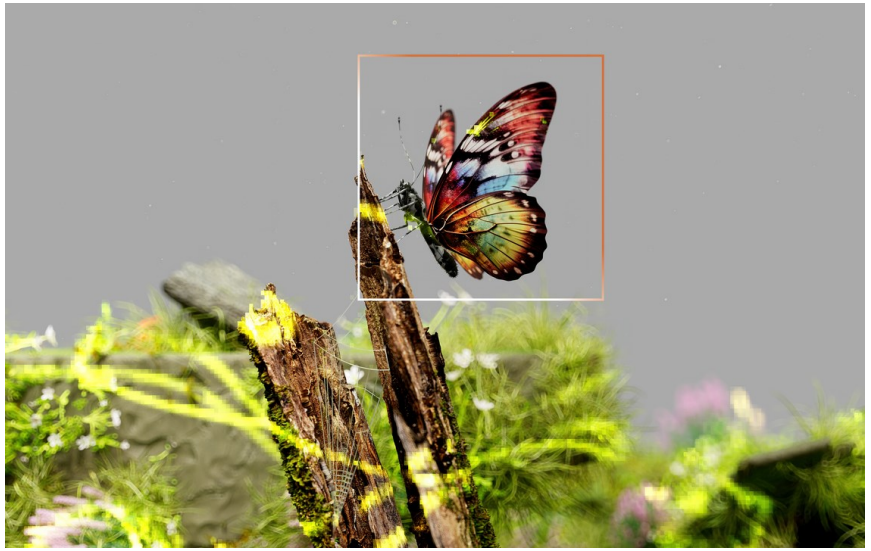
CHANCEN UND RISIKEN

Künstliche Intelligenz kann uns helfen,

- effizienter zu arbeiten,
- Kosten zu senken,
- Daten besser zu verwalten und
- unsere Kommunikation zu verbessern.

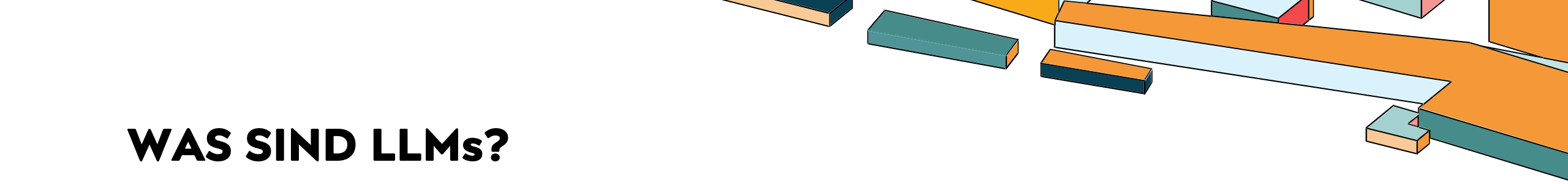
Allerdings bergen die Nutzung und Entwicklung von KI auch nicht unerhebliche Risiken.



Nidia Dias & Google DeepMind / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Daher ist es wichtig, dass wir bestehende Gesetze wie:

- Urheberrecht, Datenschutz und den Schutz von Geschäftsgeheimnissen beachten.



WAS SIND LLMs?

Generative KI-Tools arbeiten auf der Grundlage von sogenannten **Large Language Models** (LLMs). Dies sind fortschrittliche Computerprogramme, die menschliche Sprache verstehen und erzeugen können. Sie werden mit großen Mengen an Textdaten aus dem Internet, Büchern und Artikeln trainiert.

Was kann ein LLM?

- ✓ Texte schreiben oder zusammenfassen
- ✓ Fragen beantworten
- ✓ Inhalte umformulieren oder übersetzen
- ✓ Bei Ideen helfen oder strukturieren

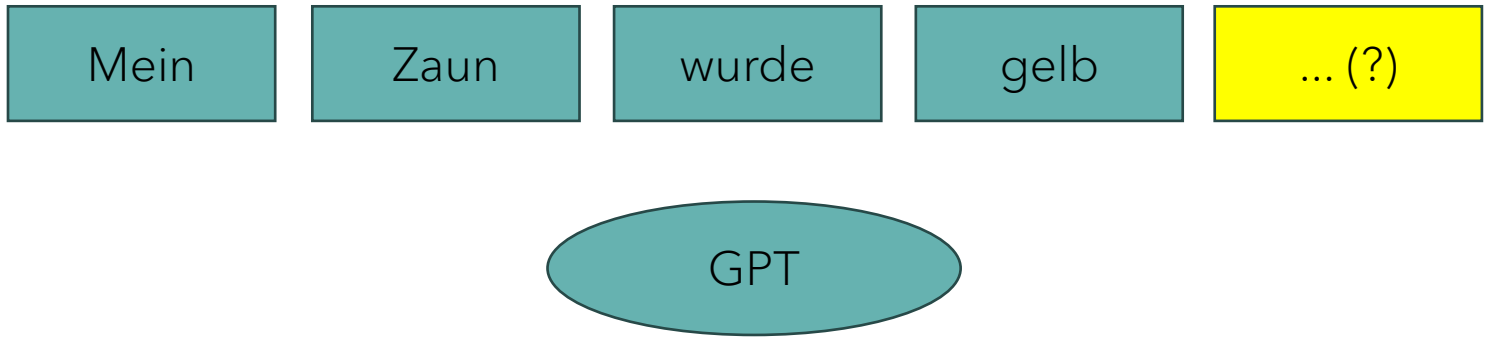
Aber: LLMs wissen nicht, was wahr oder falsch ist – sie erzeugen „wahrscheinliche" Antworten, keine geprüften Fakten.

WIE LLMs FUNKTIONIEREN
(STARK VEREINFACHT)

Datensammlung: LLMs lernen aus Millionen von Textbeispielen (Bücher, Artikel, Webseiten).

Mustererkennung: Sie erkennen Muster darin, wie Wörter und Sätze verwendet werden und in welcher Beziehung sie miteinander stehen.

Vorhersage: Bei einer Eingabe sagen sie die wahrscheinlichsten nächsten Wörter voraus und generieren diese als Antwort (ähnlich der T9-Autovervollständigung in Smartphones).



Wort	Wahrscheinlich-keit
gestrichen	35 %
gebaut	14 %
und	7 %
vor	3 %

Abbildung: eigene Darstellung nach Helmut Linde, Golem.de

TYPISCHE ANWENDUNGSBEREICHE DER GENERATIVEN KI UND GÄNGIGE TOOLS

- Übersetzungen (z. B. Deepl, Google Translator)
- Literaturrecherche (z. B. Perplexity, Scite)
- Internet-Suche (z. B. Microsoft Copilot in Bing)
- Textverständnis (z. B. Explainpaper, SciSpace)
- Textproduktion (z. B. Copy.ai, Jasper, Neuroflash)
- Textbearbeitung/Korrektur (z. B. Deepl Write, Grammarly)

TYPISCHE ANWENDUNGSBEREICHE DER GENERATIVEN KI UND GÄNGIGE TOOLS

- Bild- und Videogenerierung
  (z. B. Midjourney, Dall-E, Sora)
- Programmierung/Codierung
  (z. B. Cursor.ai, GitHub, Copilot)
- Datenanalyse (z. B. Neurons)
- Chatbots (z. B. ChatGPT, Google Gemini, DeepSeek, Claude.ai)
- Und viele mehr…

TYPISCHE ANWENDUNGSBEREICHE WEITERER KI TOOLS (NICHT-GENERATIV)

- Bilderkennung und -klassifikation
- Gesichts- und Spracherkennung
- Autonomes Fahren
- Vorhersagemodelle
- Empfehlungssysteme (z. B. in Onlineshops)

WELCHE RISIKEN KÖNNEN SICH BEI DER NUTZUNG ERGEBEN?

