Römisch-Katholische
Kirche im Aargau

Künstliche Intelligenz (KI) – Merkblatt zur Nutzung

Die Anzahl von verfügbaren KI-Systemen wächst stetig und die zugrundeliegenden Technologien entwickeln sich rasant weiter Bei den meisten Systemen handelt es sich um eine sogenannte Blackbox. Nach aussen sind lediglich die Eingaben in das System und die Ausgaben des Systems sichtbar. Wie es zur Ausgabe gelangt, bleibt meist unklar und ist häufig nicht nachvollziehbar. Zudem ist der Wahrheitsgehalt der Ausgaben oft nicht nachprüfbar.

Generative KI-Modelle sind in der Lage, eine Vielzahl an Aufgaben durchzuführen, die traditionell Kreativität und menschliches Verständnis erfordern. Sie erlernen während des Trainings Muster aus vorhandenen Daten und können in der Folge neue Inhalte wie Texte, Bilder, Audios und Videos erzeugen, die ebenfalls diesen Mustern folgen.

Die Römisch-Katholische Kirche im Aargau (kommunikation@kathaargau.ch) hat dazu diese Empfehlungen für eine sichere Nutzung zusammengestellt:

Grundsatz

Bei der Nutzung von Systemen und Werkzeugen der Künstlichen Intelligenz gelten grundsätzlich die aktuellen Gesetze, wie das Datenschutzgesetz, der Persönlichkeitsschutz (Grundrechte, Menschenrechte, Diskriminierungsverbot) oder das Urheberrecht (Schutz des geistigen Eigentums). – siehe auch Mitteilung des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB): https://www.edoeb.admin.ch/de/09112023-geltendes-dsg-ist-auf-ki-anwendbar.

Empfehlungen

Adaptiert ab einer Übersicht von Paul Meyrat, Senior Digital Transformation Consultant, «eGovWeekly»:

1. Kontoeröffnung/Daten-Verwertung

Für die Anmeldung sollten geschäftliche Kontaktdaten verwendet werden. Die geschäftlichen und die private Nutzungen sollten getrennt werden. Dabei soll die Verwertung der eingegebenen Daten so weit wie möglich eingeschränkt werden: In jedem Tool, das genutzt wird, soll die Funktion aktiviert werden, dass die eingegebenen Daten nicht zum Training genutzt werden. Beispiel für ChatGPT: https://help.openai.com/en/articles/7730893-data-controls-faq.

2. Eingabe von Informationen

Personenbezogene Informationen (Namen etc.), geheime Informationen (Firmen-Interna) oder urheberrechtlich geschützte Inhalte dürfen nicht eingegeben werden. Berufsgeheimnisträger, z.B. Seelsorgende oder Mitglieder von Behörden haben besondere Vertraulichkeitsanforderungen.

3. Datenschutz und Vertraulichkeit

Der Datenschutz muss stets eingehalten werden. Das bedeutet, dass keine sensiblen Daten eingegeben werden dürfen und Daten anonymisiert werden sollen. Nutzerinnen und Nutzer von Systemen der Künstlichen Intelligenz müssen sich bewusst sein, dass die eingegebene Daten den eigenen Kontrollbereich verlassen und für andere Zwecke verwendet werden können.

4. Verwendung und Verifikation der Ergebnisse

Die von der Künstlichen Intelligenz generierten Ergebnisse sollten immer kritisch überprüft und nur als unterstützende Hilfestellung verwendet werden. KI sind lernende Systeme und machen Fehler. Ergebnisse können falsch oder unwahr sein.

5. Transparenz

Eine auf KI gestützte Entscheidungsfindung sowie die Interaktion mit KI-Systemen sollen als solche klar erkennbar sein. Es gibt aktuell keine Kennzeichnungspflicht (ausser bei sogenannten «Deep Fakes», den täuschend echten Videos, die irreführend sein können). Aber es wird empfohlen, mit KI generierte Werke oder den Einsatz KI auf Webseiten (z.B. in Chatbot-Dialogen) entsprechend zu kennzeichnen, denn Transparenz schafft Vertrauen.

6. Urheberrecht

Hier kann man unterscheiden zwischen A) Input: Wie erwähnt, dürfen bei der Eingabe keine urheberrechtlich geschützten Werke verwendet werden. Und B) Output: Ausschliesslich mit KI erstellte Werke gelten nicht als «geistige Schöpfung» und sind demzufolge auch nicht urheberrechtlich geschützt – erst, wenn KI nur als Basis/Input/Inspiration dient und das Werk durch die Nutzer wesentlich nachbearbeitet wird, kann das neugeschaffene Werk wieder Urheberschutz geniessen bei einer entsprechenden «Schöpfungshöhe». Siehe dazu auch den Beitrag von Suisa: https://blog.suisa.ch/de/kuenstliche-intelligenz-und-urheberrecht/

7. Nutzungsrecht

Bei der Nutzung gilt es, die Einschränkungen seitens der KI-Betreiber (Systeme) zu beachten, ob die verwendeten KI-Tools und -Services irgendwelche Rechte vorbehalten, ob dazu nichts gesagt wird oder ob es ausdrücklich erlaubt ist, dass der Output frei verwendet werden kann. Normalerweise enthalten die Nutzungsbedingungen (Terms and Conditions) entsprechende Regelungen. Meistens ist eine freie und damit auch kommerzielle Verwendung möglich (teilweise jedoch erst bei kostenpflichtigen Versionen/Abonnements). Hier als Beispiel der Link zu den ChatGPT-Nutzungsbedingungen in Deutsch: https://openai.com/de-DE/policies/eu-terms-of-use/.

Weiterführende Links

- datenschutzpartner.ch Know-how und Datenschutz-Generator für Datenschutzerklärungen
- vischer.com/kuenstliche-intelligenz Blog-Serie über den rechtskonformen und auch ethischen Einsatz von KI u.a. Gängige KI Tools – wie steht es um den Datenschutz?
- Leitlinien für den Umgang mit Künstlicher Intelligenz (KI) durch die Bundesverwaltung
- KI-Handlungsanweisungen SRF Schweizer Radio und Fernsehen
- Generative KI-Modelle, Chancen und Risiken inkl. Nutzungsmöglichkeiten: umfangreiches PDF des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI)