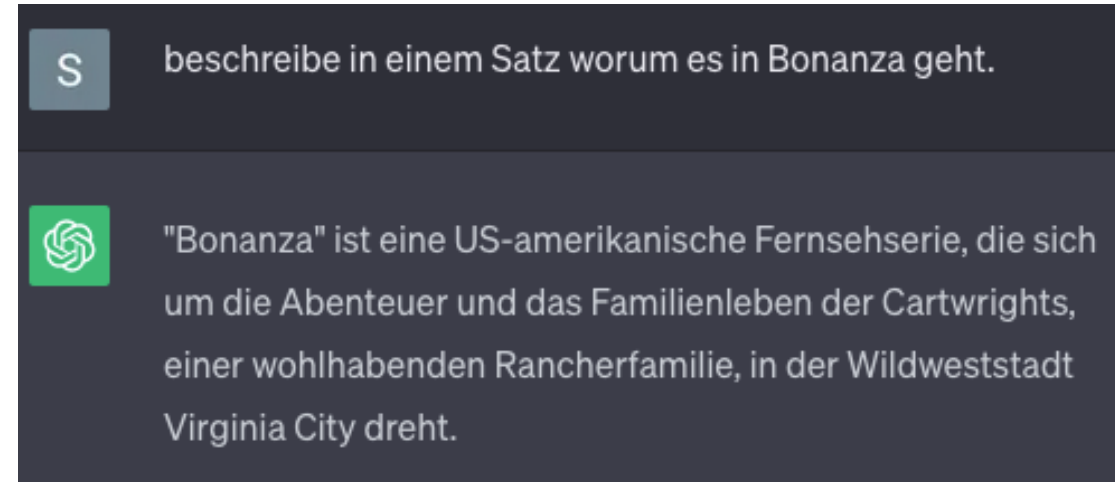
... bedeutet *Chat Generative Pretrained Transformer*

... wurde trainiert auf Daten aus dem Internet

→ Worin besteht die Intelligenz?

Funktion:

- Ich: Text Eingabe Text Input
- ChatGPT: Prozessiert Semantisches Verständnis
- ChatGPT: Text Ausgabe Text Output



Was bedeutet Semantik?

Semantik = Lehre von der Bedeutung von Wörtern und Sätzen

Klassische Suche:

Search
dax steigt Search

Title
> Elbe-Hochwasser steigt weiter - 8,54 Meter in Dresden
> Deutsche Börsen uneinheitlich - DAX fester - Verluste im NEMAX 50
> Flut steigt im Norden schneller als erwartet - Altenheime geräumt
> Elbe steigt langsam und kontinuierlich: Dresden bei 7,05 Meter
> DAX dreht ins Minus - Konjunkturdaten und Gewinnmitnahmen belasten

- Basiert auf Keyword Suche
- Kein semantisches Verständnis

Keine guten Matches

Semantische Suche:

Search
dax steigt Search

Title
> DAX wechselt nach schwachem Auftakt in die Gewinnzone
> Finanzwerte treiben DAX um mehr als sechs Prozent nach oben
> DAX nach mehreren Richtungswechseln fester - US-Märkte drehen
> Deutsche Börsen am Vormittag freundlich
> Deutsche Börse steigert Gewinne trotz Talfahrt an den Aktienmärkten

- Neuronale Netze mit semantischem Verständnis
- Von uns entwickelt und trainiert

Zufriedenstellende Matches

→ fachlich richtige Antworten nur mit Kontext

Fähigkeiten:

- Übersetzung

S

beschreibe in einem Satz worum es in Bonanza geht.



"Bonanza" ist eine US-amerikanische Fernsehserie, die sich um die Abenteuer und das Familienleben der Cartwrights, einer wohlhabenden Rancherfamilie, in der Wildweststadt Virginia City dreht.

S

übersetze das auf portugiesisch



"Bonanza" é uma série de televisão dos Estados Unidos que se concentra nas aventuras e na vida familiar dos Cartwrights, uma família de fazendeiros abastados, na cidade do Velho Oeste de Virginia City.

Grundlagen / ChatGPT


Fähigkeiten:

- Übersetzung
- Chat (Dialog/Diskussion)


S Hi, ich bin Stefan.

 Hallo Stefan! Wie kann ich Ihnen heute helfen?


S Wir können uns gerne duzen

 Natürlich, kein Problem! Wie kann ich dir heute helfen, Stefan?

