Schwetzinger IT-Rechtstage 2024

Copilot, Gemini & Co
KI-Einsatz im Unternehmen

Prof. Dr. Thomas Wilmer

h_da

Gliederung

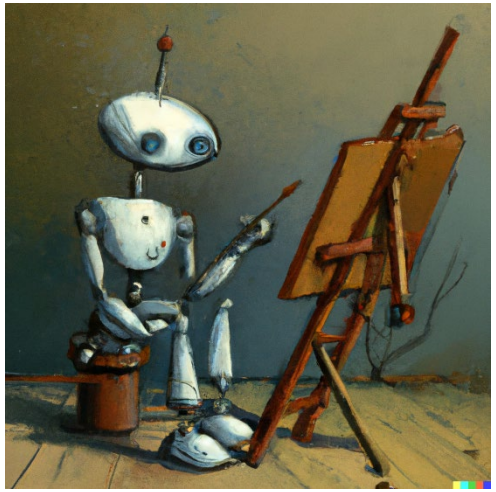
1. Funktionsweise von Copilot, Geschäftsmodell und Eigendarstellungen MS
2. Arbeitsrechtliche Fragestellungen
3. Haftung für falsche Ergebnisse oder Missbrauch?
4. Praxishinweise

FAQ und Checklisten sowie Open Access-Publikationen
unter Copilot-recht.de / chatgpt-recht.de

h_da

Funktionsweise von Copilot: Basis ChatGPT

- Textanalyse der „Prompts“ durch sogenannte Künstliche (schwache) Intelligenz
- “Ein KI-System ist ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und nach seiner Einführung eine Anpassungsfähigkeit aufweist, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können.
- Einsatz über API in vielen Funktionalitäten denkbar
- Keine Übernahme einzelner Elemente



“a depressed robot painting on a canvas, digital art”

Funktionsweise von Copilot: Basis ChatGPT

- KI-Modell für allgemeine Zwecke" ist ein KI-Modell, das - auch wenn es mit einer großen Datenmenge unter Verwendung von Selbstüberwachung in großem Maßstab trainiert wurde - eine erhebliche Allgemeinheit aufweist und in der Lage ist, ein breites Spektrum unterschiedlicher Aufgaben kompetent auszuführen, unabhängig davon, wie das Modell auf den Markt gebracht wird, und das in eine Vielzahl von nachgelagerten Systemen oder Anwendungen integriert werden kann. Dies gilt nicht für KI-Modelle, die vor ihrer Veröffentlichung auf dem Markt für Forschungs-, Entwicklungs- und Prototyping-Aktivitäten verwendet werden.

Funktionsweise von Copilot: Basis ChatGPT

https://openai.com/policies/terms-of-use

3. Content

(a) **Your Content**. You may provide input to the Services ("Input"), and receive output generated and returned by the Services based on the Input ("Output"). Input and Output are collectively "Content." As between the parties and to the extent permitted by applicable law, you own all Input. Subject to your compliance with these Terms, OpenAI hereby assigns to you all its right, title and interest in and to Output. This means you can use Content for any purpose, including commercial purposes such as sale or publication, if you comply with these Terms. OpenAI may use Content to provide and maintain the Services, comply with applicable law, and enforce our policies. You are responsible for Content, including for ensuring that it does not violate any applicable law or these Terms.

Geschäftsmodell Copilot

https://news.microsoft.com/de-de/microsoft-copilot-jetzt-fuer-mehr-menschen-und-unternehmen-verfuegbar/

Copilot Pro bietet:

- Ein einheitliches KI-Erlebnis, das auf all Ihren Geräten läuft und Ihren Kontext im Web, auf Ihrem PC, in Ihren Apps und bald auch auf Ihrem Smartphone versteht, um Ihnen die richtigen Fähigkeiten bereitzustellen, wenn sie gebraucht werden.
- Zugriff auf Copilot in Word, Excel[1], PowerPoint, Outlook und OneNote auf PC, Mac und iPad für Abonnent*innen von Microsoft 365 Single und Family.
- Bevorzugter Zugang zu den neuesten Modellen – ab sofort mit OpenAIs GPT-4 Turbo. Mit Copilot Pro haben Sie auch zu Stoßzeiten Zugang zu GPT-4 Turbo, um schneller arbeiten zu können. Und bald haben Sie auch die Möglichkeit, zwischen den Modellen zu wechseln, um Ihr Erlebnis nach Ihren Vorstellungen zu optimieren.
- Verbesserte KI-Bilderstellung mit Image Creator from Designer (ehemals Bing Image Creator), der dank 100 Boosts pro Tag schneller ist und Ihnen eine höhere Bildqualität sowie Querformat bietet.
- Die Möglichkeit, mit unserem neuen Copilot GPT Builder (in Kürze verfügbar) mit wenigen Eingabeaufforderungen Ihr eigenes Copilot GPT zu erstellen – einen auf ein bestimmtes Thema zugeschnittenen Copilot.

Geschäftsmodell Copilot

"**Copilot in Outlook** helps you manage and triage your email and time more efficiently. It provides personalized suggestions, summaries, and insights to help you stay on top of things and save time. Whether you need help drafting the appropriate email response, schedule meetings in a few clicks, find key information in an email thread, or make sure your message has the right tone and clarity, Copilot can help you achieve your goals"

https://techcommunity.microsoft.com/t5/outlook-blog/copilot-in-outlook-helps-you-achieve-more/ba-p/3981033

Beispiele unter https://adoption.microsoft.com/de-de/copilot/

Die heutigen Neuerungen umfassen:

Copilot für Microsoft 365 ist jetzt **allgemein verfügbar für kleine Unternehmen** mit Microsoft 365 Business Premium und Business Standard. Kunden können zwischen einem und 299 Zugängen für 30 US-Dollar pro Person und Monat erwerben.

Wir **heben die Mindestanzahl von 300 Zugängen für kommerzielle Pläne auf** und machen Copilot verfügbar für Kunden mit **Office 365 E3 und E5** verfügbar (bisher war eine Microsoft-365-Lizenz erforderlich).

Gewerbliche Kunden können Copilot für Microsoft 365 jetzt über unser Netzwerk von **Microsoft-Cloud-Solution-Provider-Partnern** erwerben.

Im vergangenen Monat gaben wir außerdem bekannt, dass Copilot für Microsoft 365 für **Lehrpersonal und Mitarbeitende im Bildungsbereich** zugelassen ist.

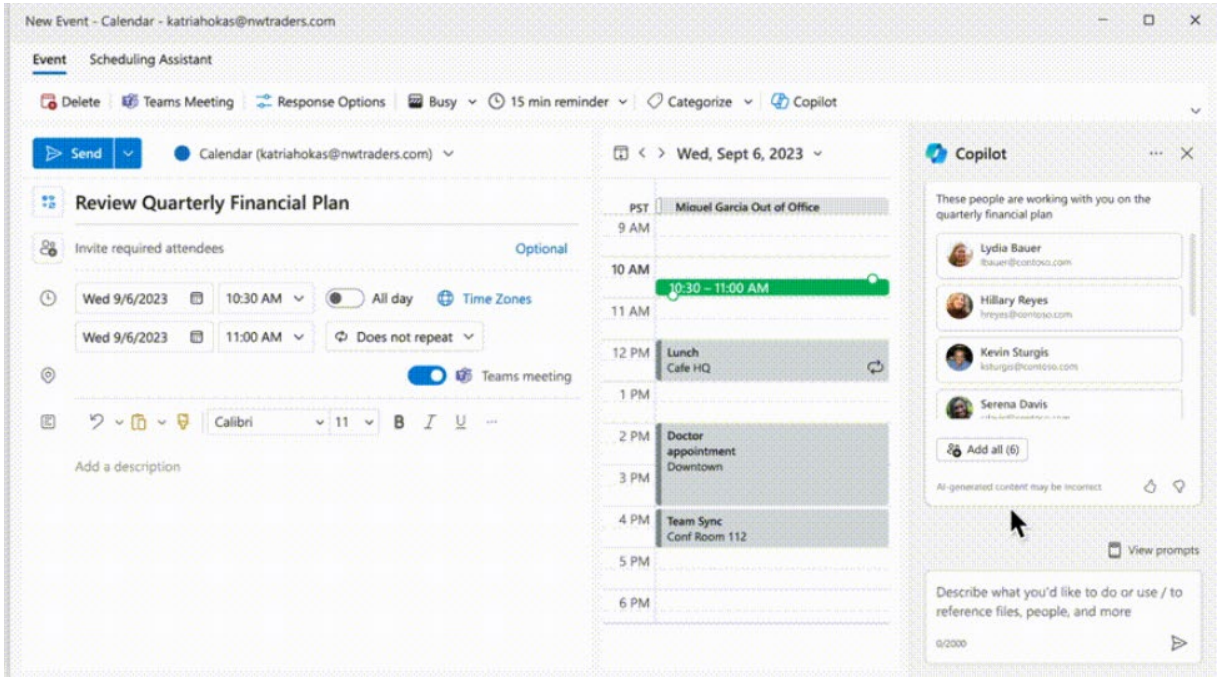
Geschäftsmodell Copilot

Copilot für Microsoft 365 ist sogar noch leistungsfähiger für Unternehmen, weil er mit ihrem gesamten Universum an Daten funktioniert, die bei der Arbeit anfallen – einschließlich E-Mails, Meetings, Chats, Dokumenten und mehr sowie Daten aus dem Internet. Mit Prompts in natürlicher Sprache wie „Erzählen Sie meinem Team, wie wir die Produktstrategie aktualisiert haben" kann Copilot ein Status-Update auf der Grundlage der Besprechungen, E-Mails und Chats des Vormittags erstellen. Copilot ist auch in die Apps integriert, die Millionen von Menschen täglich nutzen, einschließlich Microsoft Teams (das nicht mit Copilot Pro verfügbar ist). Copilot fördert Ihre Kreativität in Word, analysiert Daten in Excel[1], entwirft Präsentationen in PowerPoint, sortiert Ihren Outlook-Posteingang, fasst Meetings in Teams zusammen – unabhängig davon, ob Sie daran teilgenommen haben oder nicht – und vieles mehr. Unterstützt durch Sicherheit, Datenschutz und Compliance auf Unternehmensniveau und Microsofts Verpflichtung zum Kundenurheberrecht können wir kaum erwarten zu sehen, wie Unternehmen jeder Größe mit KI mehr erreichen. Erfahren Sie mehr auf dem Microsoft 365 Blog.

Geschäftsmodell Copilot

Ask Copilot to schedule a meeting
You can ask Copilot with a prompt to help you schedule a meeting, and it will guide you through the scheduling process. Copilot understands requests for meeting titles (E.g. Schedule a meeting to review the quarterly financial plan) and because it has access to the Microsoft Graph data it can suggest relevant people, files, and available times. Copilot can also draft an agenda, and you can do all these in a few clicks.