Zu den **rechtlichen Risiken** gehören insbesondere Herausforderungen im Zusammenhang mit:

- dem Urheberrecht:

  Das Hochladen und/oder Verarbeiten von Texten oder anderen Inhalten kann kritisch sein, wenn Unklarheit über die hierfür notwendigen Urheberrechte besteht.

  Nicht nur das Hochladen kann eine Urheberrechtsverletzung darstellen. Auch Informationen, die generative KI bereitstellt, können urheberrechtlich geschützt sein.

- dem Datenschutz sowie dem Schutz von Geschäftsgeheimnissen.

WELCHE RISIKEN KÖNNEN SICH BEI DER NUTZUNG ERGEBEN?

Zu den ethischen Risiken, die mit der Nutzung generativer KI einhergehen, gehören Aspekte wie:

- das Nahelegen von unethischen Entscheidungen;
- die Reproduktion von (diskriminierenden) Stereotypen;
- die Verwendung von Quellen ohne Kennzeichnung;
- das Erfinden von Informationen.

WELCHE RISIKEN KÖNNEN SICH BEI DER NUTZUNG ERGEBEN?

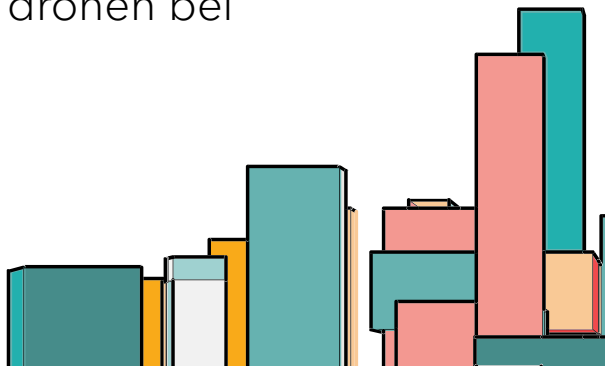
- Durch den Einsatz von generativer KI darf es nicht zu einer Überforderung von Mitarbeitenden kommen;
- Führungskräfte müssen darauf achten, dass deren Einsatz für die Mitarbeitenden entlastend, nicht belastend wirkt;
- KI-Tools sollten möglichst allen interessierten Mitarbeitenden zugänglich gemacht werden;
- Schulungsmaßnahmen sind so anzulegen, dass sie generationenübergreifend und inklusiv wirken;
- Der Einsatz von generativer KI ist sehr energieintensiv, es sollten daher Nachhaltigkeitsstrategien zur Verwendung entwickelt werden.

DIE EU-KI-VERORDNUNG

Zum Volltext der Verordnung:
http://data.europa.eu/eli/reg/2024/1689/oj

Die EU-KI-Verordnung (KIVO) ist am 1. August 2024 in Kraft getreten:

- Risikobasierter Ansatz
- Reguliert den Umgang mit KI aus Anwender und Betreiber/Entwickler-Sicht
- Geht mit umfassenden Rechten und Pflichten für Anwender und Betreiber einher (hohe Strafen drohen bei Nichteinhaltung)



DIE EU-KI-VERORDNUNG

Die EU-KI-Verordnung unterscheidet KI-Systeme nach Risikostufen. Für Verwaltungsmitarbeitende sind v. a. Systeme mit geringem oder begrenztem Risiko relevant – z. B. Chatbots zur Textgenerierung oder Übersetzungstools:

Minimal oder gar kein Risiko (geringfügige Risiken):

- KI-Systeme mit minimalem Risiko (z. B. Übersetzungstools) unterliegen nach der EU-KI-Verordnung keinen spezifischen Vorgaben, solange ihre Nutzung im Einklang mit geltenden Gesetzen erfolgt.

Unkritische Systeme (begrenztes Risiko):

- Diese Systeme (z. B. Chatbots stellen standardisierte Infos zur Verfügung) erfordern **geringe Regulierung,** z. B. eine Kennzeichnung, dass Nutzer/innen mit einem KI-System interagieren. Eine umfassende Regulierung oder Vorabprüfung ist nicht erforderlich.

DIE EU-KI-VERORDNUNG

Hohe Risiken:

- KI-Systeme, die Entscheidungen über Menschen treffen oder deren Fähigkeiten bewerten (z. B. bei Bewerbungen oder Beförderungen), gelten als hochrisikobehaftet. Sie unterliegen strengen Anforderungen an Transparenz, Risikomanagement, menschliche Aufsicht und Dokumentation. Ein pauschales Verbot besteht nur bei besonders inakzeptablen Praktiken.

Inakzeptable Risiken (verbotene Anwendungen):

- Diese Systeme stellen so hohe Risiken dar, dass sie verboten sind. Sie beinhalten z. B. KI-Systeme zur sozialen Bewertung, Emotionserkennung am Arbeitsplatz, manipulative KI oder KI-Systeme, die Menschen überwachen.

Entscheidungen über Menschen dürfen niemals ohne menschliche Prüfung ausschließlich KI-gestützt getroffen werden.

DIE EU-KI-VERORDNUNG

GPAI (General Purpose AI / KI-Systeme mit allgemeinem Verwendungszweck) bezeichnet KI-Systeme wie ChatGPT, die für viele Zwecke eingesetzt werden können – z. B. zum Formulieren von Texten, Übersetzen oder Zusammenfassen.

Diese Systeme haben keine feste Risikoeinstufung an sich. Entscheidend ist, wie sie im Arbeitsalltag konkret genutzt werden:

Je nach Einsatz kann ein GPAI-System geringe, hohe oder inakzeptable Risiken bergen.

Beispiel:

- ChatGPT-Verwendung zur Formulierung eines Anschreibens: geringes Risiko
- ChatGPT-automatisierte Entscheidungshilfe bei Bewerbungen: hohes Risiko (z.B. wenn Vorschläge zur Auswahl von Bewerber/innen erstellt werden)

DIE EU-KI-VERORDNUNG

Auch in der Verwaltung gilt: KI-generierte Inhalte müssen stets geprüft werden. KI-Tools wie ChatGPT oder DeepL liefern nicht automatisch korrekte oder neutrale Ergebnisse.

Führen Sie vor der Einführung eines KI-Tools eine Risikoanalyse durch und dokumentieren sie:

- Welches Tool wurde verwendet?
- Zu welchem Zweck?
- Welche Daten wurden wie verarbeitet (z. B. personenbezogen, öffentlich, intern)?
- Welche Risiken bestehen und welche Minderungsmaßnahmen wurden getroffen?
- Wie stelle ich menschliche Kontrolle sicher?

Empfehlung: Nutzen Sie Checklisten oder Vorlagen Ihrer Einrichtung zur Dokumentation. Ziehen Sie bei Unsicherheiten Ihre/n Datenschutzbeauftragten/r bzw. die Rechtsabteilung hinzu bzw. orientieren Sie sich an den KI-Handreichungen Ihrer Einrichtung, soweit vorhanden.

DIE EU-KI-VERORDNUNG

Falls Sie regelmäßig KI-Tools nutzen, sollte eine **interne KI-Richtlinie** erstellt werden, die dokumentiert:

- Welche Tools sind erlaubt?
- Welche Arten von Daten dürfen verarbeitet werden?
- Wie müssen KI-generierte Inhalte gekennzeichnet werden?

Ihre Einrichtung sollte Sie zudem bei der Risikobewertung der von Ihnen genutzten KI-Tools unterstützen, wenn Sie dies nicht selbst abschätzen können. Informieren Sie sich über die für Sie geltenden Rechte und Pflichten.