S Heute ist es richtig sonnig. Das gefällt mir.

 Das klingt großartig, Stefan! Sonniges Wetter kann die Stimmung wirklich heben und bietet viele Möglichkeiten, Zeit im Freien zu verbringen. Hast du besondere Pläne oder Aktivitäten, die du bei diesem schönen Wetter genießen möchtest?

S Ich gehe gleich noch laufen.

 Das klingt nach einer ausgezeichneten Idee! Laufen ist eine großartige Möglichkeit, die Sonne zu genießen und gleichzeitig aktiv zu sein. Bist du ein regelmäßiger Läufer oder heute eher für eine entspannte Runde unterwegs?

Fähigkeiten:

- Übersetzung
- Chat (Dialog/Diskussion)
- Konditionierte Text-Generation
 - Entwürfe für: Anschreiben, Spezifikationen...

S

schreibe einen Entwurf für eine kurze Mail an Giscard und teile ihm mit, dass wir am 12. September um 11 Uhr ein Webinar mit unseren Kollegen von Cloudera halten. Dauer: 1,5 Stunden, Thema: Sicherer Einsatz von ChatGPT im Behördenumfeld



Betreff: Einladung zum Webinar am 12. September um 11 Uhr



Lieber Giscard,

ich hoffe, es geht dir gut. Ich wollte dich darüber informieren, dass wir am 12. September um 11 Uhr ein Webinar mit unseren Kollegen von Cloudera planen. Das Webinar wird sich auf das Thema "Sicherer Einsatz von ChatGPT im Behördenumfeld" konzentrieren.

Hier sind die Details:

Datum: 12. September

Uhrzeit: 11:00 Uhr (Mittleuropäische Zeit)

Dauer: 1,5 Stunden

Unser Ziel ist es, die Möglichkeiten und Herausforderungen bei der Integration von ChatGPT in behördlichen Umgebungen zu diskutieren, insbesondere in Bezug auf Datenschutz und Sicherheit. Wir glauben, dass dies ein äußerst relevantes Thema ist und freuen uns darauf, Ideen und Best Practices auszutauschen.

Es wäre großartig, wenn du an dem Webinar teilnehmen könntest. Deine Erfahrung und Expertise wären eine wertvolle Bereicherung für die Diskussion.

Bitte lass mich wissen, ob du dabei sein kannst, und ich werde sicherstellen, dass dir rechtzeitig die Einwahldaten zugeschickt werden.

Vielen Dank im Voraus für deine Teilnahme, und ich freue mich darauf, dich beim Webinar zu sehen.

Fähigkeiten:

- Übersetzung
- Chat (Dialog/Diskussion)
- Konditionierte Text-Generation
→ Entwürfe für: Anschreiben, Spezifikationen...
- Beantwortung von Fragen

S

Ist der Sommer eine Jahreszeit?



Ja, der Sommer ist eine der vier Jahreszeiten. In den meisten Teilen der Welt wird der Sommer als die Jahreszeit zwischen Frühling und Herbst betrachtet. Während des Sommers steigen die Temperaturen in der Regel, die Tage sind länger, die Vegetation blüht, und viele Menschen genießen Aktivitäten im Freien wie Schwimmen, Wandern und Grillen. Die genauen Termine, an denen der Sommer beginnt und endet, können je nach geografischer Lage variieren, da sie von der Neigung der Erdoberfläche und der Position in der Umlaufbahn um die Sonne abhängen. In den meisten Teilen der nördlichen Hemisphäre dauert der Sommer in etwa von Juni bis September, während er in der südlichen Hemisphäre von Dezember bis März dauert.