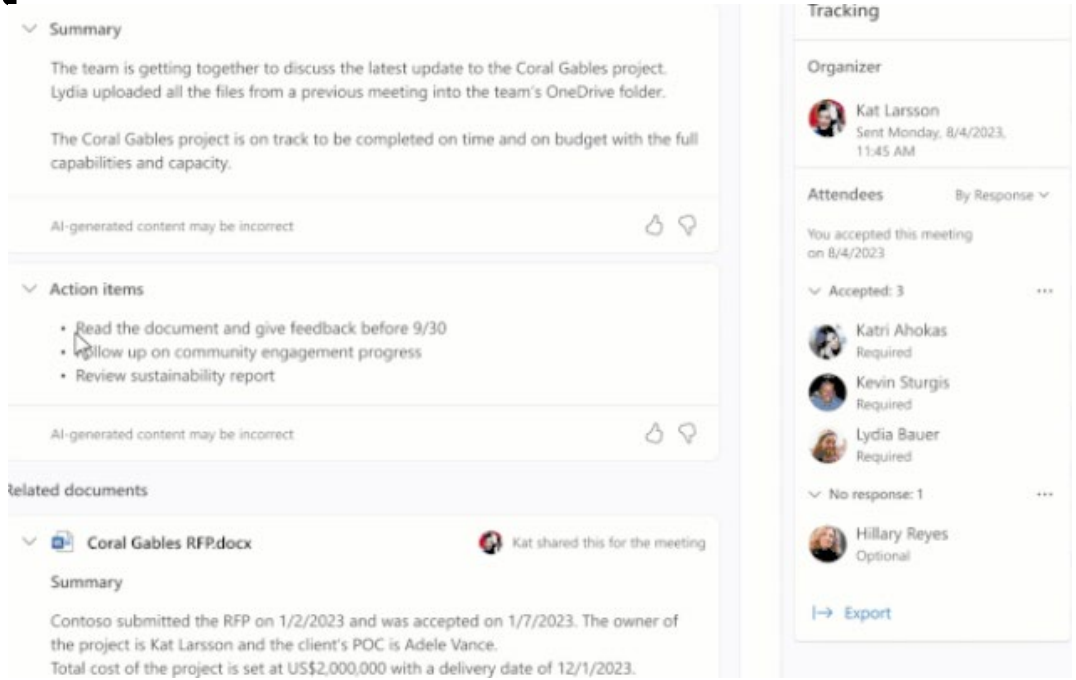
https://techcommunity.microsoft.com/t5/outlook-blog/copilot-in-outlook-helps-you-achieve-more/ba-p/3981033



Geschäftsmodell Copilot

Get ready for your next meeting in minutes
When you have an upcoming meeting, Copilot proactively shows you a "Prepare" button in your inbox which helps you quickly get context by creating a summary of the meeting and showing and summarizing relevant files.

https://techcommunity.microsoft.com/t5/outlook-blog/copilot-in-outlook-helps-you-achieve-more/ba-p/3981033



Geschäftsmodell Copilot

Summarize long email threads and get suggested actions like schedule a meeting

Copilot extracts crucial information from email threads and suggests actions like scheduling a meeting it then helps you draft agendas, summarize discussions, create meeting titles, populate attendees, append the original thread for clarity, and find available times to meet.

Follow a meeting you can't attend and stay on top of any actions items

Following a meeting allows you to stay on top of its outcomes and any actions items you might have – When you follow a meeting, Copilot will notify you when the meeting recap is ready for you to review and you can even ask Copilot questions about the meeting

Copilot for Mail Management

Copilot helps you manage your inbox, it can draft email responses that sound like you, summarize email threads extracting key information and suggesting follow up actions, and coach you to deliver your message in the right tone and clarity to communicate more effectively.

https://techcommunity.microsoft.com/t5/outlook-blog/copilot-in-outlook-helps-you-achieve-more/ba-p/3981033

Geschäftsmodell Copilot

https://www.cio.de/a/bayer-setzt-auf-microsoft-copilot,3728645

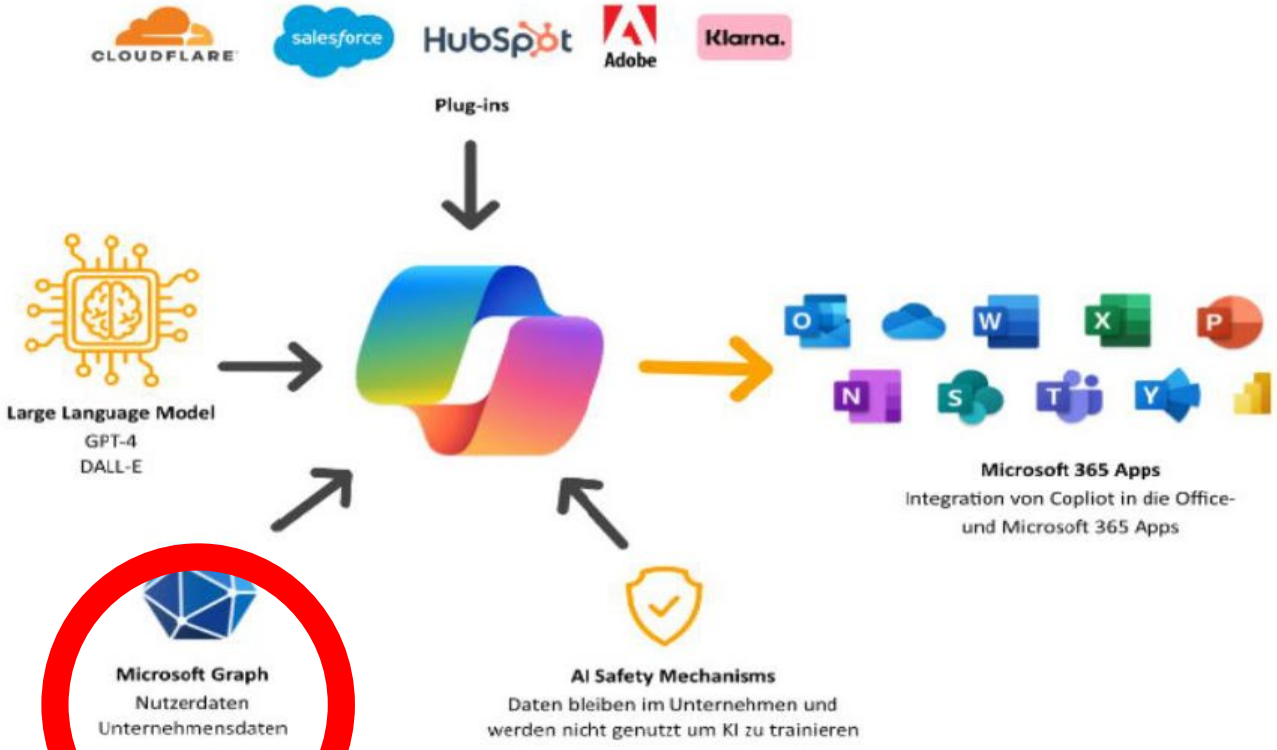
"Laut Christoph Sieger, Vice President und Head of Global Digital Workplace bei Bayer, gäbe es viel Neugierde für das KI-Tool innerhalb der Belegschaft. Das gelte besonders in den Bereichen HR, R&D, IT, Beschaffung und Marketing. "Viele Menschen sagen bereits, dass sie von Tag zu Tag produktiver werden," so der Manager. Mitarbeitende bekämen bessere Informationen aus Meetings und fänden Dokumente schneller, was die Zusammenarbeit verbessere.

(...)

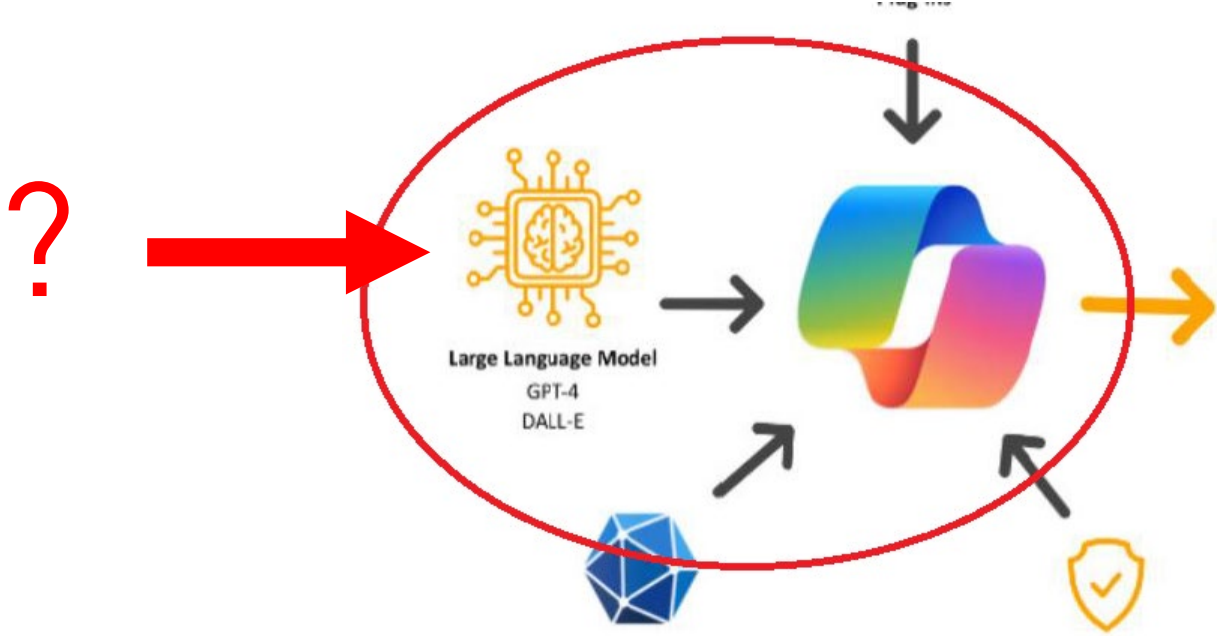
Über 700 solcher Use Cases hat Bayer identifiziert. Dazu zählten etwa, Daten einfacher aus Excel-Listen zu extrahieren, E-Mails und deren Anhänge zusammenzufassen, Textentwürfe in Word oder Powerpoint-Präsentationen zu erstellen."

Input & Output

https://learn.microsoft.com/en-us/microsoft-sales-copilot/architecture



Input & Output



h_da

Eigenangaben Microsoft

https://learn.microsoft.com/de-de/microsoft-365-copilot/microsoft-365-copilot-privacy

Wie verwendet Microsoft 365 Copilot Ihre geschützten Organisationsdaten?