DIE EU-KI-VERORDNUNG

Wenn Sie KI-Tools selbst entwickeln oder modifizieren (z. B. eigene KI-Modelle für administrative Zwecke trainieren, oder selbst Systeme anbieten), gelten verschärfte Anforderungen.

- Technische Dokumentation
  - Anbieter müssen eine umfassende technische Dokumentation erstellen und bereitstellen.
  - Darin müssen u. a. enthalten sein: Beschreibung des Modells, Trainingsdatenquellen, bekannte Einschränkungen und Risiken, Anwendungsgrenzen

Diese Dokumentation soll Regulierungsbehörden und Hochrisiko-Nutzer/innen die Möglichkeit geben, die Risiken zu bewerten.

DIE EU-KI-VERORDNUNG

Wenn Sie KI-Tools selbst entwickeln oder modifizieren (z. B. eigene KI-Modelle für administrative Zwecke trainieren, oder selbst Systeme anbieten), gelten **verschärfte Anforderungen.**

- Transparenzpflichten

Anbieter müssen veröffentlichen:

- dass es sich um ein GPAI-System handelt
- wie das System funktioniert (allgemeine Beschreibung)
- welche bekannten Risiken mit der Nutzung verbunden sein können
- Hinweise auf Nutzungsbeschränkungen

Nutzer/innen sollen verstehen, dass sie es mit einem KI-System zu tun haben und welche Grenzen bestehen.

DIE EU-KI-VERORDNUNG

Wenn Sie KI-Tools selbst entwickeln oder modifizieren (z. B. eigene KI-Modelle für administrative Zwecke trainieren, oder selbst Systeme anbieten), gelten **verschärfte Anforderungen.**

- Einhaltung des EU-Urheberrechts
  - Anbieter müssen nachweisen, dass beim Training des GPAI-Modells Urheberrechtsvorschriften eingehalten wurden (z. B. bei Trainingsdaten aus Texten, Bildern, Musik etc.).
- Prävention und Meldepflicht bei Risiken oder Vorfällen, Minderungsmaßnahmen:
  - Falls das KI-System fehlerhafte oder diskriminierende Ergebnisse liefert, müssen **Maßnahmen zur Risikominimierung** ergriffen und dokumentiert werden.
  - Falls das KI-System **Schaden** angerichtet hat, **muss** dieser **gemeldet werden** (wenden Sie sich an Ihre/n Vorgesetzte/n).

DIE EU-KI-VERORDNUNG

Die nachstehenden Folien zur Zeitabfolge des Inkrafttretens verschiedener Teile der EU-KI-Verordnung sind besonders für Führungspersonal relevant, die die Einführung bzw. den Einsatz von generativen KI-Tools verantworten. Falls Sie dies nicht betrifft, können Sie diese Folien überspringen.

- ab 2. Februar 2025:
  - Anbieter und Betreiber bestimmter KI-Systeme (insbesondere Hochrisiko-KI) müssen sicherstellen, dass Nutzer/innen über geeignete Kompetenzen in Recht, Ethik und Technik verfügen.
  - Verbotene KI-Praktiken dürfen nicht mehr angewendet werden.

DIE EU-KI-VERORDNUNG

Zeitabfolge

- ab 2. August 2025:
  - umfassendere Dokumentationspflichten insbesondere für Betreiber hochriskanter KI-Systeme und für Anbieter von GPAI-Modellen
  - Sanktionsmöglichkeiten bestehen (Abmahnungen und Geldstrafen möglich) insbesondere für hohe Risiken betreffende Sektoren (Gesundheit, Transport, Finanzwesen, Polizei)
  - Besonders betroffen sind Bereiche mit Entscheidungswirkung oder Außenwirkung – z. B. Personalmanagement, Auswahlverfahren, automatisierte Rückmeldungen, barrierefreie Kommunikation.
  - Führen Sie eine Übersicht, welche KI-Tools in Ihrer Abteilung verwendet werden und in welchem Rahmen – das erleichtert die Dokumentation und Bewertung.

DIE EU-KI-VERORDNUNG

Zeitabfolge

- ab 2. August 2025:
  - Auch in der Verwaltung gilt ab August 2025: Der Einsatz von KI-Systemen muss transparent, nachvollziehbar und ethisch verantwortbar sein – unabhängig davon, ob der Einsatz kommerziell oder nicht-kommerziell erfolgt. Entscheidungen, die mit Unterstützung von KI vorbereitet oder getroffen werden, müssen stets überprüfbar sein – es darf keine „Black Box"-Entscheidungen geben.
  - Was durch KI unterstützt wird, muss auch menschlich verantwortet und begründet werden können.

DIE EU-KI-VERORDNUNG

Zeitabfolge

- ab 2. August 2026:
  - Anwendbarkeit aller Verpflichtungen mit wenigen Ausnahmen (Forschungszwecke: Forschungsprojekte, die KI-Systeme ausschließlich für wissenschaftliche Zwecke entwickeln oder testen – ohne diese direkt in den Markt oder produktive Abläufe einzuführen – unterliegen erleichterten Vorgaben)
  - umfassendes Compliance-System muss vorliegen – Erfassung, Dokumentation, Schulung

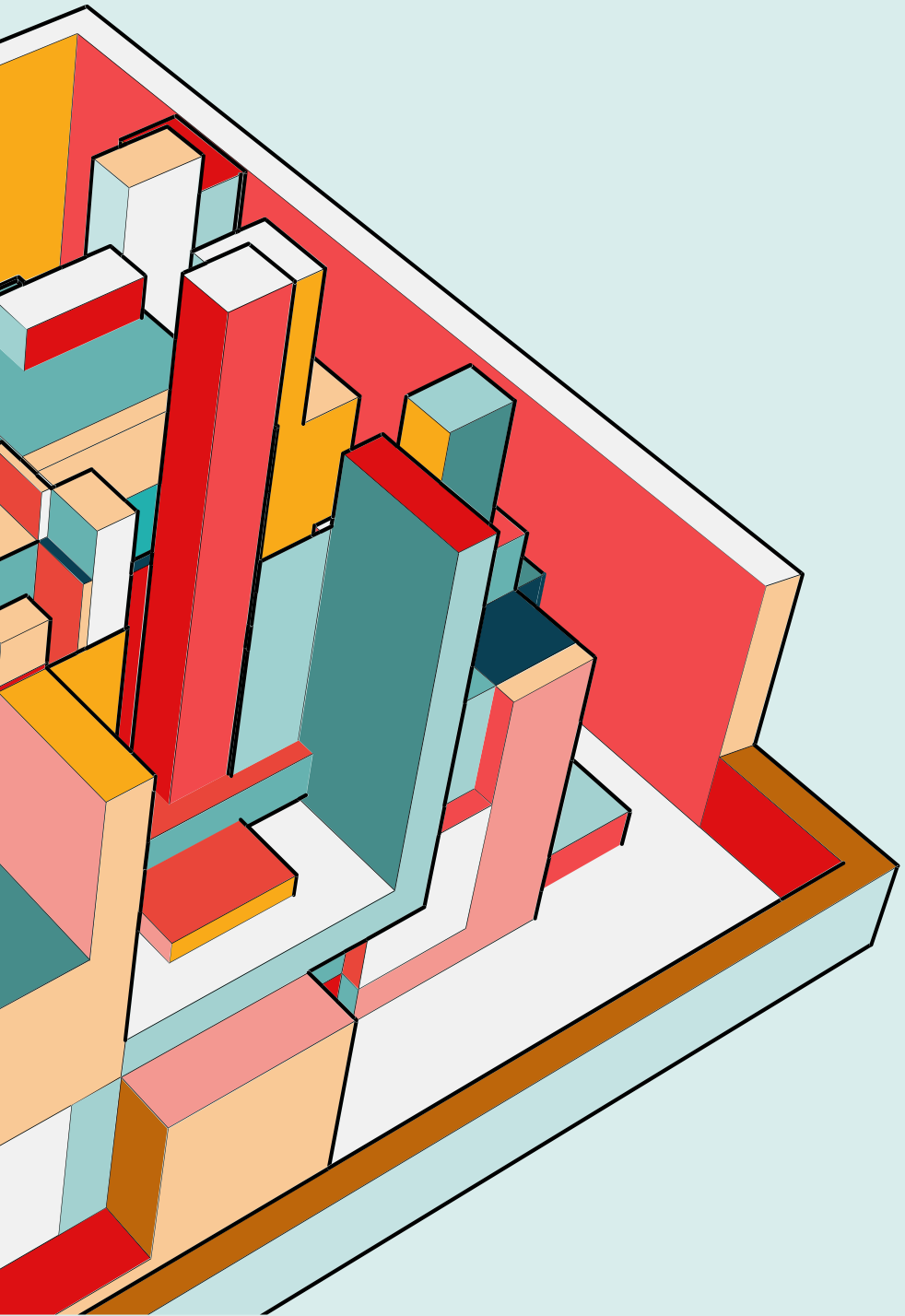
- ab 2. August 2027:
  - Erweitere Pflichten für hochriskante KI-Systeme