Das Problem

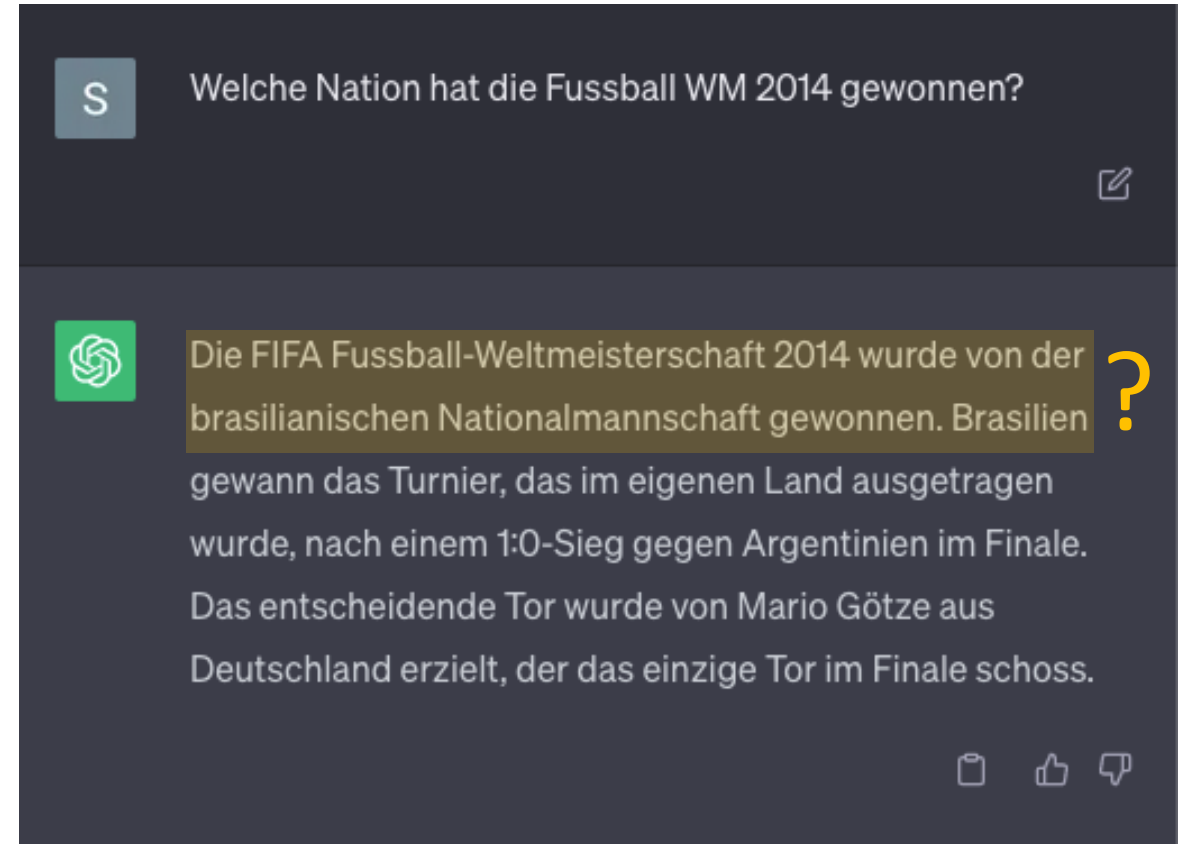
/ ChatGPT

Fähigkeiten:

- Übersetzung
- Chat (Dialog/Diskussion)
- Konditionierte Text-Generation
→ Entwürfe für: Anschreiben, Spezifikationen...
- Beantwortung von Fragen

Probleme:

- Halluzination



The screenshot shows a chat interface with a dark background. At the top, a user message (indicated by a grey 'S' icon) asks: "Welche Nation hat die Fussball WM 2014 gewonnen?". Below it, the AI response (indicated by a green OpenAI logo icon) states: "Die FIFA Fussball-Weltmeisterschaft 2014 wurde von der brasilianischen Nationalmannschaft gewonnen. Brasilien gewann das Turnier, das im eigenen Land ausgetragen wurde, nach einem 1:0-Sieg gegen Argentinien im Finale. Das entscheidende Tor wurde von Mario Götze aus Deutschland erzielt, der das einzige Tor im Finale schoss." The first sentence of the AI response is highlighted in yellow. A large yellow question mark is placed to the right of the highlighted text. At the bottom right of the chat area, there are icons for a clipboard, a thumbs up, and a thumbs down.