Microsoft 365 Copilot bietet einen Mehrwert durch die Verbindung von LLMs mit Ihren Organisationsdaten. Microsoft 365 Copilot greift auf Inhalte und Kontext über Microsoft Graph zu. **Es kann Antworten generieren, die in Ihren Organisationsdaten verankert sind, wie z. B. Benutzerdokumente, E-Mails, Kalender, Chats, Besprechungen und Kontakte. Microsoft 365 Copilot kombiniert diese Inhalte mit dem Arbeitskontext des Benutzers, z. B. der Besprechung, in der sich ein Benutzer gerade befindet, der E-Mail-Austausch, den der Benutzer zu einem Thema hatte, oder die Chatunterhaltungen, die der Benutzer in der letzten Woche geführt hat.** Microsoft 365 Copilot verwendet diese Kombination aus Inhalt und Kontext, um genaue, relevante und kontextbezogene Antworten zu liefern.

h_da

Eigenangaben Microsoft

https://learn.microsoft.com/de-de/microsoft-365-copilot/microsoft-365-copilot-privacy

Eingabeaufforderungen, Antworten und Daten, auf die über Microsoft Graph zugegriffen wird, werden nicht für das Training von Foundation LLMs verwendet, auch nicht für die von Microsoft 365 Copilot verwendeten.

Eigenangaben Microsoft

https://learn.microsoft.com/de-de/microsoft-365-copilot/microsoft-365-copilot-privacy

h_da

Eigenangaben Microsoft

https://learn.microsoft.com/de-de/microsoft-365-copilot/microsoft-365-copilot-privacy

- Microsoft verwendet strenge physische Sicherheit, Hintergrundprüfung und eine mehrschichtige Verschlüsselungsstrategie, um die Vertraulichkeit und Integrität von Kundeninhalten zu schützen.
- Microsoft 365 verwendet dienstseitige Technologien, die Ruhe- und Transitinhalte von Kunden verschlüsseln, einschließlich BitLocker, dateibasierter Verschlüsselung, Transport Layer Security (TLS) und Internetprotokollsicherheit (Internet Protocol Security, IPsec). Spezifische Informationen zur Verschlüsselung in Microsoft 365 finden Sie unter Verschlüsselung in der Microsoft Cloud.
- Ihre Kontrolle über Ihre Daten wird durch Microsofts Verpflichtung zur Einhaltung allgemein geltender Datenschutzgesetze, wie z. B. der GDPR, und von Datenschutzstandards, wie z. B. ISO/IEC 27018, dem weltweit ersten internationalen Verhaltenskodex für den Datenschutz in der Cloud, verstärkt.
- Bei Inhalten, auf die über Microsoft 365 Copilot-Plug-Ins zugegriffen wird, kann die Verschlüsselung den programmgesteuerten Zugriff ausschließen und so den Zugriff des Plug-Ins auf die Inhalte beschränken. Weitere Informationen finden Sie unter Konfigurieren von Nutzungsrechten für Azure-Informationsschutz.

Input & Output: Basis ChatGPT

https://openai.com/blog/memory-and-new-controls-for-chatgpt
13.2.2024

“Memory and new controls for ChatGPT
We’re testing the ability for ChatGPT to remember things you discuss to make future chats more helpful. You’re in control of ChatGPT’s memory.

Evolving our privacy and safety standards
Memory brings additional privacy and safety considerations, such as what type of information should be remembered and how it’s used. We’re taking steps to assess and mitigate biases, and steer ChatGPT away from proactively remembering sensitive information, like your health details - unless you explicitly ask it to.”

h_da

Input & Output: Basis ChatGPT

How memory works

As you chat with ChatGPT, you can ask it to remember something specific or let it pick up details itself. ChatGPT's memory will get better the more you use it and you'll start to notice the improvements over time. For example:

- You've explained that you prefer meeting notes to have headlines, bullets and action items summarized at the bottom. ChatGPT remembers this and recaps meetings this way.
- You've told ChatGPT you own a neighborhood coffee shop. When brainstorming messaging for a social post celebrating a new location, ChatGPT knows where to start.
- You mention that you have a toddler and that she loves jellyfish. When you ask ChatGPT to help create her birthday card, it suggests a jellyfish wearing a party hat.
- As a kindergarten teacher with 25 students, you prefer 50-minute lessons with follow-up activities. ChatGPT remembers this when helping you create lesson plans.

You're in control

You can turn off memory at any time (Settings > Personalization > Memory). While memory is off, you won't create or use memories.

h_da

Input & Output

„Microsoft 365 Copilot und öffentliche Webinhalte

Microsoft 365 Copilot Chaterfahrungen können auf öffentliche Webinhalte verweisen, wenn sie auf die Eingabeaufforderung eines Benutzers reagieren. Basierend auf der Eingabeaufforderung des Benutzers bestimmt Microsoft 365 Copilot, ob bing verwendet werden muss, um öffentliche Webinhalte abzufragen, um dem Benutzer eine relevante Antwort zu geben.(…)

Diese Abfrage kann die Daten Ihrer Organisation enthalten, aber das Konto des Benutzers und seine Mandanten-ID sind in der an Bing gesendeten Suchabfrage nicht enthalten.“

.

Input & Output

Hinweis

Die Richtlinieneinstellungen, die die Verwendung optionaler verbundener Erfahrungen in Microsoft 365 Apps steuern, gelten nicht für Microsoft 365 Copilot und öffentliche Webinhalte.

h_da

Input & Output

Hinweis

Wenn Sie Microsoft Copilot für Microsoft 365 verwenden, verlassen die Daten Ihrer organization unter den folgenden Umständen möglicherweise die Microsoft 365-Dienstgrenze:
Wenn Sie Microsoft Copilot mit Graph-geerdetem Chat erlauben, auf Webinhalte zu verweisen. Die an Bing gesendete Abfrage kann die Daten Ihrer organization enthalten.

https://learn.microsoft.com/de-de/microsoft-365-copilot/microsoft-365-copilot-privacy

Eigenangaben Microsoft

https://learn.microsoft.com/de-de/microsoft-365-copilot/microsoft-365-copilot-privacy

Ressourcen nach Rolle

Finden Sie Ressourcen zur Bereitstellung, Nutzung und Skalierung von Copilot für Sie, Ihr Team und Ihre Organisation. Eine Frage haben? Tritt unser ... bei Microsoft 365 Copilot-Community um andere auf der Copilot-Reise zu treffen.


Überblick


Geschäftsbenutzer


Führer


Adoptionsmanager


Computerspezialist


Entwickler

h_da

Input & Output

Zentrale Aufgaben:

- Zugriffsrechte definieren: Rollenmodelle sind entscheidend!
- Copilot denkt technisch, nicht rechtlich:
  - **Einbeziehung von Daten von**
    - **Geschäftsführung,**
    - **Betriebsrat,**
    - **Betriebsärztin,**
    - **DSB,**
    - **BEM,**
    - **Meldestellen etc.**
- Interne Datenbasis klären: Welche Apps, welcher Zeitraum?

Individualarbeitsrecht: Persönliche Leistungserbringung

Leistungserbringung durch KI zulässig?

Mit Einverständnis des AG

§ 106 GewO erlaubt ein Verbot

Nutzung der vom Ag gestellten KI im vorgesehenen Umfang

Konkludente Abbedingung von § 613 S. 1 BGB, „General Purpose"-Scope definieren

Ohne klare Regelung

- Ausgangspunkt § 613 S. 1 BGB: Persönliche Leistungserbringung: Zulässiges Mittel oder Übertragung?
- Gegen Zulässigkeit etwa bei Programmierungen:: Mohn: Dürfen Beschäftigte ChatGPT zur Erledigung ihrer Aufgaben einsetzen? NZA 2023, 538, 539. Anstellung als Programmierer, nicht als Promptograf
- Hinweispflicht des AN nach § 241 II wegen der Risiken für den AG (Fehlerhaftigkeit, Rechte und deren Übertragung, Zeitabrechnung, Leistungsbetrug)

Individualarbeitsrecht:

Einsatz im Personalmanagement u.a.

- Abgleich Bewerbendendaten
- Absage Bewerberinnen (Realakt)
- Weisungen durch KI als Ausübungen des Direktionsrechts, Automatische WE mit Handlungswillen und Erklärungsbewusstsein des AG. Problem: Billiges Ermessen?
- Automatische Anweisungserteilung
- Talent Management
- Compliance- und Leistungsprüfungen
- Automatisierte Abmahnungen / Kündigung

Kollektives Arbeitsrecht:

Einbeziehung Betriebsrat nach BetrVG:

§ 87 Abs.1 Nr. 1:	Betriebliche Ordnung
§ 87a Abs. 1 Nr. 6:	Leistungskontrolle
§ 90 Abs. 1 Nr. 3:	KI-Einsatz
§ 95a Abs. 2:	Erstellung von Richtlinien
§ 80 Abs. 3:	SV-Hinzuziehung

Kollektives Arbeitsrecht:

Einbeziehung Betriebsrat nach BetrVG:

§ 87 Abs.1 Nr. 1: Betriebliche Ordnung

Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb;

§ 87 Abs. 1 Nr. 6: Leistungskontrolle

Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt (geeignet) sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen;

LAG Köln, Beschluss vom 21. Mai 2021 (9 TaBV 28/20)

: Bereits die Einführung von MS 365 ist mitbestimmungspflichtig.

h_da

Kollektives Arbeitsrecht:

Einbeziehung Betriebsrat nach BetrVG:

§ 90 Abs. 1 Nr. 3: KI-Einsatz

1) Der Arbeitgeber hat den Betriebsrat über die Planung

1. von Neu-, Um- und Erweiterungsbauten von Fabrikations-, Verwaltungs- und sonstigen betrieblichen Räumen,

2. von technischen Anlagen,

3. von Arbeitsverfahren und Arbeitsabläufen einschließlich des Einsatzes von Künstlicher Intelligenz oder

4. der Arbeitsplätze

rechtzeitig unter Vorlage der erforderlichen Unterlagen zu unterrichten.

(2) Der Arbeitgeber hat mit dem Betriebsrat die vorgesehenen Maßnahmen und ihre Auswirkungen auf die Arbeitnehmer, insbesondere auf die Art ihrer Arbeit sowie die sich daraus ergebenden Anforderungen an die Arbeitnehmer so rechtzeitig zu beraten, dass Vorschläge und Bedenken des Betriebsrats bei der Planung berücksichtigt werden können. Arbeitgeber und Betriebsrat sollen dabei auch die gesicherten arbeitswissenschaftlichen Erkenntnisse über die menschengerechte Gestaltung der Arbeit berücksichtigen

Kollektives Arbeitsrecht:

§ 95 Auswahlrichtlinien

(1) Richtlinien über die personelle Auswahl bei Einstellungen, Versetzungen, Umgruppierungen und Kündigungen bedürfen der Zustimmung des Betriebsrats. Kommt eine Einigung über die Richtlinien oder ihren Inhalt nicht zustande, so entscheidet auf Antrag des Arbeitgebers die Einigungsstelle. Der Spruch der Einigungsstelle ersetzt die Einigung zwischen Arbeitgeber und Betriebsrat.