DIE EU-KI-VERORDNUNG

Zeitabfolge

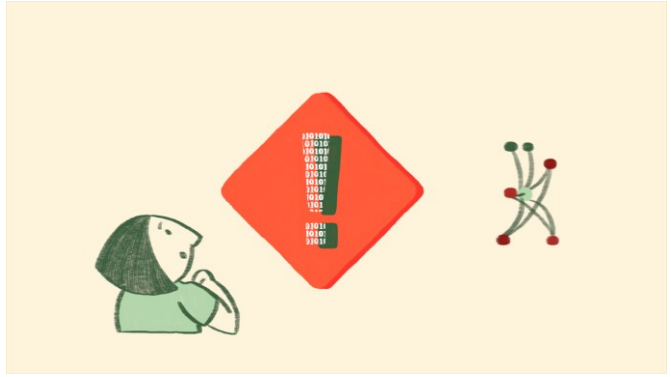
- Beginnen Sie frühzeitig mit der internen Abstimmung und klären Sie:

  - ✓ Welche KI-Systeme werden genutzt?
  - ✓ Wo liegen Risiken?
  - ✓ Wer ist zuständig für Bewertung, Dokumentation und Schulung?



ALLGEMEINE REGELN ZUR NUTZUNG VON GENERATIVEN KI-TOOLS

SELBSTVERSTÄNDNIS IM UMGANG MIT GENERATIVER KI



Yasmin Dwiputri & Data Hazards Project / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Viele Einrichtungen haben bereits KI-Regelungen veröffentlicht. Bitte informieren Sie sich über diese und betrachten Sie die vorliegende Schulung als Ergänzung.

Bei Widersprüchlichkeiten wenden Sie sich an den/die Schulungsbeauftragte.

Die Schulung fokussiert auf den Einsatz von generativen KI-Tools in der Verwaltung, ist aber auch auf den generellen Einsatz von KI übertragbar. Dort gelten zudem aber weiterführende Rechte & Pflichten, die sich aus der KI-Verordnung ergeben. Diese sollten individuell an jeder Einrichtung geprüft und in Regeln überführt werden.

SELBSTVERSTÄNDNIS IM UMGANG MIT GENERATIVER KI

Die wichtigsten Prinzipien bei der Nutzung von Generativer KI sollten sein:

Zuverlässigkeit, Ehrlichkeit, Respekt, Verantwortungsübernahme.

SELBSTVERSTÄNDNIS IM UMGANG MIT GENERATIVER KI

Zuverlässigkeit:

KI-Systeme sollten konsistente und gut begründete Ergebnisse liefern, die auf überprüfbaren Daten und wissenschaftlich fundierten Methoden basieren, sodass die Nutzer darauf vertrauen können.

Ehrlichkeit:

Alle durch KI generierten Ergebnisse sollten transparent, offen und ohne Täuschung als solche präsentiert werden.

SELBSTVERSTÄNDNIS IM UMGANG MIT GENERATIVER KI

Respekt:

Der Einsatz von KI sollte die Würde, Rechte und die Privatsphäre von Individuen respektieren. Alle Beteiligten müssen sicherstellen, dass KI fair und ohne Diskriminierung eingesetzt wird, insbesondere im Umgang mit sensiblen Daten und der Interaktion mit Personen.

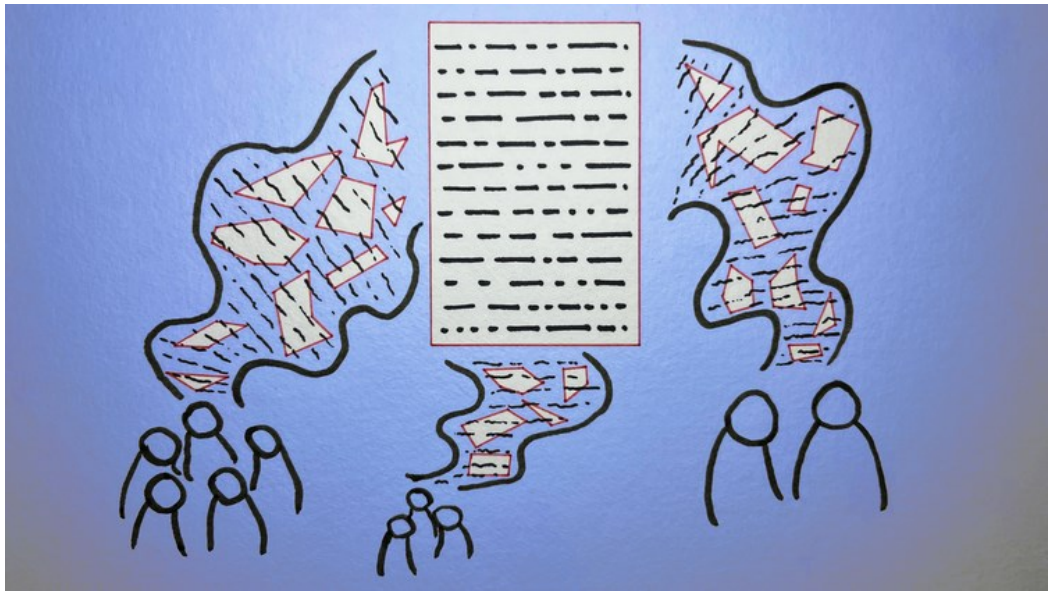
Verantwortungsübernahme:

Die Verantwortung für die Ergebnisse, die mit Hilfe von KI erzielt werden, liegt bei den Anwender/innen. Forschende, Lehrende, Studierende und Verwaltung müssen sicherstellen, dass KI-Anwendungen ethisch und sicher eingesetzt werden und mögliche Fehler oder Missbrauch vermieden bzw. zügig korrigiert werden.

SELBSTVERSTÄNDNIS IM UMGANG MIT GENERATIVER KI

Um einen Handlungsrahmen und eine Nutzungskultur zu etablieren, die einen möglichst rechtssicheren und verantwortungsvollen Umgang ermöglichen, folgen

10 einfache Regeln für die Nutzung von generativer KI.



Yasmine Boudiaf & LOTI / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

REGEL 1: RECHTLICHE RAHMENBEDINGUNGEN EINHALTEN

Wir halten auch bei der Nutzung von generativer KI die geltenden Gesetze und arbeitsrechtlichen Verpflichtungen ein.

