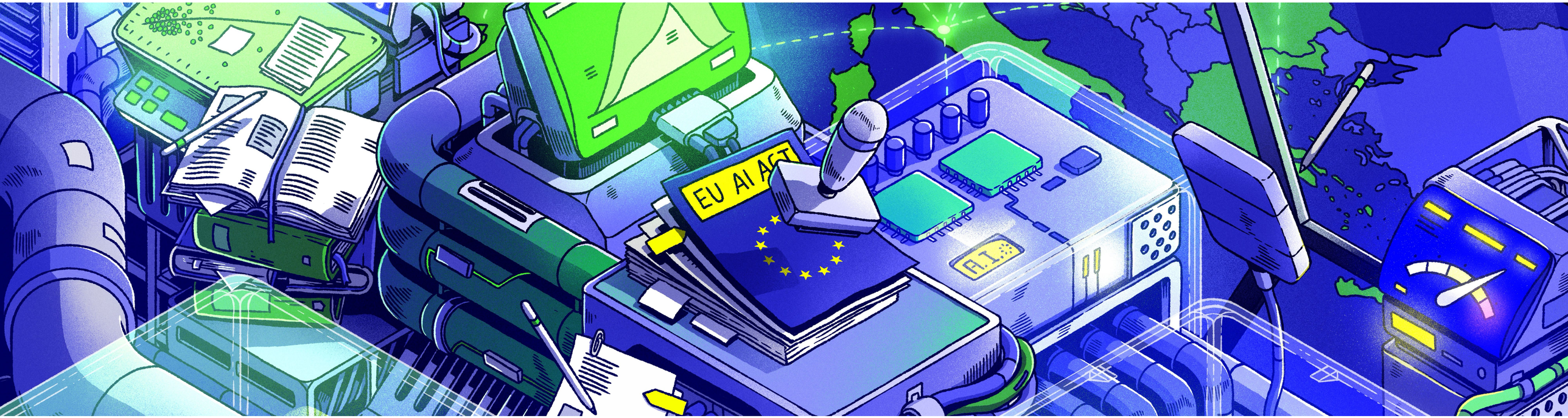
TECH MEETS LAW:
DER AI ACT KOMMT – WIE DIE UMSETZUNG GELINGT



In dieser Lunch-Session bringen unsere Experten die wichtigsten rechtlichen Neuerungen auf den Punkt und geben wertvolle Tipps zur Umsetzung. Das Besondere: Neben der regulatorischen Perspektive beleuchten wir die konkreten Auswirkungen des AI Acts auf die Praxis – Tech meets Law!

KÜNSTLICHE INTELLIGENZ

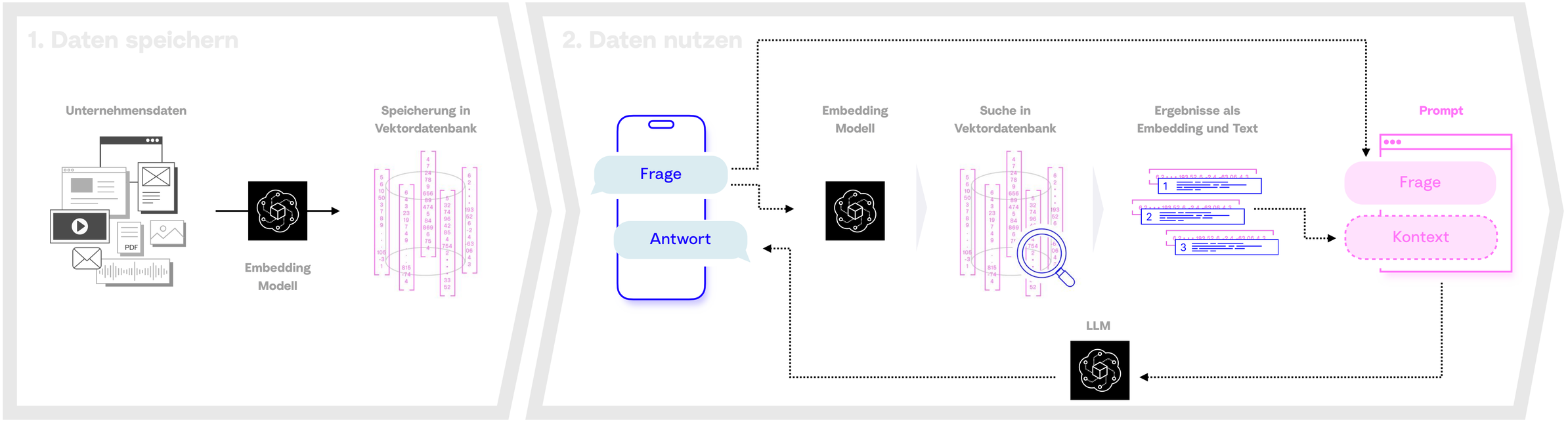
Die EU hat notgedrungen versucht, den Terminus „KI-System“ zu definieren. Was ist denn KI? Wann liegt deiner Meinung nach ein KI-System vor, wann nicht?