Das Problem

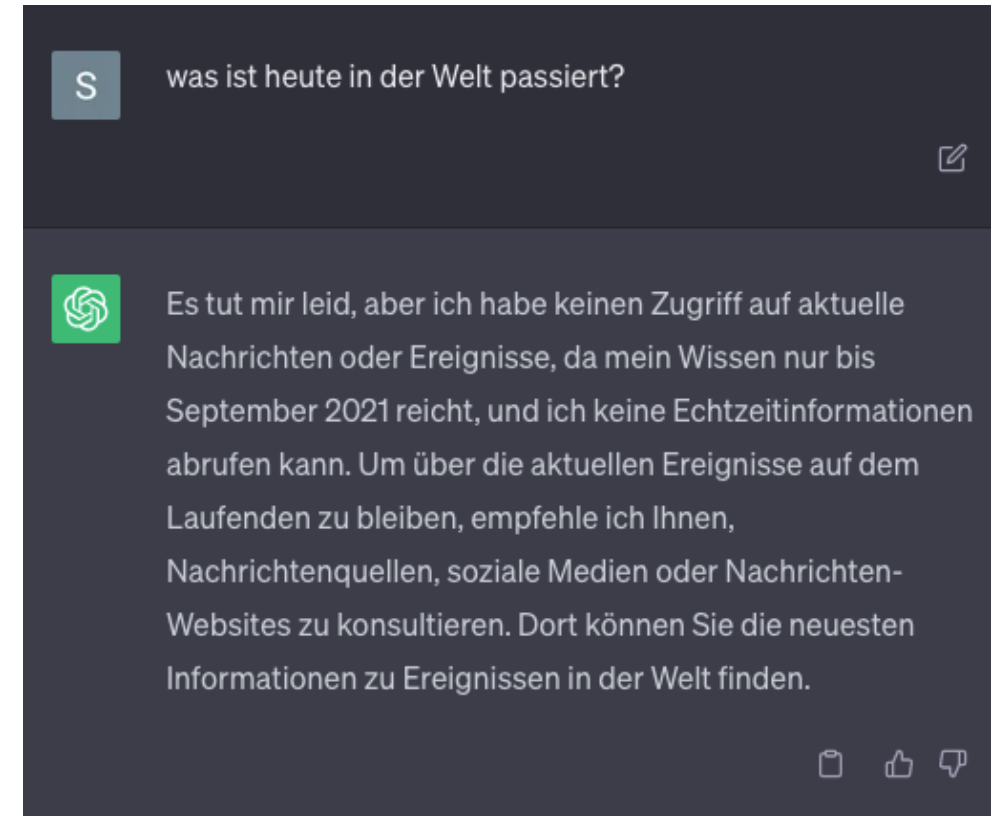
/ ChatGPT

Fähigkeiten:

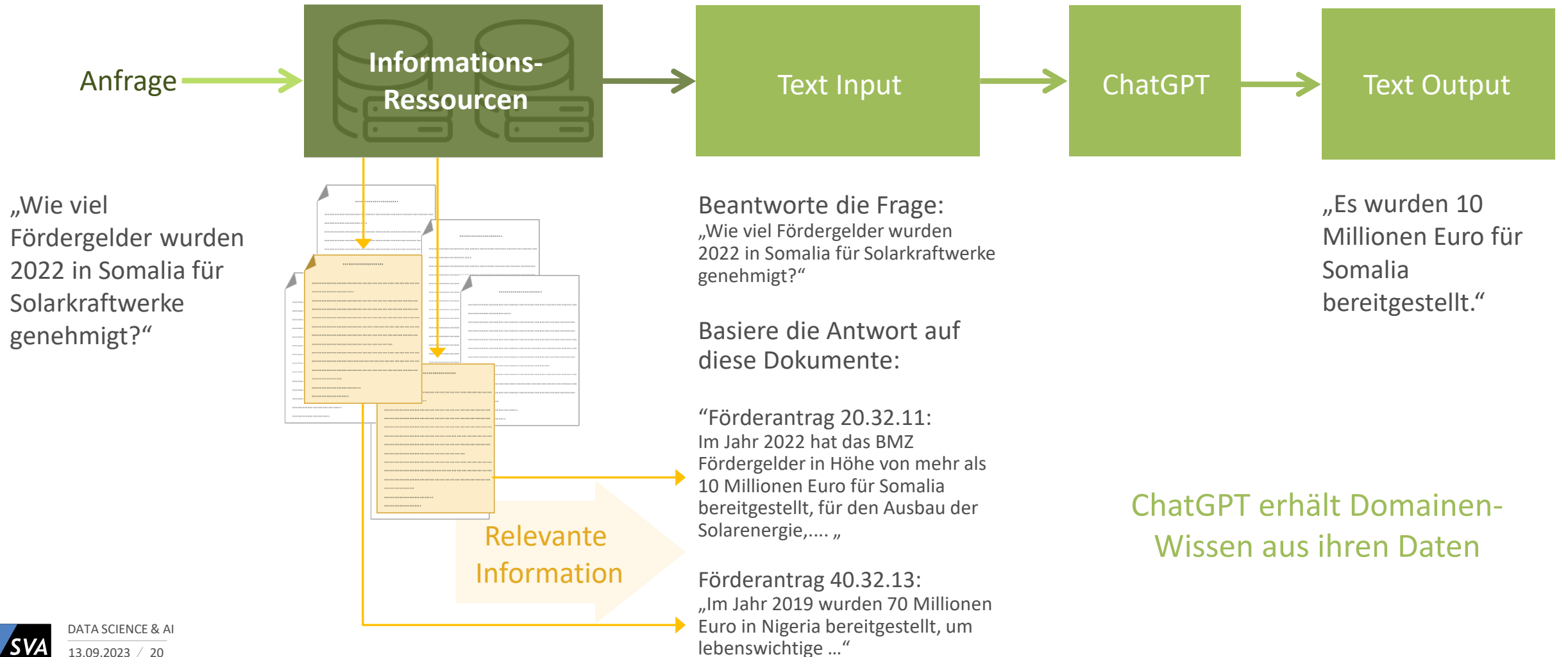
- Übersetzung
- Chat (Dialog/Diskussion)
- Konditionierte Text-Generation
 - Entwürfe für: Anschreiben, Spezifikationen...
- Beantwortung von Fragen