Die wichtigsten rechtlichen Bestimmungen betreffen die Themen:

- Datenschutz
- Urheberrecht
- Geheimhaltung
- Sanktionsrecht
- Markenrecht
- Strafrecht

Bild: herbinisaac auf Pixabay

REGEL 1: RECHTLICHE RAHMENBEDINGUNGEN EINHALTEN

Prüfen Sie...

- Darf ich die einzugebenden Daten aus rechtlicher Perspektive verwenden (Datenschutzrecht, Urheberrecht, Strafrecht, Sanktionsrecht, Personendaten etc.)?
- Verwende ich ausschließlich freigegebene Tools und Dienste gemäß den Richtlinien meiner Einrichtung?
- Haben ich kritisch geprüft, was mit meinen hochgeladenen Dateien passiert und ob dies den Richtlinien meiner Einrichtung entspricht (z. B. Datenschutz und Geheimhaltungsregeln)?
- Einrichtungen sollten KI-Richtlinien entwickeln, die klare Regelungen zur Nutzung generativer KI in Forschung, Verwaltung, Lehrveranstaltungen und Prüfungen enthalten. Bitte informieren Sie sich dazu und berücksichtigen Sie diese.
- Gerade in der Bearbeitung von Anträgen, interner Kommunikation oder Personalangelegenheiten sollte sorgfältig geprüft werden, welche Informationen in KI-Systeme eingegeben werden dürfen.

REGEL 1: RECHTLICHE RAHMENBEDINGUNGEN EINHALTEN

- Wir achten darauf, keine KI-generierten Inhalte zu erstellen oder hochzuladen, die gegen das Urheberrecht verstoßen.
- Wir laden Personenabbildungen nur dann in KI-Tools hoch, wenn wir vorher das Einverständnis der Abgebildeten eingeholt haben und alle rechtlichen Vorgaben erfüllt sind.
- Wir geben personenbezogene Daten nur dann in KI-Umgebungen ein, wenn alle rechtlichen Voraussetzungen hierfür vorliegen (z. B. Zustimmung, Datenverarbeitungserklärung, etc.).
- Achten Sie z. B. bei der Nutzung von KI zur Erstellung von Textbausteinen, Vorlagen oder Präsentationen darauf, keine geschützten Inhalte (z. B. aus Fachliteratur) zu verwenden oder hochzuladen.

REGEL 1: RECHTLICHE RAHMENBEDINGUNGEN EINHALTEN

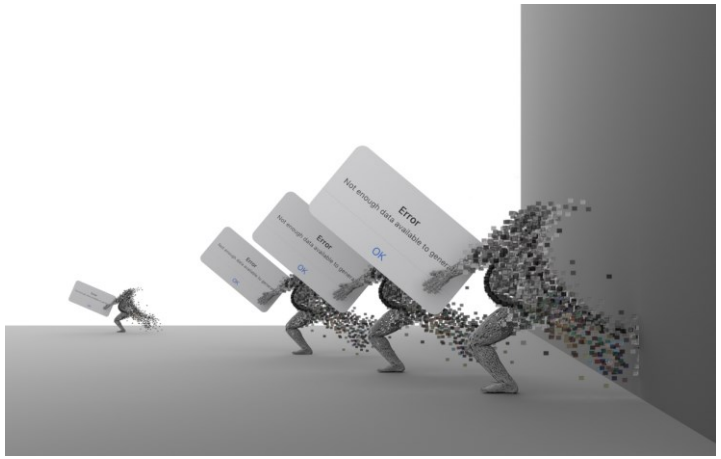
- Auch im Verwaltungsalltag gelten die allgemeinen rechtlichen Pflichten beim Einsatz generativer KI. Achten Sie insbesondere auf den Schutz personenbezogener Daten, Urheberrechte und Vertraulichkeit.

! Grundsätzlich gilt: Was rechtlich ohne KI nicht erlaubt ist, bleibt auch mit KI unzulässig.

REGEL 2: SONDERVEREINBARUNGEN KENNEN UND BEACHTEN

Beachten Sie die Lizenzbedingungen bei der Verwendung von KI-generierten Inhalten oder externen Materialien (z. B. bei Präsentationen, Handouts, Webseiten). Also wer hält die Rechte an den Quellen, die ich ggf. mit KI verarbeiten will?

- Verwenden Sie bevorzugt Inhalte, die unter Creative Commons (Open Source) lizenziert oder explizit zur Weiterverwendung freigegeben sind.
- Wenn Sie unsicher sind, ob Sie Quellen mit KI verarbeiten dürfen, klären Sie vorab urheberrechtliche Fragen mit der Rechtsabteilung, KI-Beauftragten oder Datenschutzbeauftragten Ihrer Einrichtung.



Amritha R Warrier & AI4Media / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

REGEL 3: KI-PROGRAMME VOR DER VERWENDUNG SORGFÄLTIG PRÜFEN

Viele KI-Tools bergen Risiken, da für Laien oft nicht klar ist, was mit den eingegebenen Daten passiert und ob sie gemäß den geltenden Gesetzen, wie der Datenschutzgrundverordnung (DSGVO), behandelt werden.

- Prüfen Sie in den Lizenz- und Datenschutz-informationen vor der Nutzung eines externen Tools, ob es den Anforderungen Ihrer Einrichtung entspricht.
- Nutzen Sie zentral empfohlene und datenschutzkonforme Tools, die durch Ihre Einrichtung freigegeben wurden.
- Bei Unsicherheiten zur Tool-Nutzung: Wenden Sie sich an Ihre IT-Abteilung, die Datenschutzstelle oder an KI-Beauftragte.

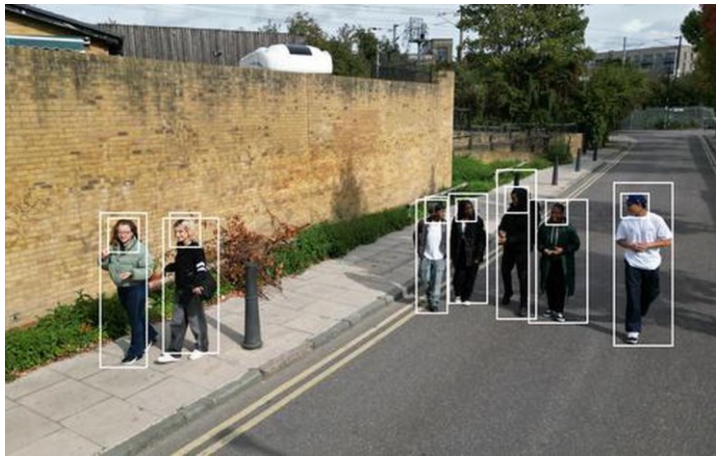


Image by Comuzi / © BBC / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

REGEL 3: NUTZEN SIE EMPFOHLENE KI-PROGRAMME

Bitte prüfen Sie, ob Ihre Einrichtung abweichende Regelungen zur Nutzung erlassen hat.

- **Texte und Rechtschreibprüfung:** DEEPL Übersetzer und Write in der Pro-Variante (besserer Datenschutz)

- **KI-Allrounder:** falls keine internen Plattformen zur Verfügung stehen: z. B. ChatGPT Plus und aufwärts
  - ✓ Auch hier bieten Bezahlversionen in der Regel einen besseren Datenschutz. Stellen Sie sicher, dass in den Einstellungen „Modell für alle verbessern“ bzw. „Eingaben für Trainingsdaten verwenden“ ausgeschaltet ist.

- **KI-Allrounder:** Academic Cloud (www.academiccloud.de)
  - ✓ Falls Sie an einer Hochschule oder Forschungseinrichtung arbeiten, prüfen Sie, ob Sie sich kostenfrei für die Academic Cloud registrieren und diese auch ihren Mitarbeitenden bzw. Studierenden zur Verfügung stellen können. Diese bietet DSGVO-konformen und kostenfreien Zugang zu einfachen, nichtkommerziellen generativen KI-Modellen und auch attraktive Bezahlversionen von kommerziellen Lizenzen.