RETRIEVAL AUGMENTED GENERATION

Was hat es mit „RAGs“ auf sich? Was ist das überhaupt und wie funktioniert es? In welchem Verhältnis steht es zu KI-Modellen?

WAS IST EIN RAG UND WIE FUNKTIONIERT ES?

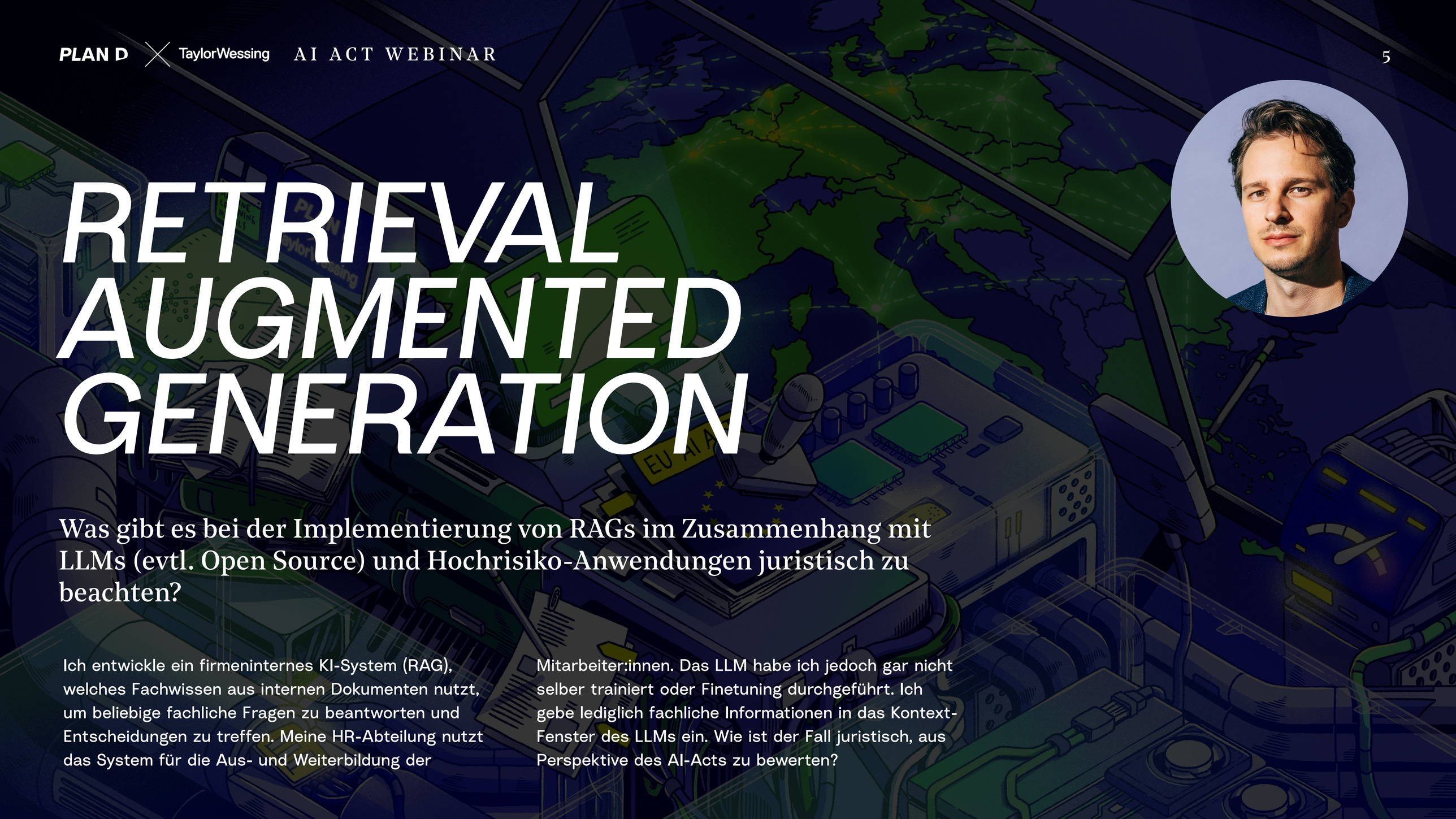
1. Daten im Unternehmen finden und säubern
2. KI übersetzt Fachwissen in Vektoren und speichert es
3. Fachliche Frage durch Nutzer:in an das KI-System
4. Relevantes Wissen für Antwort in Datenbank finden
5. Prompt für das LLM durch Frage und Suchergebnisse
6. Generierung der Antwort durch das LLM