Probleme:

- Halluzination
- Informationshorizont: Ende 2021
 - **potentielle Falsch-Informationen**

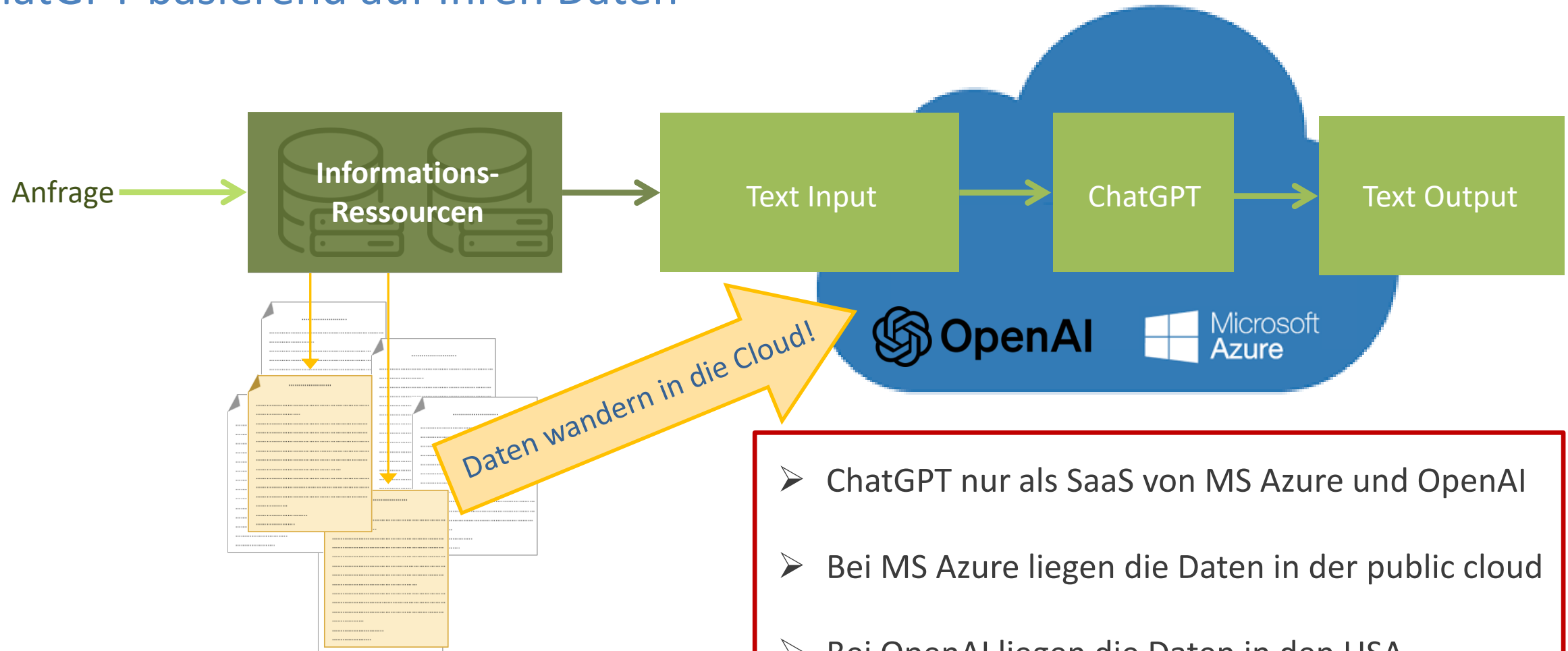


/ ChatGPT basierend auf Ihren Daten



Noch ein Problem

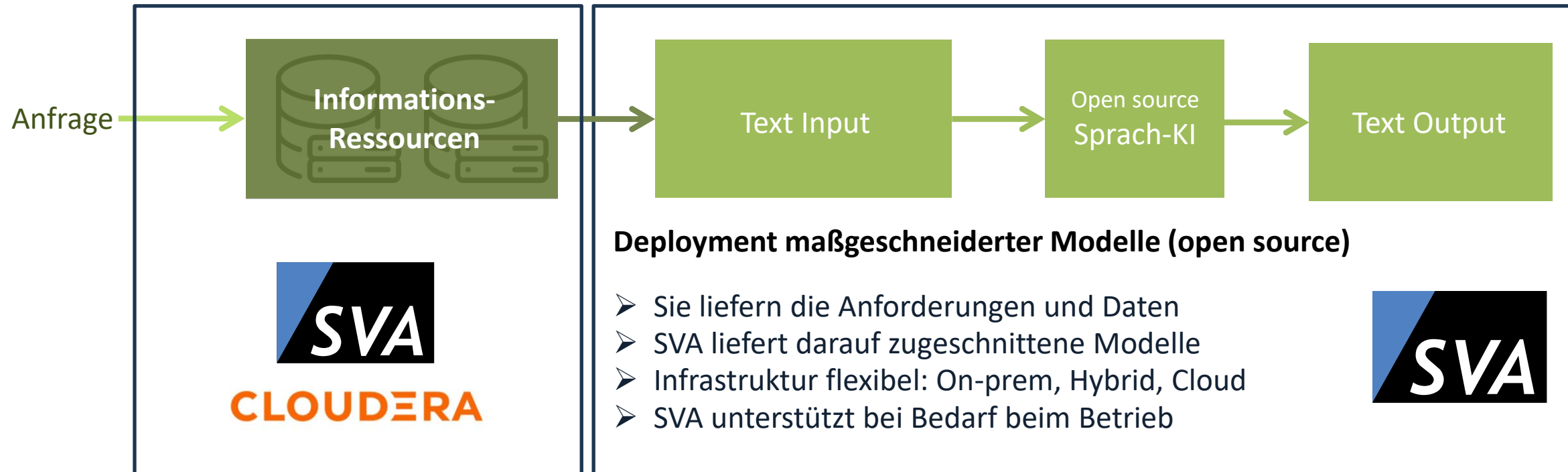
/ ChatGPT basierend auf Ihren Daten



- ChatGPT nur als SaaS von MS Azure und OpenAI
- Bei MS Azure liegen die Daten in der public cloud
- Bei OpenAI liegen die Daten in den USA

Risiko des Kontroll-Verlustes über Ihre Daten

/ Behalten Sie die digitale Souveränität



ChatGPT Funktionalität basierend auf Ihren Daten:

- Umfassende Kontrolle über ihre Daten bei gleichzeitiger Flexibilität der Infrastruktur

Agenda

- Einführung KI und Anwendungen
Giscard Venn, SVA
- Grundlagen
Stefan Kammer, SVA
- Fragen & Antworten

- Open Source Sprachmodell in der Cloudera Datenplattform
Friedel Rothkötter, Jürgen Bienzeisler, Cloudera
- Fragen & Antworten
- Vorgehensmodell
Giscard Venn, SVA
- Fragen & Antworten

Agenda

- Einführung KI und Anwendungen
Giscard Venn, SVA
- Grundlagen
Stefan Kammer, SVA
- Fragen & Antworten

- Open Source Sprachmodell in der Cloudera Datenplattform
Friedel Rothkötter, Cloudera
- Fragen & Antworten
- **Vorgehensmodell**
Giscard Venn, SVA
- **Fragen & Antworten**

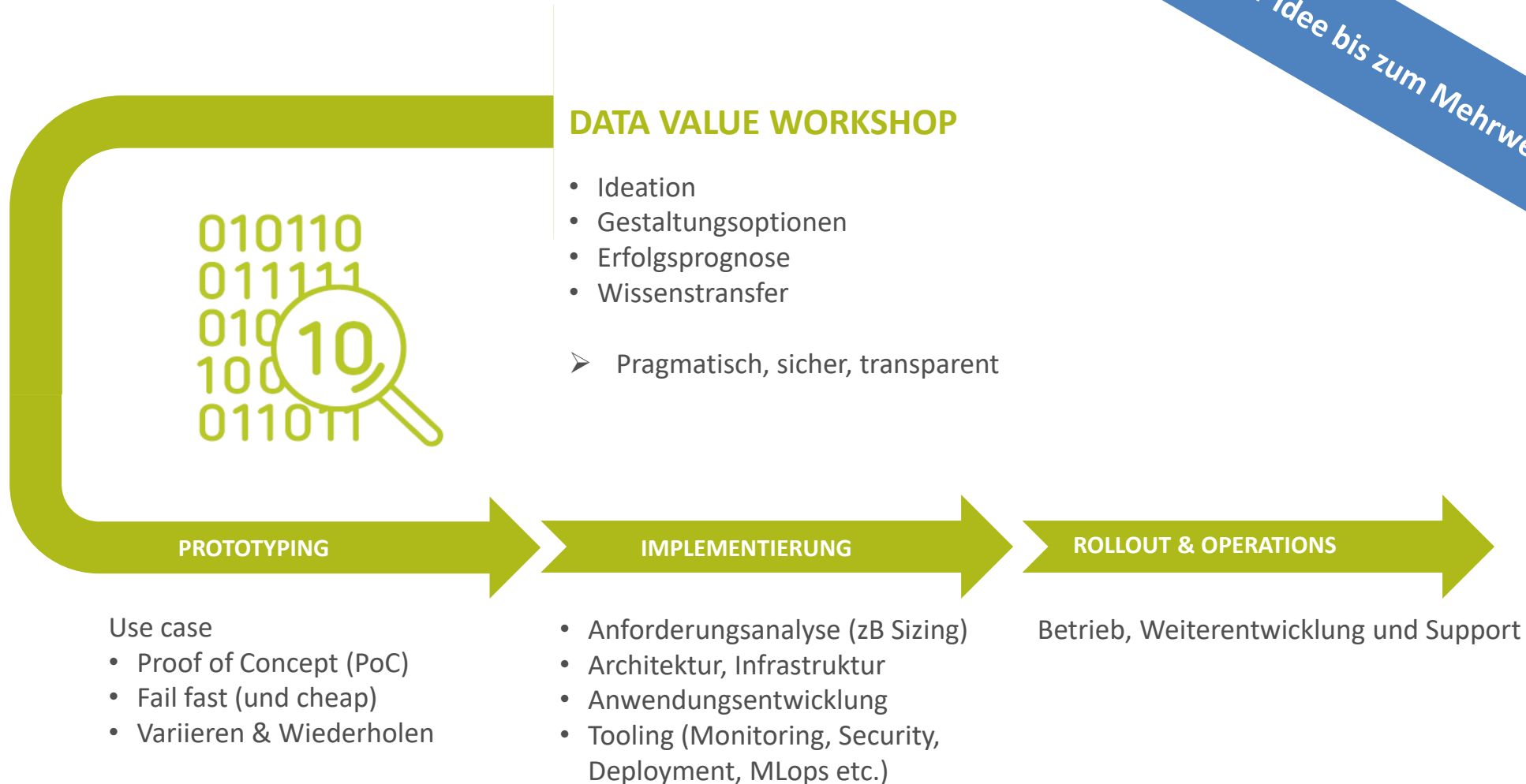
/ Herausforderung KI

Häufige Probleme innovativer Projekte:

- Unscharfes Ziel, kein Lastenheft
- Schwierige Projekt- und Budgetplanung
- Sehr viele Beteiligte aus unterschiedlichsten Bereichen
- Unklare Datenlage
- Es gibt kein best-practise
- Ideenentwicklung unabhängig von der Möglichkeit zur Umsetzung