Wes Cockx & Google DeepMind / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

REGEL 3: NUTZEN SIE EMPFOHLENE KI-PROGRAMME

- **Bilderstellung:** Adobe Firefly
  - ✓ Teil der Adobe Creative Suite, bietet ein aktuell sehr sicheres Urheberrecht und schützt vor Missbrauch

- **Weitere KI-Tools**
  - ✓ Informieren Sie sich an Ihrer Einrichtung zu weiteren empfohlenen KI-Tools

- **Sicherheit**
  - ✓ Wissenschaftseinrichtungen sollten sichere, geschützte KI-Plattformen für den Verwaltungsbetrieb zur Verfügung stellen

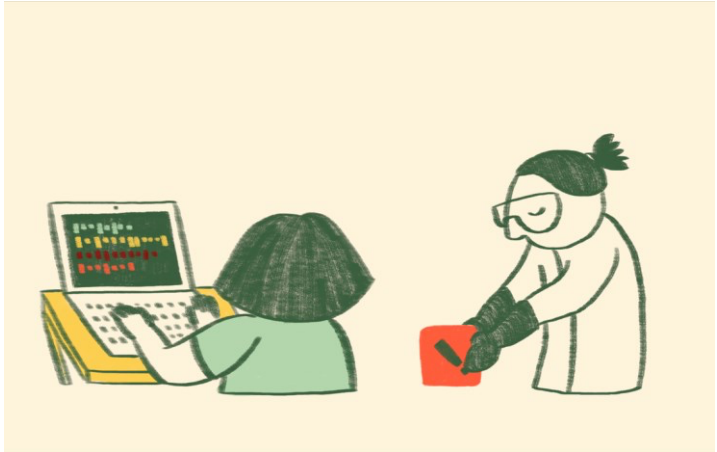
Wes Cockx & Google DeepMind / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

REGEL 4: DER MENSCH HAT IM EINSATZ DER KI DAS LETZTE WORT

- Der Einsatz und die Freigabe von KI-generierten Inhalten unterliegt stets der **gewissenhaften Überwachung und Kontrolle durch Menschen**.

- Wir verpflichten uns, Inhalte, die mithilfe von generativer KI erstellt wurden, stets **von mindestens einer qualifizierten Person** auf Richtigkeit, Faktentreue und Kontext zu überprüfen.

- Wir übernehmen die **volle Verantwortung** für alle KI-gestützten Inhalte, die wir im Verwaltungskontext weiterverwenden – z. B. in Schreiben, Vorlagen oder E-Mails.



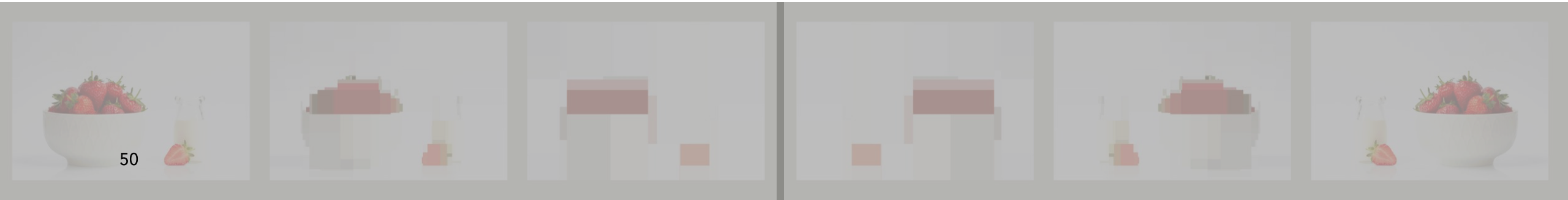
Yasmin Dwiputri & Data Hazards Project / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

REGEL 5: BESONDERE SORGFALT BEI PERSONENBEZOGENEN DATEN

Die Eingabe **personenbezogener Daten** in KI-Umgebungen ist nur dann erlaubt, wenn **alle rechtlichen Voraussetzungen hierfür vorliegen** (z. B. Zustimmung, Datenverarbeitungserklärung, etc.).

- Beachten Sie, dass Sie bei vielen (insbesondere kostenlos frei verfügbaren) KI-Tools implizit der Weiterverarbeitung der eingegebenen Daten durch das anbietende Unternehmen zustimmen.
- Eine gute Lösung ist die Anonymisierung von Daten, so dass keine Rückschlüsse auf personenbezogene Daten möglich sind (durch Entfernung von Namen und anderen Identifikatoren).
- Auf die Verarbeitung personenbezogener Daten durch KI-Systeme ist in einer entsprechenden Datenschutzerklärung hinzuweisen.
- Werden Daten außerhalb der EU gehostet, müssen die Vorschriften des Internationalen Datenverkehrs beachtet werden.

Catherine Breslin & Rens Dimmendaal / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/



REGEL 6: GEHEIMHALTUNGS-VERPFLICHTUNG BEACHTEN

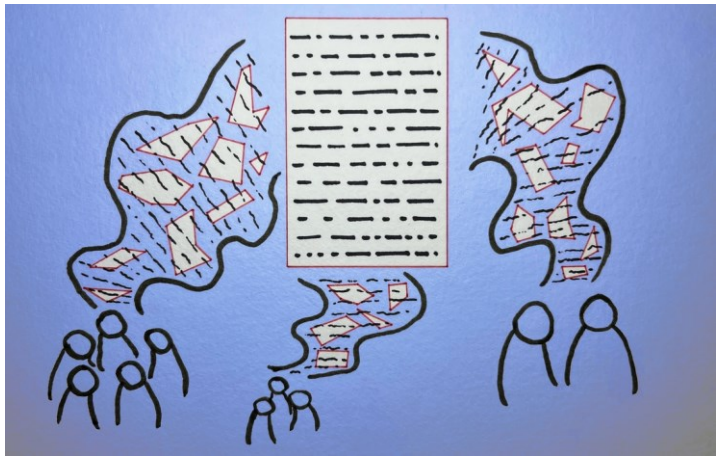
Vertrauliche oder sensible Informationen dürfen niemals in generativen KI-Anwendungen verwendet werden, auch nicht zu Analyse- oder Formulierungszwecken.

REGEL 7: UMGANG MIT DER QUALITÄT VON KI-GENERIERTEN INHALTEN

- Als Autor/in sind wir für die Integrität der von uns mithilfe von generativer KI erstellten Inhalte verantwortlich.

- KI-Systeme sind weder Autoren noch Co-Autoren. Autorenschaft impliziert Handlungsfähigkeit und Verantwortung, sie liegt also bei uns als den Nutzern/innen von KI-Tools.

- Inhalte, die mit KI erstellt wurden, dürfen erst nach sorgfältiger Prüfung weiterverwendet werden.



Yasmine Boudiaf & LOTI / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

REGEL 8: ETHISCHE GRUNDLAGEN

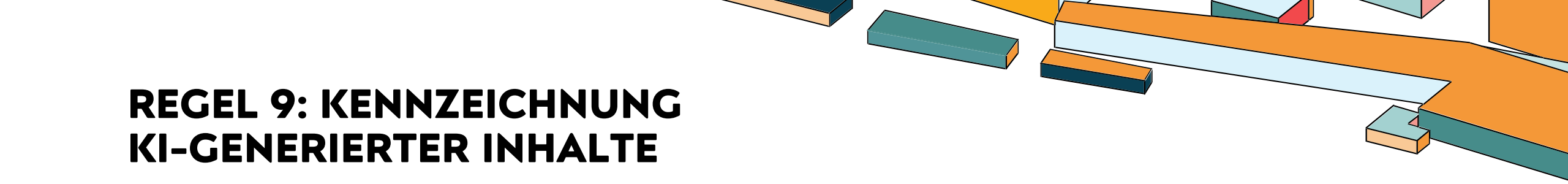
- KI trifft keine moralischen Entscheidungen. Es liegt an uns, Inhalte verantwortungsvoll zu bewerten und ggf. zu korrigieren.
- KI-Systeme können Vorurteile, stereotype Sprache oder diskriminierende Darstellungen erzeugen – z. B. bei automatisch formulierten Texten oder generierten Bildern.
- Wir prüfen deshalb alle KI-generierten Inhalte darauf, ob sie neutral, respektvoll und diskriminierungsfrei sind.