LLM
Ein LLM, ein vortrainiertes KI-Modell, analysiert große Textmengen, um sie zu verstehen und neue Texte zu generieren.

Embeddings
Mathematische und abstrakte Darstellung der Bedeutung von Worten oder Textabschnitten durch Vektoren mit vielen Dimensionen.

Prompt
Befehle und Anweisungen für große KI-Sprachmodelle über Inhalt, Formulierung und Struktur ihrer Antwort in Textform.



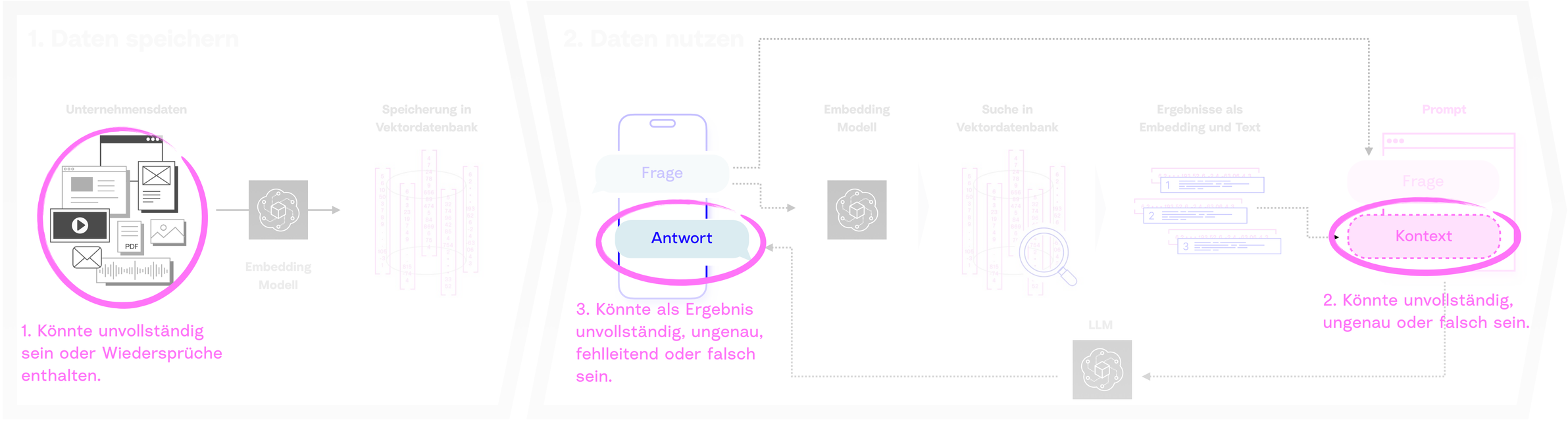
RETRIEVAL AUGMENTED GENERATION

Was gibt es bei der Implementierung von RAGs im Zusammenhang mit LLMs (evtl. Open Source) und Hochrisiko-Anwendungen juristisch zu beachten?