(2) In Betrieben mit mehr als 500 Arbeitnehmern kann der Betriebsrat die Aufstellung von Richtlinien über die bei Maßnahmen des Absatzes 1 Satz 1 zu beachtenden fachlichen und persönlichen Voraussetzungen und sozialen Gesichtspunkte verlangen. Kommt eine Einigung über die Richtlinien oder ihren Inhalt nicht zustande, so entscheidet die Einigungsstelle. Der Spruch der Einigungsstelle ersetzt die Einigung zwischen Arbeitgeber und Betriebsrat.

(2a) Die Absätze 1 und 2 finden auch dann Anwendung, wenn bei der Aufstellung der Richtlinien nach diesen Absätzen Künstliche Intelligenz zum Einsatz kommt.

(3) Versetzung im Sinne dieses Gesetzes ist die Zuweisung eines anderen Arbeitsbereichs, die voraussichtlich die Dauer von einem Monat überschreitet, oder die mit einer erheblichen Änderung der Umstände verbunden ist, unter denen die Arbeit zu leisten ist. Werden Arbeitnehmer nach der Eigenart ihres Arbeitsverhältnisses üblicherweise nicht ständig an einem bestimmten Arbeitsplatz beschäftigt, so gilt die Bestimmung des jeweiligen Arbeitsplatzes nicht als Versetzung.

Kollektives Arbeitsrecht:

Einbeziehung Betriebsrat nach BetrVG:

§ 80 Abs. 3: SV-Hinzuziehung

(3) Der Betriebsrat kann bei der Durchführung seiner Aufgaben nach näherer Vereinbarung mit dem Arbeitgeber Sachverständige hinzuziehen, soweit dies zur ordnungsgemäßen Erfüllung seiner Aufgaben erforderlich ist. Muss der Betriebsrat zur Durchführung seiner Aufgaben die Einführung oder Anwendung von Künstlicher Intelligenz beurteilen, gilt insoweit die Hinzuziehung eines Sachverständigen als erforderlich. Gleiches gilt, wenn sich Arbeitgeber und Betriebsrat auf einen ständigen Sachverständigen in Angelegenheiten nach Satz 2 einigen.

Kollektives Arbeitsrecht:

§ 111 Betriebsänderungen

In Unternehmen mit in der Regel mehr als zwanzig wahlberechtigten Arbeitnehmern hat der Unternehmer den Betriebsrat über geplante Betriebsänderungen, die wesentliche Nachteile für die Belegschaft oder erhebliche Teile der Belegschaft zur Folge haben können, rechtzeitig und umfassend zu unterrichten und die geplanten Betriebsänderungen mit dem Betriebsrat zu beraten. Der Betriebsrat kann in Unternehmen mit mehr als 300 Arbeitnehmern zu seiner Unterstützung einen Berater hinzuziehen; § 80 Abs. 4 gilt entsprechend; im Übrigen bleibt § 80 Abs. 3 unberührt. Als Betriebsänderungen im Sinne des Satzes 1 gelten

1. Einschränkung und Stilllegung des ganzen Betriebs oder von wesentlichen Betriebsteilen,
2. Verlegung des ganzen Betriebs oder von wesentlichen Betriebsteilen,
3. Zusammenschluss mit anderen Betrieben oder die Spaltung von Betrieben,
4. grundlegende Änderungen der Betriebsorganisation, des Betriebszwecks oder der Betriebsanlagen,
5. Einführung grundlegend neuer Arbeitsmethoden und Fertigungsverfahren.

Kollektives Arbeitsrecht:

Einbeziehung Betriebsrat

Use Case vorbereiten, insbesondere um Zugriffsberechtigungen und Anwendungsfälle zu klären.

h_da

Diskriminierungsfragen / AGG

§ 7 AGG Benachteiligungsverbot

(1) Beschäftigte dürfen nicht wegen eines in § 1 genannten Grundes benachteiligt werden; dies gilt auch, wenn die Person, die die Benachteiligung begeht, das Vorliegen eines in § 1 genannten Grundes bei der Benachteiligung nur annimmt.
(2) Bestimmungen in Vereinbarungen, die gegen das Benachteiligungsverbot des Absatzes 1 verstoßen, sind unwirksam.
(3) Eine Benachteiligung nach Absatz 1 durch Arbeitgeber oder Beschäftigte ist eine Verletzung vertraglicher Pflichten.

§ 22 AGG Beweislast

Wenn im Streitfall die eine Partei Indizien beweist, die eine Benachteiligung wegen eines in § 1 genannten Grundes vermuten lassen, trägt die andere Partei die Beweislast dafür, dass kein Verstoß gegen die Bestimmungen zum Schutz vor Benachteiligung vorgelegen hat.

Diskriminierungsfragen

§ 19 Zivilrechtliches Benachteiligungsverbot

(1) Eine Benachteiligung aus Gründen der Rasse oder wegen der ethnischen Herkunft, wegen des Geschlechts, der Religion, einer Behinderung, des Alters oder der sexuellen Identität bei der Begründung, Durchführung und Beendigung zivilrechtlicher Schuldverhältnisse, die

1. typischerweise ohne Ansehen der Person zu vergleichbaren Bedingungen in einer Vielzahl von Fällen zustande kommen (Massengeschäfte) oder bei denen das Ansehen der Person nach der Art des Schuldverhältnisses eine nachrangige Bedeutung hat und die zu vergleichbaren Bedingungen in einer Vielzahl von Fällen zustande kommen oder
2. eine privatrechtliche Versicherung zum Gegenstand haben,

ist unzulässig.

Urheberrecht oder sonstige Schutzrechte an den Ergebnissen? – Lizenzierungsfolgen

Gesetzlicher Schutz? Steinalte IT-Probleme

- § 2 UrhG Werk ohne menschliche Schöpfung?
  - Vorbereitende Anteile?
  - Keine Übernahme von Strings
- § 87a UrhG? -> Trainingsdatenbank
- § 69a UrhG -> Programmierung
- GeschGehG -> Keine Geheimhaltungsmaßnahmen

h_da

Datenschutzfragen: Datenverarbeitung bei Eingabe und Ergebnisausgabe

- Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen (Art. 4 Ziff. 1 DS-GVO)
- Art. 6 I f DSGVO ? § 26 BDSG
- Art. 9 Abs. 2 e) DSGVO Rechtsgrundlage für die Verarbeitung öff. zugänglicher Daten?
  - Offensichtlich von betroffener Person selbst öffentlich gemacht?
  - Durch Bots erkennbar? Social Media Defaults?
- Nach Art. 10 Abs. 5 der KI-VO-E dürfen KI-Anbieter personenbezogene Daten verarbeiten, soweit dies für die Beobachtung, Erkennung und Korrektur von (Parl: negativen) Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist.
- https://www.lda.bayern.de/media/ki_checkliste.pdf
- https://www.datenschutzkonferenz-online.de/media/pm/23-11-29_DSK-Pressemitteilung_KI-Regulierung.pdf
- https://datenschutz-hamburg.de/news/checkliste-zum-einsatz-llm-basierter-chatbots

h_da

Aufgaben

Details: https://fbgw.h-da.de/forschung/chatgpt-dall-e-co/vorgehensmodell-ki-einfuehrung

Datenschutzkonformität eines Tools

- Datenschutzfolge-abschätzung
- Einbeziehung DSB
- Einsatzszenario
- Auftragsverarbeitung
- Auslandsdatentransfer

Datenschutzkonformität des Einsatzes

- Datenkombinationen
- Sensible Daten
- Datenoffenbarung
- KI-Entscheidungen
- Rechtsgrundlagen
- Rollenmodelle
- Weisungen durch KI ja, rechtlich wirksame Entscheidungen: Nein

h_da

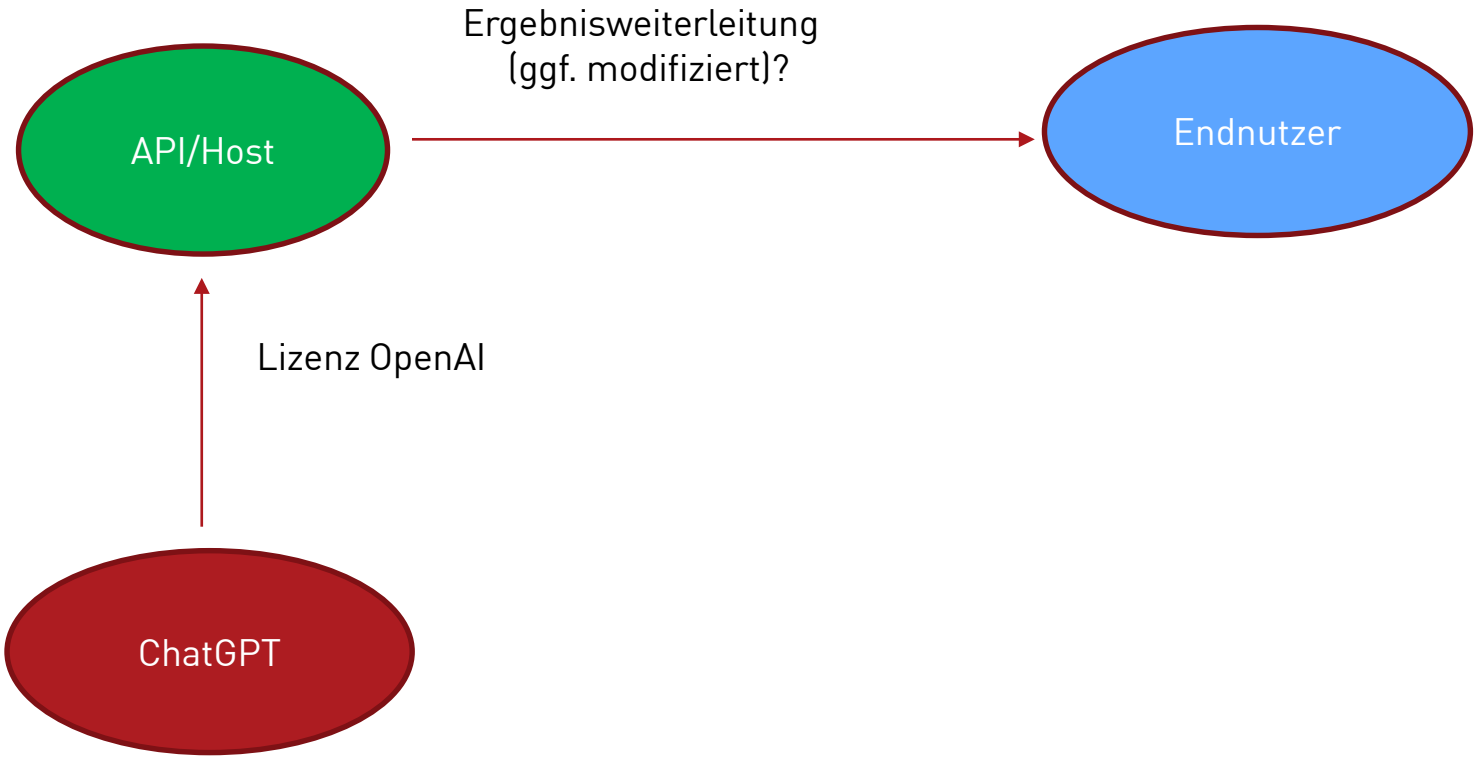
Aufgaben

Orientierungshilfen-Navigator KI & Datenschutz (ONKIDA)