/ SVA End-to-end Lösungsangebot

Von der Idee bis zum Mehrwert



/ Strukturierte und erprobte Methode von SVA



DATA VALUE WORKSHOP

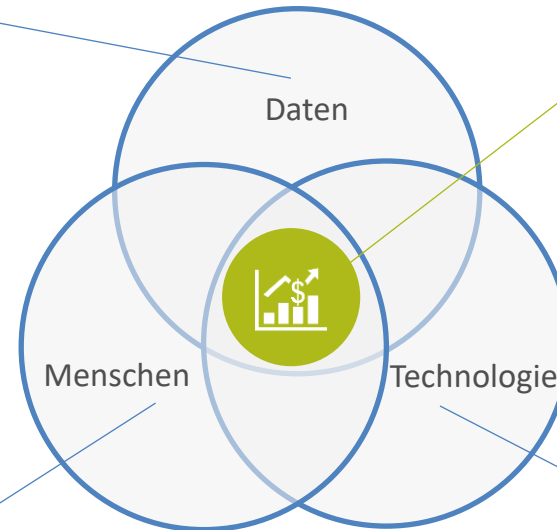
- Kategorie
 - Analytics
 - Vorhersagen
 - Generative KI
- Einsatzszenarien
 - Mehrwert aus Daten (Information aus Daten, Wissen aus Information, Erfahrung)
 - Erwarteter output (Wissen , KPI, Bilder, Text, Sprache)
 - Automatisierung (zB Repetitive Aufgaben, Prozesssteuerung)
 - Assistenzsystem (zB Entscheidungshilfe, Interaktive Guidance, Information)
- Use Cases und Priorisierung
- Vorqualifikation der Daten (zB relevante Datenquellen, Qualität, Governance)
- Erfassung der Ist-Situation (inkl. Datenquellen, vorhandene Architektur, Restriktionen, Besonderheiten,...)
- Technologische Optionen und High Level Architektur (IT, Algorithmik)
- Umsetzungsplanung
 - Voraussetzungen
 - Zeitraum
 - Aufwand
 - Budget

/ Die Idee des **Data Value** Workshops

- Ungenutzte Data entdecken
- Relevante Datenquellen und Stakeholder identifizieren
- Datenqualität einschätzen
- Metadata einbeziehen
- Governance

Kleine crossfunktionale Teams:

- Breite Kompetenzstreuung
- Fachexpertise
- Offenes Mindset
- Selbstorganisierend



Data Value

- Anforderungsmanagement
- Entscheidungskriterien
- Fit-Gap Analyse
- Managen der Komplexität
- Schnelle Ergebnisse / Weites Ziel

/ Der erste Schritt zur Einführung von ChatGPT



DATA VALUE WORKSHOP - Phase 0

- Einführung - Generative KI
 - Definition des Projektscopes in der Co-Creation mit Ihnen
 - Erfassung der Ist-Situation
 - Exploration der Datenlage (Quellen, Quantität, Qualität, Ownership)
 - Technologische Optionen und High Level Architektur
 - Infrastruktur und Tech-Stack
 - Model-Lifecycle Management
 - Governance, Risk, Compliance
 - Projektplanung
- Übergang in Phase 1 (häufig PoC oder MVP)

1N73LL1G3NC3
15 7H3 4B1L17Y
70 4D4P7
70 CH4NG3.

573PH3N H4WK1NG

Schon bei der ziewten ächlnih gglaeetren Afagbue geht es veil snehellcr. Das nnet man Efrhunrag.

Erfahrung und Expertise sind zwei herausragende Qualitätsmerkmale von SVA.

Agenda

- Einführung KI und Anwendungen
Giscard Venn, SVA
- Grundlagen
Stefan Kammer, SVA
- Fragen & Antworten

- Open Source Sprachmodell in der Cloudera Datenplattform
Friedel Rothkötter, Cloudera
- Vorgehensmodell
Giscard Venn, SVA
- Fragen & Antworten



Giscard Venn

Fachvertrieb Big Data | Analytics | KI

SVA GmbH

Mobil: +49 151 26427874

Giscard.Venn@sva.de

/

Wir, die Referenten Giscard Venn und Stefan Kammer, bestätigen bei der Erstellung meiner Präsentation die rechtlichen/urheberrechtlichen Vorgaben für die Nutzung von Werken Dritter beachtet zu haben. Wir versichern, dass für den Fall der Nutzung fremder Werke in meiner Präsentation die erforderlichen Lizenzen / Genehmigungen eingeholt wurden. Wir sind Urheber der Präsentation und zu erreichen unter:
SVA System Vertrieb Alexander GmbH, Borsigstraße 26, 65205 Wiesbaden