Ich entwickle ein firmeninternes KI-System (RAG), welches Fachwissen aus internen Dokumenten nutzt, um beliebige fachliche Fragen zu beantworten und Entscheidungen zu treffen. Meine HR-Abteilung nutzt das System für die Aus- und Weiterbildung der Mitarbeiter:innen. Das LLM habe ich jedoch gar nicht selber trainiert oder Finetuning durchgeführt. Ich gebe lediglich fachliche Informationen in das Kontext-Fenster des LLMs ein. Wie ist der Fall juristisch, aus Perspektive des AI-Acts zu bewerten?

JURISTISCHE ASPEKTE BEI DER IMPLEMENTIERUNG VON RAGS MIT LLMS IN HOCHRISIKO-ANWENDUNGEN

1. Daten im Unternehmen finden und säubern
2. KI übersetzt Fachwissen in Vektoren und speichert es
3. Fachliche Frage durch Nutzer:in an das KI-System
4. Relevantes Wissen für Antwort in Datenbank finden
5. Prompt für das LLM durch Frage und Suchergebnisse
6. Generierung der Antwort durch das LLM



LLM
Ein LLM, ein vortrainiertes KI-Modell, analysiert große Textmengen, um sie zu verstehen und neue Texte zu generieren.

Embeddings
Mathematische und abstrakte Darstellung der Bedeutung von Worten oder Textabschnitten durch Vektoren mit vielen Dimensionen.

Prompt
Befehle und Anweisungen für große KI-Sprachmodelle über Inhalt, Formulierung und Struktur ihrer Antwort in Textform.

JURISTISCHE ASPEKTE BEI DER IMPLEMENTIERUNG VON RAGS MIT LLMS IN HOCHRISIKO-ANWENDUNGEN

1. Daten im Unternehmen finden und säubern
2. KI übersetzt Fachwissen in Vektoren und speichert es
3. Fachliche Frage durch Nutzer:in an das KI-System
4. Relevantes Wissen für Antwort in Datenbank finden
5. Prompt für das LLM durch Frage und Suchergebnisse
6. Generierung der Antwort durch das LLM

LLM
Ein LLM, ein vortrainiertes KI-Modell, analysiert große Textmengen, um sie zu verstehen und neue Texte zu generieren.

Embeddings
Mathematische und abstrakte Darstellung der Bedeutung von Worten oder Textabschnitten durch Vektoren mit vielen Dimensionen.

Prompt
Eingaben und Anweisungen für große KI-Sprachmodelle über Inhalt, Formulierung und Struktur ihrer Antwort in Textform.

VERMEIDUNG VON BIAS

Was genau ist Bias? Wie lässt sich so etwas verlässlich feststellen und wie kann man ihn verhindern?

Hochrisiko-KI-Systeme, in denen Techniken eingesetzt werden, bei denen KI-Modelle mit Daten trainiert werden, müssen mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden, die bestimmten Qualitätskriterien entsprechen. Unter anderem muss „eine Untersuchung im Hinblick auf mögliche Verzerrungen (Bias)“ angestellt werden, „die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken oder zu einer nach den Rechtsvorschriften der Union verbotenen Diskriminierung führen könnten, insbesondere wenn die Datenausgaben die Eingaben für künftige Operationen beeinflussen“ – was genau ist Bias? Wie lässt sich so etwas verlässlich feststellen? Wie kann man das ausschließen?