https://www.baden-wuerttemberg.datenschutz.de/onkida/

	A. EDPS Guidelines on generative AI and the EUDPR (2024, PDF) *Datenverarbeitung durch EU-Organe*	B. Report der EDSA Taskforce ChatGPT (2024, PDF)	C. DSK: Orientierungshilfe zu KI und Datenschutz (2024, PDF)	D. LfDI BW: Rechtsgrundlagen zum Einsatz von KI (2023)	E. BayLDA: Checkliste Datenschutzkonforme KI (2024, PDF)	F. Hamburger BfDI: Checkliste zum Einsatz LLM-basierter Chatbots (2023, PDF)	G. CNIL: Recommendations on the development of AI systems („How-to sheets") (2024)	H. DSB Österreich: FAQ KI und Datenschutz (2024)	I. DSK: Positionspapier zu TOM bei Entwicklung und Betrieb von KI-Systemen (2019, PDF)	J. DSK: Ham Erklärung PDF)
1. Grundsatz der Datenrichtigkeit Art. 5 I lit. d) DSGVO	(+) S. 15 f. (Art. 4 I lit. d) VO 2018/1725)	(+) Rn. 29 ff. sowie im Fragebogen im Annex, S. 11	(+/–) Recht auf Berichtigung Rn. 27, Überprüfung der Richtigkeit der Ergebnisse Rn. 64 f.	(–)	(+/–) Recht auf Berichtigung, S. 6, 10	(+/–) Überprüfung der Richtigkeit des Ergebnisses S. 4	(+/–) „data cleaning", „monitoring and updating" Sheet 7	(+)	(–)	(–)
2. Grundsatz der Datenminimierung Art. 5 I lit. c) DSGVO **Zweckbindungsgrundsatz** Art. 5 I lit. b) DSGVO	(+) Datenminimierung: S. 14 (Art. 4 I lit. c) VO 2018/1725) (+/–) Zweckbindung: nur sehr indirekt („consistent with original purpose"), S. 12	(+/–) nur im Rahmen des Fragebogens im Annex, S. 10	(+) Zweckbindung Rn. 1 f.	(+/–) Berücksichtigung Datenminimierung bei Art. 6 I lit. f DSGVO (S. 17) u. § 13 LDSG BW (S. 25) (+) Zweckänderung S. 15	(+/–) Zweckbindung nur eher indirekt S. 6, 8, 11 (Checkliste)	(–)	(+) Sheet 2, Datenminimierung auch Sheet 6, Zweckkompatibilität auch Sheet 4 (2/2)	(+)	(+) Datenminimierung S. 9, 14, 17 (+) Zweckbindung S. 6 f., 7 (Fragebogen), 8, 9, 14, 17	(+) Datenmini (+) Zweckbinc
3. Personenbezug Art. 4 Nr. 1 DSGVO	(+) S. 7 (Art. 3 Nr. 1 VO 2018/1725)	(–)	(+) Rn. 4 ff., 7 f., 48 ff.	(+) insbes. S. 6	(+) S. 4, 5, 9,10, 11 (Checklisten)	(+) S. 2 f. *vgl. auch Hamburger Thesen zum Personenbezug in Large Language Models v. 15.7.2024*	(+) Introduction	(–)	(+) S. 15 kurzer Satz im Zusammenhang mit Vertraulichkeit beim Training	(–)
4. Rechtsgrundlagen für die Datenverarbeitung Art. 6 I u. 9 II DSGVO	(+) S. 11 ff. (Art. 5 und 10 II VO 2018/1725)	(+) Rn. 13 ff., ebenso im Fragebogen S. 12 f.	(+) Rn. 9 ff. (zudem Verweis auf Positionspapier LfDI BW), Rn. 62 (im Zusammenhang mit sensiblen Daten)	(+) insbes. S. 11 ff.	(+) S. 4 und 9 (Checklisten)	(+) S. 2 (indirekt im Zusammenhang mit Personenbezug) und S. 4 (im Zusammenhang mit Diskriminierung)	(+) Sheet 4 (1/2 und 2/2), Sheet 8 (in consultation)	(+/–) nur allgemeine Bezugnahme	(+/–) vereinzelt kurze Bezugnahmen, dass es einer Rechtsgrundlage bedarf	(–)
5. (Mit–)Verantwortlichkeit Art. 26 (und 28) DSGVO	(+) S. 6	(+/–) Rn. 23 ff. in Zusammenhang mit Fairness-Prinzip, „Abwälzung" der Verantwortlichkeit auf betroffene Personen; im Rahmen des Fragebogens S. 14	(+) Rn. 32 ff.	(+) S. 9 ff.	(+) S. 9	(–)	(+) Sheet 3	(–)	(+/–) indirekt: Klärung der Zugriffsmöglichkeiten von Cloud-Anbietern S. 16; „Rollen- und Berechtigungskonzept" S. 15,18,19	(+/–) S. 4 (nu Bezugnahme der Verantwo
6. Transparenzgebot und Informationspflichten Art. 5 I lit. a und 12 ff. DSGVO	(+) S. 17 (Art. 14 VO 2018/1725)	(+) Rn. 27 f., ebenso im Fragebogen S. 13	(+) Rn. 21 ff.	(+) S. 12 (im Zusammenhang mit informierter Einwilligung)	(+) Transparenz S. 7 (als Teil des „Datenschutz-Risikomodells") (+) Infopflichten S. 5 (Checkliste)	(–)	(+) Sheet 2, Dokumentation in Sheet 7	(+)	(+) S. 5, 11 ff., 16 f.	(+) S. 3
7. Auskunftsanspruch Art. 15 DSGVO **Recht auf Löschung** Art. 17 DSGVO	(+/–) allgemein Betroffenenrechte S. 22	(+) allgemein Betroffenenrechte Rn. 32 ff.	(+) nur Recht auf Löschung Rn. 26, 28 f.; „weitere Betroffenenechte" Rn. 30	(+) nur Recht auf Löschung S. 12	(+) Auskunftsanspruch S. 5, 10 (Checkliste), Recht auf Löschung S. 6, 10 (Checkliste)	(–)	(–)	(+/–) nur allgemeine Bezugnahme auf Betroffenenrechte	(+) Auskunftsanspruch, S. 7; Betroffenenrechte allgemein S. 18 (in einem Satz)	(–)
8. Automatisierte Entscheidungen und Profiling Art. 22 DSGVO	(+) S. 18 (Art. 24 VO 2018/1725)	(–)	(+) Rn. 12 ff.	(–)	(–)	(+) S. 22	(–)	(+)	(+) S. 5 (mehr oder weniger), S. 14 (Bezugnahme in einem Satz, indirekt), S. 18	(+) S. 3
9. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen Art. 25 DSGVO	(+) S. 9 (Art. 27 VO 2018/1725)	(+) Rn. 7 knappe Bezugnahme; Rn. 35 im Zusammenhang mit Betroffenenrechten	(+) Rn. 43	(+/–) S. 7 (Bewertung Personenbezug), S. 18 Fn. 57 (Berücksichtigung bei Art. 6 I lit. f DSGVO)	(+), S. 7 (nur ein knapper Satz)	(–)	(+) Sheet 6 (Vorschrift wird nicht direkt genannt, aber Konzept DPbD wird beschrieben), Sheet 7	(–)	(+) S. 7 (analog?)	(+) S. 2, 4
10. Datenschutz-Folgenabschätzung Art. 35 DSGVO	(+) S. 9 f. (Art. 39 u. 89 VO 2018/1725)	(+/–) nur im Rahmen des Fragebogens im Annex, S. 11	(+) Rn. 38 ff.	(–)	(+) S. 4, 6, 9, 11 (Checklisten), S. 7	(+) S. 2	(+) Sheet 5	(–)	(+) S. 5	(+) S. 4

Einbindung durch Dritte



h_da

Vertragliche Entscheidungen durch KI

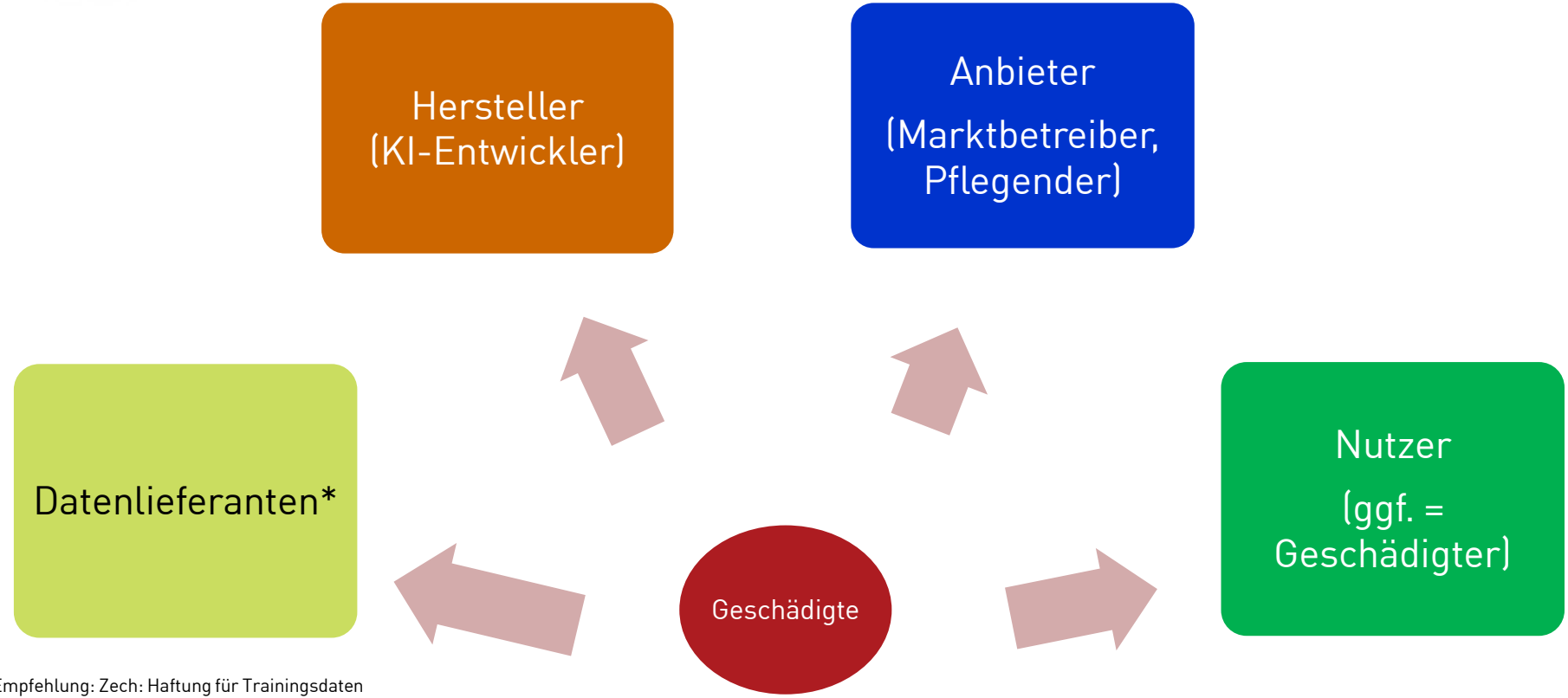
- Anwendbarkeit §§ 119, 120 BGB?
- Computerklärung / Warenwirtschaftssysteme?
- Änderung durch Autonomie und Opazität?
- Möglicherweise kein Fall der Fortwirkung einer menschlichen Fehleingabe