Jamillah Knowles / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

REGEL 8: ETHISCHE GRUNDLAGEN

- Auch Analysewerkzeuge und Bildgeneratoren stehen vor ähnlichen Herausforderungen. Ein Beispiel dafür ist die Tendenz einiger KI-Modelle, Bilder zu generieren, die sexistisch, bzw. diskriminierend sind oder Stereotypen bedienen.
- Prüfen Sie zudem auch, ob ein KI-Einsatz für die Bearbeitung der Aufgabe wirklich notwendig ist – viele Tools haben einen hohen Energieverbrauch.

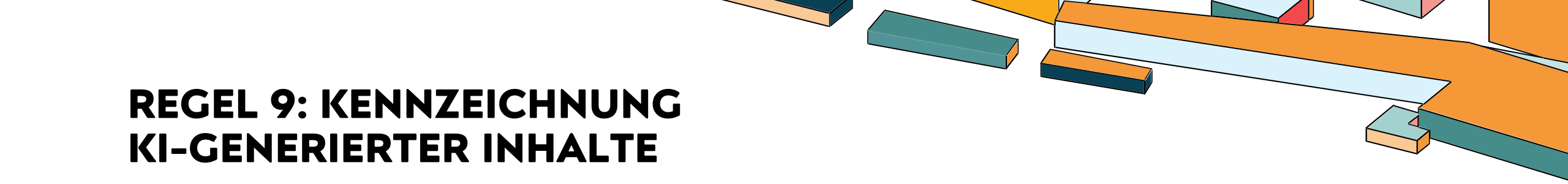
Adobe Firefly Eingabebefehl: Erstelle ein Bild von einem Geschäftstermin an einem langen Tisch in New York, fotorealistisch.



REGEL 9: KENNZEICHNUNG KI-GENERIERTER INHALTE

Bitte prüfen Sie, ob Ihre Einrichtung abweichende oder detailliertere Regelungen zur Nutzung erlassen hat.

- Wenn Inhalte mithilfe von KI erstellt oder wesentlich beeinflusst wurden, sollte dies transparent gemacht werden.
- Eine klare Kennzeichnung schafft Vertrauen – intern wie extern. Stellen Sie ggf. dar, wie KI Sie konkret bei der Erledigung der Aufgabe unterstützt hat, welche KI und welche Version sie verwendet haben und verweisen Sie auf die menschliche Qualitätskontrolle, z.B. in Form eines Disclaimers.
- Für interne Dokumente reicht oft ein Hinweis am Ende (z. B. ‚mit Unterstützung von KI erstellt').



REGEL 9: KENNZEICHNUNG KI-GENERIERTER INHALTE

Beispiel für einen Flyer-Text:

Dieser Text wurde mithilfe von ChatGPT 4.0 erstellt und unter den Gesichtspunkten der KI-Regelungen unserer Organisation sorgfältig von fachkundigen Personen überprüft und überarbeitet.

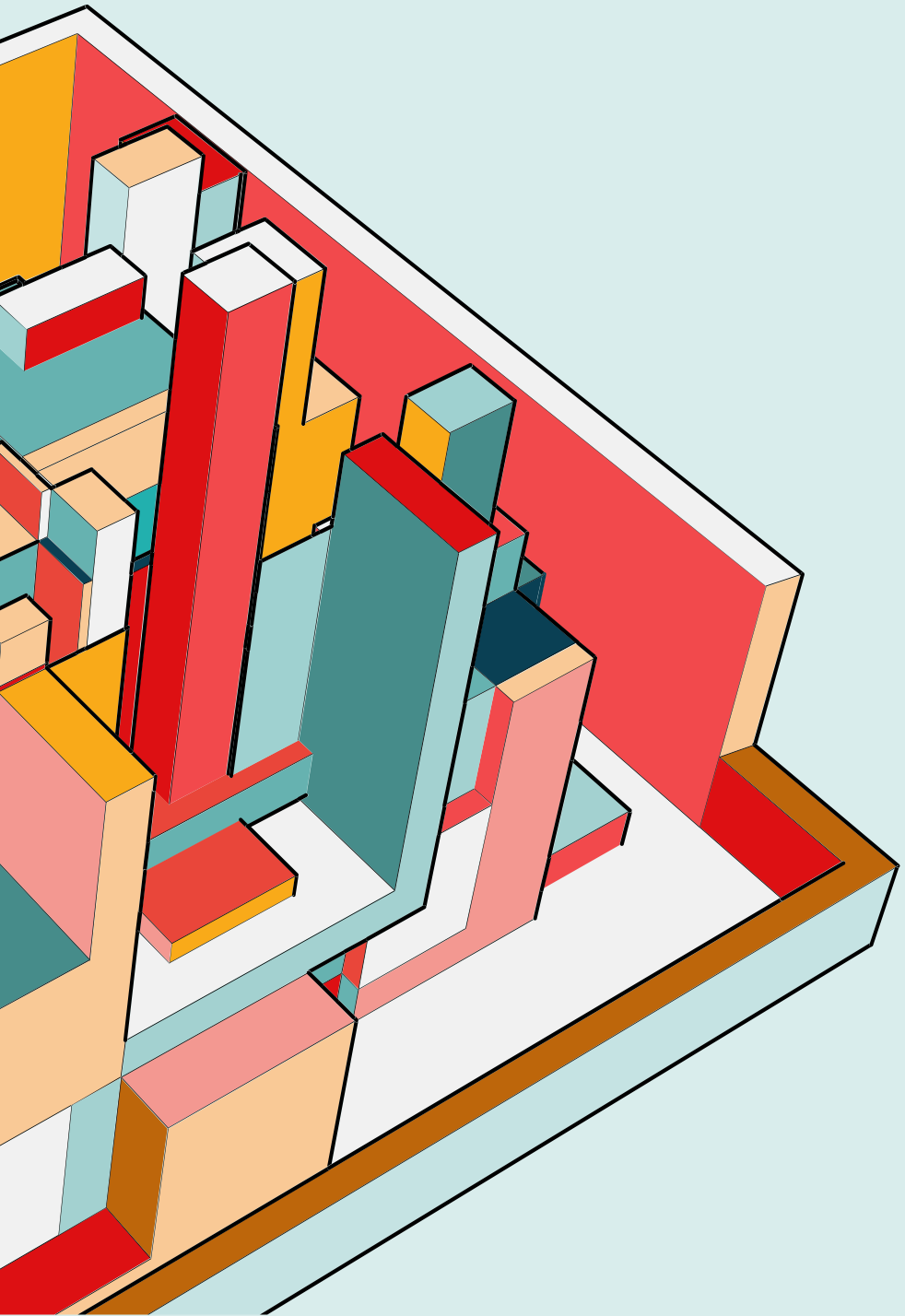
Beispiel für ein erstelltes Bild:

Dieses Bild wurde mithilfe von Dall-E erstellt und unter den Gesichtspunkten der KI-Regelungen unserer Organisation von fachkundigen Personen sorgfältig überprüft.