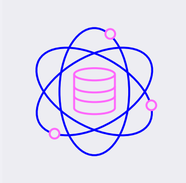
TECHNISCHE MAßNAHMEN GEGEN BIAS IN KI-MODELLEN

Vielfältige Daten

- Wenn möglich Verwendung unterschiedlicher Daten-quellen.
- Sicherstellen, dass verschiedene Gruppen repräsentiert sind.
- Repräsentive Zeiträume verwenden.
- Vermeidung von Überre-präsentation einzelner Gruppen.

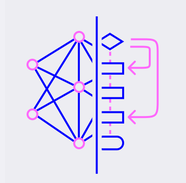
Datenanalyse und -vorbereitung

- Analyse der Datenquellen auf potenzielle Verzerrungen, Vorurteile und Fehler.
- Validieren der Annahmen durch Expertenwissen oder zusätzliche Datenquellen.
- Korrigieren oder Entfernen unrepräsentativer Datenpunkte.



Datenanreicherung oder -reduktion

- Hinzufügen fehlender Datenpunkte zur Verbesserung der Repräsentation (synthetisch).
- Entfernen von Daten, die zu Verzerrungen führen könnten.
- Ausgleich von Datenungleichgewichten durch Gewichtung oder Anpassung.



Test nach dem Training

- Durchführung von automatischen qualitativen Tests.
- Durchführung von automatischen quantitativen Tests nach mathematischen Metriken.
- Vergleich der Modellvorhersagen für verschiedene statistische Gruppen.

Monitoring

- Kontinuierliche Überwachung der Modellleistung im Echtbetrieb.
- Regelmäßige Überprüfung auf neue oder sich verändernde Verzerrungen.
- Anpassung des Modells basierend auf aktuellen Überwachungsdaten.

REGELMÄßIGKEIT DER PRÜFUNG

Wie regelmäßig muss ich mir bei ständiger Weiterentwicklung meines KI-Produktes über die KI-Regulierung Gedanken machen?

Ich bin Founder:in eines jungen SaaS-Unternehmens; wir setzen viel KI im Coding, im Marketing, aber vor allem in unserem eigenen Produkt ein. Die Technologie entwickelt sich wahnsinnig schnell und ständig erweitern wir unser Produkt oder tauschen Technologien und KI-Modelle aus. Wie regelmäßig muss ich mir über die Regulierung und den Abgleich von Produkt und AI Act Gedanken machen?

BEAUFSICHTIGUNG VON KI

Wie könnte die Beaufsichtigung von KI-Systemen in der Praxis aussehen? Welche technischen sowie organisatorischen Maßnahmen könnte man treffen?

Die KI-Verordnung schreibt für Hochrisiko-KI-Systeme vor, dass sie so konzipiert und entwickelt werden, dass sie während der Dauer ihrer Verwendung – auch mit geeigneten Instrumenten einer Mensch-Maschine-Schnittstelle – von natürlichen Personen wirksam beaufsichtigt werden können. Wie könnte das in der Praxis aussehen? Welche technischen sowie organisatorischen Maßnahmen könnte man treffen?

TOMS FÜR DIE BEAUFSICHTIGUNG DER KI

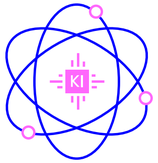
Human in the Loop

- Mensch kontrolliert und überwacht jede Entscheidung der KI.
- KI unterstützt den Menschen bei der Entscheidungsfindung mit Vorschlägen.
- Mensch hat die endgültige Kontrolle und Verantwortung durch Bestätigung.
- **Lösung: Benutzeroberflächen, welche Ergebnisse zeigen und nach Bestätigung fragen.**

Human on the Loop

- Mensch überwacht das KI-System in Echtzeit.
- Eingreifen des Menschen nur bei Bedarf, z.B. bei Fehlern der KI.
- KI trifft eigenständig Entscheidungen, aber unter menschlicher Aufsicht.
- **Lösung: Benutzeroberfläche die aktuelle und historische Entscheidung der KI darstellt, Mensch kann Entscheidung der KI überschreiben.**

Human out of the Loop



- KI arbeitet komplett autonom ohne menschliches Eingreifen.
- Mensch ist nicht direkt in den Entscheidungsprozess involviert.
- Menschliche Kontrolle erfolgt nur bei der Entwicklung und initialen Einrichtung der KI.
- **Lösung: System protokolliert Entscheidung der KI, benötigt den Menschen jedoch nicht.**

Viele KI-Projekte starten mit "Human in the Loop”-Ansätzen, werden aber durch Effizienzdruck, Fachkräftemangel und KI-Überlegenheit immer autonomer.