Einbindung durch Dritte

- Datenschutz: gemeinsame Verantwortlichkeit Art. 26 DSGVO
- Bisher § 10 TMG? Host Providing?
- TDDDG / Art. 13 DSGVO / Transparente Information über Einbindung
- Störerhaftung?
- NetzDG
- Kontrollpflichten / Mitwirkungspflichten laut Open AI
- 22 DSGVO / Scoring: HITL
- Arztberuf/ Anwaltsberuf/ höchstpersönliche Leistungserbringung
- Spezialgesetze / Medizinprodukte / Kreditwesen etc.
- DSA/DMA/DDG

h_da

Haftung: Beteiligte



*Empfehlung: Zech: Haftung für Trainingsdaten Künstlicher Intelligenz, NJW 2022, 502

h_da

Haftung: Auszug der Verantwortlichkeiten der Beteiligten

Datenlieferanten	Hersteller (KI-Entwickler)	Anbieter (Marktbetreiber, Pflegender)	Nutzer (ggf. = Geschädigter)

•Datenqualität
•Datenherkunft
•Metadaten
	•Programmierung
	•Training
	  •Prozess
	  •Datenqualität
	•Überwachung
		•Scope der Nutzung
		•Nutzerhinweise
		•Beschränkung der Autonomie?
		•Vorgaben TMG, Störerhaftung, DSA, DMA etc.
		•Beobachtung
			•Instruktionsbeachtung
			•Zweckbegrenzung
			•Datenbasis beachten

Haftung für falsche Ergebnisse oder Missbrauch?

Sollzustand:

Studie zur Zuverlässigkeit von ChatGPT 3 / Zustimmungsrate zu Falschbehauptungen bei 26% / Preprint University of Waterloo, Canada

https://arxiv.org/pdf/2306.06199.pdf

Der Copilot von Microsoft liefert angeblich nicht nur falsche Umfragewerte und Wahltermine, sondern erfindet auch Skandale über Politiker.

https://www.golem.de/news/microsoft-copilot-liefert-wohl-falsche-infos-ueber-politische-wahlen-2312-180391.html

Unerkannte KI-Einbindung?

Kopierer als (fehlerhafter) OCR-Scanner

https://www.spiegel.de/netzwelt/apps/blogger-schreibt-bug-xerox-scankopierern-sollen-zahlen-vertauschen-a-914897.html, zuletzt abgerufen am 21.02.2023.

Haftung nach aktuellem (nationalem) Recht

BGB-AT: Anfechtbarkeit von KI-“Entscheidungen“?

Analog zum Warenwirtschaftssystem §§ 119, 120 BGB

Vertraglich

- §§ 276, 280 BGB, Beweislastumkehr
- § 254 BGB
- Mitwirkungspflichten und Haftungsausschlüsse
- Abweichung von wesentlichen Grundgedanken welcher gesetzlichen Regelung?
- AGB-Recht: Grenzen der Haftungseinschränkung
- Was ist der typische vorhersehbare Schaden?

Haftung nach aktuellem (nationalem) Recht

Gesetzlich

- § 823 I BGB Produzentenhaftung (Vermögensschaden nicht abgedeckt…)
  Konstruktionsfehler, Fabrikationsfehler, Instruktionsfehler, Produktbeobachtungsfehler
- § 823 II BGB i.V.m. Schutzgesetzen ?
- § 830 I S. 2 BGB Mehrere Mittäter / Fehlende Ermittlungsmöglichkeit
- ProdHG (KI-Anbieter als (Teil-) hersteller, Produkt, Fehlerhaftigkeit, Verletzungshandlung, Kausalität)
  Verschuldensvermutung bei Konstruktions-, Fabrikations- oder Instruktionsfehler
- Spezialgesetze nach Einsatzzweck, Medizinprodukte, KUG…

Haftung nach aktuellem (nationalem) Recht

Sorgfaltspflichtverletzungen der Akteure

- Verletzung von Standards oder Fehler bei Entwicklung, Training, Überwachung.
- Einsatz von KI generell unverantwortlich?
  - Genügt geringere Fehlerquote als bei Menschen?
  - Beachtung der geltenden technischen Standards
- Einsatz dann nie sorgfaltswidrig?
- Autonomierisiko immer beim Nutzer?

BGHZ 80, 186:

Berechtigte Sicherheitserwartungen des Verkehrs und der zumutbare Aufwand: Welche Bedrohung von Rechtsgütern Dritter besteht, wie hochrangig sind die bedrohten Rechtsgüter sind.

Haftung: ProduktthaftRL Entwurf

Artikel 4 Begriffsbestimmungen

Für die Zwecke dieser Richtlinie gelten folgende Begriffsbestimmungen:

(1)„Produkt“ bezeichnet alle beweglichen Sachen, auch wenn diese in eine andere bewegliche oder unbewegliche Sache integriert sind. Dazu zählen auch Elektrizität, digitale Bauunterlagen und **Software.**

[….]

(3)„Komponente“ bezeichnet jeden materiellen oder **immateriellen Gegenstand** und jeden verbundenen **Dienst**, der vom Hersteller eines Produkts oder unter Kontrolle des Herstellers in das Produkt integriert oder mit dem Produkt verbunden wird.

(4)„Verbundener Dienst“ bezeichnet einen **digitalen Dienst, der so in ein Produkt integriert oder so mit ihm verbunden ist, dass das Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte;**

(5)**„Kontrolle des Herstellers“** bezeichnet die Tatsache, dass der Hersteller eines Produkts a) die Integration, Verbindung oder Lieferung einer Komponente einschließlich Software-Updates oder -Upgrades durch einen Dritten oder b) die Änderung des Produkts genehmigt.

h_da

Haftung: KI-Haftungsrichtlinie

Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung)
COM/2022/496 final

Art. 1
a) die Offenlegung von Beweismitteln betreffend **Hochrisiko-KI-Systeme** mit dem Ziel, es einem Kläger zu ermöglichen, **einen außervertraglichen verschuldensabhängigen zivilrechtlichen Schadensersatzanspruch** zu begründen;

b) die Beweislast bei der Geltendmachung außervertraglicher verschuldensabhängiger zivilrechtlicher Ansprüche vor nationalen Gerichten in Bezug auf Schäden, die durch ein KI-System verursacht wurden.

Haftung: KI-Haftungsrichtlinie

Art. 4 Widerlegbare Vermutung eines ursächlichen Zusammenhangs im Fall eines Verschuldens

(1)

Vorbehaltlich der in diesem Artikel festgelegten Anforderungen **vermuten die nationalen Gerichte für die Zwecke der Anwendung der Haftungsvorschriften auf einen Schadensersatzanspruch einen ursächlichen Zusammenhang zwischen dem Verschulden des Beklagten und dem vom KI-System hervorgebrachten Ergebnis** oder aber der Tatsache, dass das KI-System kein Ergebnis hervorgebracht hat, **wenn alle folgenden Bedingungen** erfüllt sind:

h_da

Archivierung

Konsequenzen für die Archivierung? Originär digital erstellte Unterlagen….

257 HGB

(1) Jeder Kaufmann ist verpflichtet, die folgenden Unterlagen geordnet aufzubewahren:

1. Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,

2. die empfangenen Handelsbriefe,

3. Wiedergaben der abgesandten Handelsbriefe,

4. Belege für Buchungen in den von ihm nach § 238 Abs. 1 zu führenden Büchern (Buchungsbelege).

h_da

Archivierung

Konsequenzen für die Archivierung? Originär digital erstellte Unterlagen….

257 HGB

3) Mit Ausnahme der Eröffnungsbilanzen und Abschlüsse können die in Absatz 1 aufgeführten Unterlagen auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, daß die Wiedergabe oder die Daten

1. mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden,

2. während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können.

Sind Unterlagen auf Grund des § 239 Abs. 4 Satz 1 auf Datenträgern hergestellt worden, können statt des Datenträgers die Daten auch ausgedruckt aufbewahrt werden; die ausgedruckten Unterlagen können auch nach Satz 1 aufbewahrt werden.

h_da

Archivierung

Konsequenzen für die Archivierung? Originär digital erstellte Unterlagen….

239 HGB

(2) Die Eintragungen in Büchern und die sonst erforderlichen Aufzeichnungen müssen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden.

(3) Eine Eintragung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, daß der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiß läßt, ob sie ursprünglich oder erst später gemacht worden sind.

(4) Die Handelsbücher und die sonst erforderlichen Aufzeichnungen können auch in der geordneten Ablage von Belegen bestehen oder auf Datenträgern geführt werden, soweit diese Formen der Buchführung einschließlich des dabei angewandten Verfahrens den Grundsätzen ordnungsmäßiger Buchführung entsprechen. Bei der Führung der Handelsbücher und der sonst erforderlichen Aufzeichnungen auf Datenträgern muß insbesondere sichergestellt sein, daß die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können. Absätze 1 bis 3 gelten sinngemäß.

h_da

Archivierung

Konsequenzen für die Archivierung? Originär digital erstellte Unterlagen….

147 AO

§ 147 Ordnungsvorschriften für die Aufbewahrung von Unterlagen

(1) Die folgenden Unterlagen sind geordnet aufzubewahren:

1. Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,

2. die empfangenen Handels- oder Geschäftsbriefe,

3. Wiedergaben der abgesandten Handels- oder Geschäftsbriefe,

4. Buchungsbelege,

4a. Unterlagen nach Artikel 15 Absatz 1 und Artikel 163 des Zollkodex der Union,

5. sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind.

Archivierung

Konsequenzen für die Archivierung? Originär digital erstellte Unterlagen….
147 AO

§ 147 Ordnungsvorschriften für die Aufbewahrung von Unterlagen

(7) Die Verarbeitung und Aufbewahrung der nach Absatz 6 zur Verfügung gestellten Daten ist auch auf mobilen Datenverarbeitungssystemen der Finanzbehörden unabhängig von deren Einsatzort zulässig, sofern diese unter Berücksichtigung des Stands der Technik gegen unbefugten Zugriff gesichert sind. Die Finanzbehörde darf die nach Absatz 6 zur Verfügung gestellten und gespeicherten Daten bis zur Unanfechtbarkeit der die Daten betreffenden Verwaltungsakte auch auf den mobilen Datenverarbeitungssystemen unabhängig von deren Einsatzort aufbewahren.

Archivierung

Konsequenzen für die Archivierung? Originär digital erstellte Unterlagen….

GOBD

GOBD-Änderungen 2024:

https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/AO-Anwendungserlass/2024-03-11-aenderung-gobd.pdf?__blob=publicationFile&v=4

„167 Datenüberlassung (Z3) Die Finanzbehörde kann ferner verlangen, dass ihr die aufzeichnungs- und aufbewahrungspflichtigen Daten, einschließlich der jeweiligen Meta-, Stamm- und Bewegungsdaten sowie der internen und externen Verknüpfungen (z. B. zwischen den Tabellen einer relationalen Datenbank), und elektronische Dokumente und Unterlagen in einem maschinell lesbaren und auswertbaren Format zur Auswertung überlassen werden. Dies kann z. B. auf einem Datenträger oder durch Zurverfügungstellung der Daten über eine Datenaustauschplattform erfolgen, für die die Finanzbehörde einen Zugang eröffnet hat (§ 87a Absatz 1 AO). Dieses Verlangen kann gem. § 197 Absatz 3 AO mit der Prüfungsanordnung innerhalb einer angemessenen Frist bereits vor dem Beginn der Prüfung geltend gemacht werden. Die Finanzbehörde ist nicht berechtigt, selbst Daten aus dem DV-System herunterzuladen oder Kopien vorhandener Datensicherungen vorzunehmen.

Praxishinweise

Neben den Formalia (https://fbgw.h-da.de/forschung/chatgpt-dall-e-co/vorgehensmodell-ki-einfuehrung)
steht Folgendes im Fokus:

- **Freigabe aller Office-Programme?**
- **Möglichkeit von Zugriffsrechtsdefinitionen? Promptberechtigungskonzept?**
- **Kollision mit Privatnutzungsmöglichkeiten**
- **Herausnahme sensibler Daten aus dem Pool?**

Checklisten zur Einführung: Copilot-recht.de

h_da

Praxishinweise

Wir implementieren bereits mehrere Arten des Schutzes, um zu verhindern, dass Kunden Microsoft 365-Dienste und -Anwendungen gefährden oder nicht autorisierten Zugriff auf andere Mandanten oder das Microsoft 365 System selbst erhalten. Hier sind einige Beispiele für diese Formen des Schutzes:

Die logische Isolation von Kundeninhalten innerhalb der einzelnen Mandanten für Microsoft 365-Dienste wird durch Microsoft Entra Autorisierung und rollenbasierte Zugriffssteuerung erreicht. Weitere Informationen finden Sie unter Microsoft 365 Isolationssteuerelemente.

https://learn.microsoft.com/de-de/microsoft-365-copilot/microsoft-365-copilot-privacy

https://techcommunity.microsoft.com/t5/copilot-for-microsoft-365/how-to-prepare-for-microsoft-365-copilot/ba-p/3851566

Checklisten zur Einführung: Copilot-recht.de

Praxishinweise: Prozess KI-Einführung

Prozess zur rechtskonformen Einführung / Einsatz von KI / Copilot & Co im Unternehmen

Der KI-Einsatz sollte sorgfältig geplant sein, wichtig ist vor allem Transparenz sowohl hinsichtlich der Einbeziehung der KI, als auch der Qualitätssicherung der Trainingsdaten und Ergebnisse sowie der Einbindung von API-Schnittstellen. Ein verstärkter Einsatz in den Feldern ECM / DMS, ERP und E-Mail-Management ist zu beobachten, eine Ausweitung auf andere Felder – weit über Textgenerierungsfunktionen hinaus - steht in vielen Unternehmen bevor.

Neben zahlreichen datenschutzrechtlichen Fragen sind etliche Themen im Bereich des Arbeitsrechts zu beachten, die hier nicht vollständig abgebildet werden können. Daneben kann es bereichsspezfiische Vorgaben geben*.

Es sollte ein Prozess zur rechtlichen KI-Einbindung erstellt werden, der abhängig von Art des Tools und des Einsatzzwecks klare Meilensteine zu unter Anderem folgenden Punkten enthält:

*AT 8.2 MaRisk Änderungen betrieblicher Prozesse oder Strukturen 1 Vor wesentlichen Veränderungen in der Aufbau- und Ablauforganisation sowie in den IT-Systemen hat das Institut die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren. In diese Analysen sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten. Im Rahmen ihrer Aufgaben sind auch die Risikocontrolling-Funktion, die ComplianceFunktion und die Interne Revision zu beteiligen.

h_da

Praxishinweise: Prozess KI-Einführung

1. **Definition der Zwecke des KI-Einsatzes / juristische Vorklärung**

a. Abklärung juristisch bedeutsamer Vorfragen:

1. Ist es erforderlich, bei den Prompts (Dateneingaben) personenbeziehbare Angaben zu machen?
2. Könnten die Prompts Rückschlüsse auf Geschäftsgeheimnisse (Patententwürfe etc.) zulassen?
3. Werden die KI-Ergebnisse auch Dritten – eventuell automatisiert – zur Verfügung gestellt? Können Dritte (z.B. Kunden) auch Prompts eingeben?
4. Umfasst der Einsatzzweck verbotene Systeme nach Art. 5 KI-Verordnung („KI-VO“) oder Hochrisikosysteme nach Art. 6 KI-VO i.V.m. Anhang III KI-VO?
5. Hat der KI-Einsatz Auswirkungen auf bestehende Arbeitsplätze? Könnte der KI-Einsatz geeignet sein, die Leistung der Beschäftigten zu überwachen?
6. Sind die Schnittstellen zu nichtlokaler KI IT-sicherheitszertifiziert / KRITIS-tauglich?
7. Werden alle vom KI-System verarbeiteten Daten in Deutschland verarbeitet, ohne dass Muttergesellschaften der KI oder Subunternehmer des KI-Anbieters in den USA oder sonst außerhalb der EU ansässig sind?
8. Beim Einsatz im HR-Bereich: Kann das System mittelbare Beeinträchtigungen nach Art. 3 Abs. 2 AGG ausschließen?

h_da

Praxishinweise: Prozess KI-Einführung

1. **Definition der Zwecke des KI-Einsatzes / juristische Vorklärung**

b. Von den Ergebnissen abhängige Klärung

1. ob die KI einen Datenabfluss nach außen zulässt / eine lokale Begrenzung der Prompt-Speicherung möglich ist,
2. die KI-Nutzung daneben auf nicht- Geschäftsgeheimnisgesetz-relevante Bereiche begrenzt werden kann,
3. ob Mechanismen eingerichtet werden können, die eine Reaktion auf Missbrauch durch oder zu Lasten Dritter begrenzen,
4. ob die KI den Vorgaben der KI-VO entspricht,
5. ob der Betriebsrat frühzeitig einbezogen wurde oder sich eine Eignung zur Leistungskontrolle der Beschäftigten vermeiden lässt,
6. welche Maßnahmen zur IT-Sicherheit getroffen werden müssen, um Cybersicherheitsprobleme zu verhindern,
7. welche Maßnahmen getroffen werden müssen, um einen Drittstaatentransfer personenbezogener Daten zu gestatten.

h_da

Praxishinweise: Prozess KI-Einführung

2. Einbeziehung Betriebsrat / Personalrat

Nach § 90 Abs. 1 BetrVG Nr. 3 hat der Arbeitgeber den Betriebsrat über die Planung von Arbeitsverfahren und Arbeitsabläufen einschließlich des Einsatzes von Künstlicher Intelligenz rechtzeitig unter Vorlage der erforderlichen Unterlagen zu unterrichten, gleiches gilt bei Betriebsänderungen mit wesentlichen Nachteilen für die Belegschaft nach § 111 BetrVG.

Soweit KI bei der Erstellung von Richtlinien über die personelle Auswahl bei Einstellungen, Versetzungen, Umgruppierungen und Kündigungen genutzt wird, bedarf dies nach § 95a Abs. 2 BetrVG der Zustimmung des Betriebsrats, ggf. ist die Einigungsstelle hinzuzuziehen. Der Betriebsrat kann ggf. nach § 80 Abs. 3 BetrVG einen Sachverständigen hinzuziehen.

Soweit der KI-Einsatz geeignet sein kann, die Leistung der Beschäftigten zu überwachen, hat der Betriebsrat nach § 87a Abs. 1 Nr. 6 BetrVG über die Einführung mitzubestimmen. Gleiches gilt bei der Regelung der Ordnung im Betrieb nach § 87 Abs.1 Nr. 1 BetrVG. Den Betriebsrat daher frühzeitig bei den Planungen zu Privacy by Design, Privacy by Default einbeziehen, je nach Einsatzweck Betriebsvereinbarung vorbereiten. Daneben sind Informationspflichten gegenüber Beschäftigten und ggf. auch - je nach Unternehmensgröße und -organisation dem Aufsichtsrat / Wirtschaftsausschuss (§ 106 BetrVG) zu berücksichtigen.