REGEL 10: AUS- UND WEITERBILDUNGEN ZU KÜNSTLICHER INTELLIGENZ

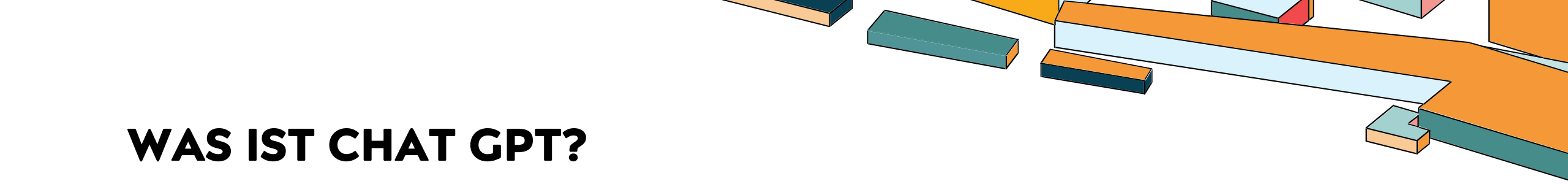
- Wir informieren uns regelmäßig in Schulungen zum verantwortungsbewussten Umgang mit generativer KI, falls diese in unserem Arbeitsalltag Anwendung finden.

- Schulungen helfen uns dabei…
  - ✓ *das Bewusstsein für die Chancen und Risiken des Einsatzes von KI zu schärfen.*
  - ✓ *das Risiko eines fahrlässigen und unbedachten Einsatzes zu verringern.*
  - ✓ *Überforderung durch technischen Fortschritt zu verhindern.*



TECHNISCHE EINFÜHRUNG

ChatGPT als Beispiel für die Verwendung von LLMs



WAS IST CHAT GPT?

Definition: ChatGPT ist ein fortschrittliches KI-Modell, entwickelt von OpenAI, das auf der GPT-Architektur (Generative Pre-trained Transformer) basiert.

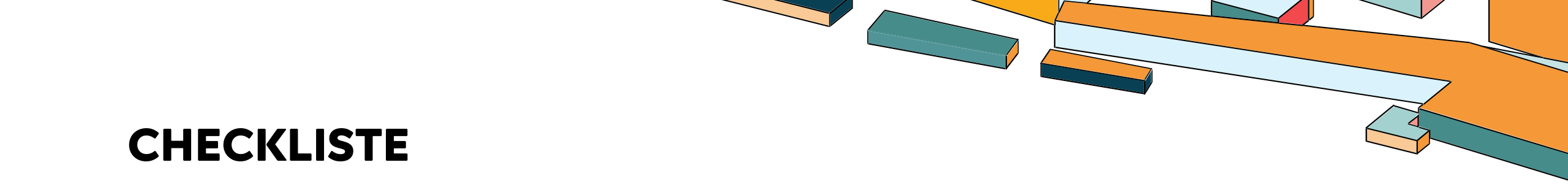
Funktionalität: Es verarbeitet und generiert Text, indem es natürliche Sprache versteht und darauf reagiert (Chat-Bot).

Technologie: ChatGPT verwendet maschinelles Lernen und Deep Learning, um menschenähnliche Texte zu erstellen.

Prompt: Bezeichnung für den Eingabebefehl innerhalb von Chat-Bots. Dieser kann per Text oder als Sprache erfolgen.

GPT: Bezeichnung für innerhalb von ChatGPT angelegte Miniprogramme, die festgelegte Regeln ausführen bzw. auf bestimmte Wissensquellen zugreifen

Konkurrenten: Gemini (Google), Copilot/Bing (Microsoft), Claude 3 (Anthropic), Writesonic (Chatsonic), Copy.ai, Character.ai, Deepseek



CHECKLISTE

1. Rechtliche Vorgaben prüfen:

- ✓ Wurden die Datenschutzvorgaben (DSGVO) und das Urheberrecht eingehalten?
- ✓ Wurde geprüft, ob das verwendete KI-Tool freigegeben und datenschutzkonform ist?

2. Risikoanalyse durchführen:

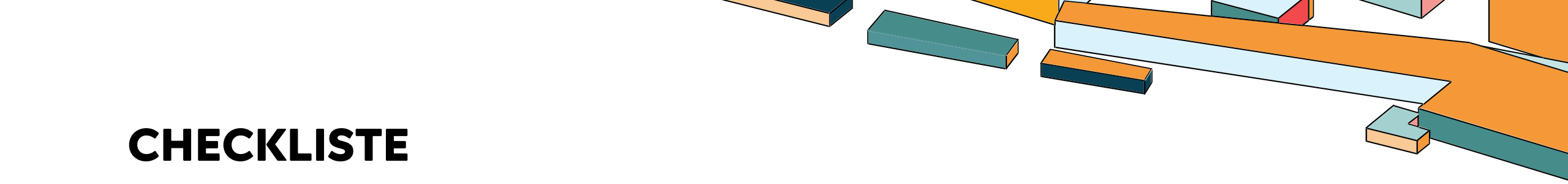
- ✓ Wurde geprüft, ob das eingesetzte KI-System als geringes, begrenztes oder hohes Risiko einzustufen ist (nach EU-KI-Verordnung)?
- ✓ Gibt es eine dokumentierte Bewertung möglicher Risiken?

3. Menschliche Kontrolle sicherstellen:

- ✓ Werden KI-generierte Inhalte immer von qualifizierten Personen geprüft (Richtigkeit, Kontext, Ethik)?
- ✓ Ist klar geregelt, wer die finale Entscheidung verantwortet?

4. Vertraulichkeit und Datenschutz gewährleisten:

- ✓ Werden keine vertraulichen oder personenbezogenen Daten ohne rechtliche Grundlage in KI-Systeme eingegeben?
- ✓ Werden sensible Daten (z. B. Geschäftsgeheimnisse) konsequent geschützt?



CHECKLISTE

5. Transparenz herstellen:

- ✓ Sind KI-gestützte Inhalte klar gekennzeichnet?
- ✓ Ist für alle Beteiligten erkennbar, wenn KI bei der Erstellung von Inhalten mitgewirkt hat?

6. Ethische Standards einhalten:

- ✓ Werden diskriminierende, stereotype oder unfaire Inhalte aktiv vermieden?
- ✓ Entspricht der KI-Einsatz den ethischen Leitlinien der Organisation?

7. Verantwortung übernehmen:

- ✓ Liegt die finale Verantwortung immer bei einer menschlichen Person, nicht beim KI-System?
- ✓ Wurden Zuständigkeiten für Prüfung, Freigabe und Monitoring klar definiert?

8. Kontinuierliche Weiterbildung sicherstellen:

- ✓ Gibt es regelmäßige Schulungen zu KI-Nutzung, Recht und Ethik für Führungskräfte und Teams?

VIELEN DANK

Kontakt:

info@ki-wisskom.de
www.ki-wisskom.de

KI-Hinweis:

Für die Erstellung diese Präsentation wurde ChatGPT 4.5 für die Rechtschreibkontrolle und Textredaktion genutzt.

Für die Vertonung des Videos wurde die KI elevenlab.io verwendet.

Alle KI-generierten oder -überarbeiteten Inhalte wurden von fachkundigen Personen überprüft.

Die vermittelten Inhalte dieser Schulung wurden sorgfältig recherchiert und zusammengestellt. Sie dienen der allgemeinen Information und Weiterbildung zum Thema "Einsatz von generativer KI - Recht, Ethik, Technik" zur Umsetzung einer Schulungspflicht, die sich aus der EU KI-Verordnung ergibt. Eine individuelle rechtliche Beratung im Einzelfall erfolgt nicht. Für die Umsetzung der erlernten Inhalte in der jeweiligen Organisation sind die Teilnehmenden selbst verantwortlich.