STRAFBARKEIT UND BUßGELDER

Wer ist bei der Entwicklung von künstlicher Intelligenz für den Verstoß in Dienstleistungsbeziehungen verantwortlich?

Ich bin Dienstleister:in und entwickle KI-Lösungen für Kund:innen. Innerhalb eines Projektes bemerke ich, dass meine Kund:innen die Vorgaben durch die KI-Regulierung vernachlässigen oder die Regulierung sehr zum eigenen Vorteil auslegen. Wie gehe ich vor und mache ich mich als Entwickler:in selbst strafbar, wenn ich an diesem Projekt mitwirke?

AI LITERACY

Was ist „AI literate“, warum ist es wichtig und wie kann man es erreichen? Welche Formate und Vorgehensweisen eignen sich?

Die KI-Verordnung fordert ja „AI Literacy“, also von Anbietern und Betreibern, „nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind“ – was kann man vor diesem Hintergrund tun, um als „AI literate“ zu gelten?

KI PROJEKT-MANAGEMENT

Ab wann sollen meine Teammitglieder den Rat eines juristischen Experten in ihren KI-Projekten einbeziehen?

Wir fangen im Unternehmen zurzeit ein neues KI-Projekt an. Wann ist der richtige Zeitpunkt Experten bzw. Expertinnen für die Regulierung einzubeziehen? Ganz am Anfang oder nach meinen ersten POCs und der genauen Ermittlung der Funktionen, Datenquellen und Datenmerkmale, die überhaupt verwendet werden? Kurz: Wie sieht ab jetzt mein Projektplan für KI-Projekte aus?

EINZIGARTIGE BERATUNG FÜR EINE NEUARTIGE REGULIERUNG

PLAN D × TaylorWessing

Komplexe Zeiten erfordern innovative Mittel. In Kooperation mit der führenden Kanzlei für IT- und Datenschutzrecht bündeln wir unsere Expertisen, um mit einem neuen Beratungsansatz eine elementare Lücke zu schließen: zwischen juristischen Regularien und technologischer Umsetzung.

ZWEI FLIEGEN, EINE KLAPPE

FRITZ-ULLI PIEPER, LL.M.

Salary Partner bei TAYLOR WESSING
Fachanwalt für IT-Recht

Fritz-Ulli Pieper berät nationale und internationale Mandanten im IT-, Telekommunikations- und Datenschutzrecht. Er verfügt über besondere Erfahrung zu Rechtsfragen der Digitalisierung und Künstlicher Intelligenz. Zudem berät er die öffentliche Hand bei großvolumigen IT- und Infrastrukturvorhaben.

- TOP Anwalt für IT-Recht, WirtschaftsWoche 2021, 2022
- Führender Anwalt im Datenschutzrecht, Kanzleimonitor (diruj) 2019-2022
- Hervorgehoben als Kernanwalt für Informationstechnologie und Digitalisierung, Legal 500 Germany 2021

F.Pieper@taylorwessing.com

SEBASTIAN BLUHM

Managing Partner bei PLAN D
Informatiker, Experte für KI-Technologien und Strategien

Sebastian Bluhm hat jahrelange Erfahrung in der Leitung und Umsetzung komplexer Technologieprojekte – in mittelständischen Unternehmen wie in multinationalen Konzernen. Seine Arbeitsschwerpunkte zielen insbesondere auf die nachhaltige Entwicklung und Implementierung von KI-Produkten, IT-Architekturen und neuen Technologien.

- Mitglied des KI Bundesverbandes
- Certified Data Scientist Specialized in Deep Learning
- Best of Consulting Mittelstand 2021 Digitalisierung & KI, WirtschaftsWoche

Sebastian.Bluhm@plan-d.com