Praxishinweise: Prozess KI-Einführung

3. Datenschutz

b. Prüfung der Vorgaben von DSGVO, TDDDG, BDSG

8. Klärung, ob das Tool in seiner technischen Struktur (IP-Erfassung, Anbindung der Software, Verarbeitung der Eingaben) datenschutzkonform ist (ggf. TTDSG bei Webanbindung).
9. Abschluss eines Controller-to-Controller-Vertrags (meist kein Auftragsverarbeitungsvertrag, da der KI-Anbieter auch eigene Interessen verfolgt bei der Verarbeitung der erhobenen/übermittelten Daten), alternativ AVV (insb. wenn Abfluss personenbeziehbarer Daten ausgeschlossen (s.o. 1.a.i), alternativ ggf. gemeinsame Verarbeitung nach Art. 26 DSGVO).
10. Bei Auslandsdatenübertragung Prüfung des datenschutzkonformen Einsatzes (je nach Land Angemessenheitsbeschluss / DPF USA vom 10.07.2023, siehe **www.dataprivacyframework.gov/s/)**, SCCs etc., jeweiligen Stand der Klagen von NOYB im Auge behalten)
11. Zu Einzelfragen des Datenschutzes sind unter Anderem die Orientierungshilfe der Datenschutzkonferenz „Künstliche Intelligenz und Datenschutz“ Version 1.0 vom 06.11.2024 und die Checkliste zum Einsatz LLM-basierter Chatbots der Hamburger Datenschutzaufsicht vom 13.11.2023 zu beachten (Links und Updates auf chatgpt-recht.de) und weiterer Hinweise entsprechend Orientierungshilfen-Navigator KI & Datenschutz (ONKIDA).

Praxishinweise: Prozess KI-Einführung

b. Prüfung der Vorgaben von DSGVO, TDDDG, BDSG

8. Klärung, ob das Tool in seiner technischen Struktur (IP-Erfassung, Anbindung der Software, Verarbeitung der Eingaben) datenschutzkonform ist (ggf. TTDDG bei Webanbindung).
9. Abschluss eines Controller-to-Controller-Vertrags (meist kein Auftragsverarbeitungsvertrag, da der KI-Anbieter auch eigene Interessen verfolgt bei der Verarbeitung der erhobenen/übermittelten Daten), alternativ AVV (insb. wenn Abfluss personenbeziehbarer Daten ausgeschlossen (s.o. 1.a.i), alternativ ggf. gemeinsame Verarbeitung nach Art. 26 DSGVO).
10. Bei Auslandsdatenübertragung Prüfung des datenschutzkonformen Einsatzes (je nach Land Angemessenheitsbeschluss / DPF USA vom 10.07.2023, siehe **www.dataprivacyframework.gov/s/)**, SCCs etc., jeweiligen Stand der Klagen von NOYB im Auge behalten)
11. Zu Einzelfragen des Datenschutzes sind unter Anderem die Orientierungshilfe der Datenschutzkonferenz „Künstliche Intelligenz und Datenschutz“ Version 1.0 vom 06.11.2024 und die Checkliste zum Einsatz LLM-basierter Chatbots der Hamburger Datenschutzaufsicht vom 13.11.2023 zu beachten (Links und Updates auf chatgpt-recht.de) und weiterer Hinweise entsprechend Orientierungshilfen-Navigator KI & Datenschutz (ONKIDA).

c. Dokumentation der Datenschutzcompliance

Praxishinweise: Prozess KI-Einführung

4. IT-Sicherheit, Lizenzmanagement

1. Einbeziehung IT-Sicherheitsbeauftragter / Unternehmens-IT, IT-Lieferanten
2. Vorgaben TOMs Art. 32 DSGVO.
3. Konformität technischer Vorgaben der KI-VO.
4. Integration in bestehendes IT-Sicherheitskonzept.
5. Vorgaben IT-Sig. 2.0 soweit anwendbar, Ausschluss Sicherheitsvorfälle.
6. Klärung der Einsatzzwecke im Hinblick auf bestehende Softwarenutzung: Hat der KI-Einsatz Auswirkung auf andere Verträge / Nutzungsrechte? Wird die KI Software nutzen, welche nicht dafür lizenziert wurde (Lizenzmodell prüfen)?

Praxishinweise: Prozess KI-Einführung

5. Bei Plattformeinsatz des KI-Systems (Zugriff Dritter über große Plattform) und / oder Einsatz in smarten Produkten

1. Erfüllung der Anforderungen des DDG und TTDSG sowie der Störerhaftung, ggf. NetzDG / des ProdHG, der Produzentenhaftung nach § 823 Ab.1 BGB
2. Compliance mit den Neuregelungen des Digital Markets Act, des Digital Services Act, des Data Act
3. Erfüllung Transparenzpflichten
4. Klärung der Verwertung personenbezogener Endnutzerdaten / Zugangsrecht, Berücksichtigung GeschGehG
5. Erfüllung Meldesystempflichten
6. Berücksichtigung der Vorgaben der Neuregelungen der ProdukthaftRL und der KI-HaftungsRL
7. Erfüllbarkeit Discoverypflichten
8. Verfügbarkeit potentieller Beweismittel

Praxishinweise: Prozess KI-Einführung

6. Prüfung des KI-Anbieters / KI-VO / Vereinbarungen

1. Vorlage und Prüfung von Zertifizierungen, Konformitätsbewertungsverfahren, Konformitätskennzeichnungen, technische Dokumentationen
2. Compliance mit der KI-VO abhängig von Risikoklassifizierung, Berücksichtigung weiterer Regulierungen je nach Einsatzzweck (Produktsicherheit etc. und Hochrisikoklassifizierung), u.v.a..:
3. Kein Verstoß gegen Verbotsliste Art. 5 KI-VO.
4. Klassifizierungsprüfung nach Art. 6 KI-VO / Anhang III
5. Konzeptions- und Transparenzpflichten Artt. 53ff. KI-VO, Art. 4 II KI-HaftungsRL, Beachtung von Leitfäden nach Art. 56 KI-VO.
6. Art. 10 KI-VO Vorgaben für Trainings-, Validierungs- und Testdatensätze. Diese müssen relevant, hinreichend repräsentativ und im Hinblick auf den beabsichtigten Zweck so weit wie möglich fehlerfrei und vollständig sein. Sie müssen die geeigneten statistischen Eigenschaften aufweisen, gegebenenfalls auch in Bezug auf die Personen oder Personengruppen, für die das Hochrisiko-KI-System eingesetzt werden soll.
7. Art. 16 KI-VO Anbieterpflichten bei Hochrisikosystemen (unter Anderem Qualitätsmanagement und Dokumentation)

Praxishinweise: Prozess KI-Einführung

6. Prüfung des KI-Anbieters / KI-VO / Vereinbarungen

Art. 26 KI-VO Pflichten der Betreiber: Können diese rechtzeitig erfüllt werden?

8. Schulung vereinbaren zur Prompt- / Ergebnisoptimierung
9. Klärung der Rechte an Input und Output
10. Wahl einer erfolgsorientierten Leistungsbeschreibung / Eindeutige Beschreibung des Sollzustandes / Fehlerdefinition (insb. Compliance Art. 6 ProduktHaftRL !) / Gewährleistungsfragen / insb. Rechtsmängelfreiheit der Trainingsdaten und Ergebnisse / Haftung.
11. Absicherung der Freiheit der KI-Ergebnisse von Rechten Dritter
12. Klärung Datenschutz und Datensicherheit (s.o. 3 und 4.), Klärung des Status von Subunternehmern, Klärung Datenschutzcompliance bei KI-Anbieter, ggf. initialer Audit
13. Je nach Einsatzzweck Spezialvorgaben, z.B. Erfüllbarkeit Archivierungspflichten nach AO / HGB bei Verarbeitung steuerrelevanter Daten / Geschäftsbriefen
14. Bei marktmächtigen Anbieter: Strategien zur Aushebelung nicht verhandelbarer AGB im Bestellprozess prüfen (Best Practice-Thema).

Praxishinweise: Prozess KI-Einführung

7. Einführungsphase / Start des Systems

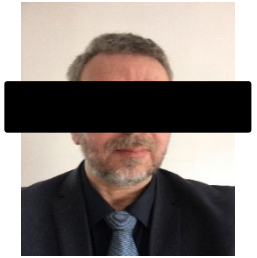
1. Schulung der Nutzenden: Information über Datenschutzsituation, Wahrung der Vertraulichkeit bei Prompts, Erwartungsmanagement zur Fehlerhaftigkeit von Ergebnissen.
2. Finale Erstellung von FAQ / Anwenderinformationen / Ethikleitlinien (bei sensiblen Anwendungen) / Datenschutzerklärungen.
3. Dokumentation des Vorliegens der Rechtsgrundlagen für die Datenerhebung, Abschluss Betriebsvereinbarung, Fertigstellung und Einholung Einwilligungserklärungen.
4. Durchatmen, progressive Muskelentspannung nach Jacobson, sodann: 1 Knoppers, 1 Heißgetränk mit Milchschaum und wiederverwendbarem Röhrchen (Metall, kein selbstauflösendes und deshalb zur Eile gemahnendes Zellstoffrezyklat).
5. Start des Systems.

Praxishinweise: Prozess KI-Einführung

8. Laufende Compliance / ständiges Update

1. Qualitätssicherung Prompteingabe, Feedbackrunden, Störfallanalysen.
2. Notice- und Takedown-Verfahren für Rechtsverletzungen bei Einbindung Dritter.
3. Prüfung der Compliance bei Controller-to-Controller und Controller-to-Processor Vereinbarungen, Prüfung der Rechtsentwicklung bei Auslandsdatenübertragungen, fortlaufende Audits.
4. Prüfung der Entwicklung bei Rechtsgrundlagen, insb. hinsichtlich des Beschäftigtendatenschutzes
5. Fortlaufende Beachtung der Zweckbindung nach Art. 5 I b DSGVO.
6. Erfassung und Umsetzung der Widerrufe bei einwilligungsbasierter Datenverarbeitung nach Art. 6 I a DSGVO.
7. Laufende Prüfung gesetzlicher Neuregelungen / Hinweise der Aufsichten.

Fragen? Diskussion!



Prof. Dr. Thomas Wilmer
thomas.wilmer@h-da.de
Copilot-recht.de, chatgpt-recht.de

Literaturhinweise:

- Wilmer, Rechtliche Rahmenbedingungen für KI-Systeme , Tatup 2021, 56-62, https://doi.org/10.14512/tatup.30.3.56
- Wilmer, Europäisches Daten-Lizenzrecht im Umbruch , NJW-Spezial 2022, S. 2-4, https://neuheiten.beck.de/llm-special/67043655.
- Wilmer, Rechtsfragen bei ChatGPT & Co. Einsatz und Nutzung nach aktuellem und künftigem Recht.
- K&R 2023, 233.
- Wilmer, Rechtsfragen bei DALL-E & Co. - Schutzfähigkeit der „Promptografie“? K&R 2023, 385
- Gutjahr, Hornung, Krieger, Schaller, Selzer, Spiecker gen. Döhmann, Wilmer: Studie: Fehlende Rechtssicherheit für Big Data und KI
- https://www.athene-center.de/fileadmin/Downloads/Systematic_Privacy_Studie_2023.pdf?_=1699890300
- Wilmer, Herausforderungen der Vertragsgestaltung mithilfe Künstlicher Intelligenz, EuZW 2024, 868
- Wilmer, KI-Recht, Textsammlung, 1.A. 2024
- Wilmer, KI-Recht, in Jandt/Steidle, Datenschutz im Internet, 2.A. 2024