

Technisch-organisatorische Maßnahmen (TOMs) für den KI-gestützten Recherche-Dienst „KIRK“ in den Online-Diensten der Walhalla Mediengruppe

Im Rahmen des Online-Dienstes kommt ein KI-gestütztes Recherchetool mit dem Namen „KIRK“, ein generatives KI-System (im Folgenden: KI-System), zum Einsatz.

Dieses basiert auf dem Sprachmodell GPT-4 des Unternehmens OpenAI, L.L.C., und wurde ausschließlich mit den verlagseigenen, geprüften Inhalten (Kommentare, Erläuterungen, Vorschriften, Rechtsprechung usw.) des Online-Dienstes trainiert. Der Nutzer kann Fragen natürlicher Sprache an das KI-System richten.

Das KI-System verwendet ein RAG-System (retrieval augmented generation) zu Erstellung der Antworten anhand der Inhalte des Online-Dienstes. Zur Validierung der Antwort durch den Nutzer werden der Antwort die Fundstellen inklusive Verlinkung an die entsprechenden Volltexte mitgegeben. Der Nutzer kann die Antwort mit weiteren Fragen an das KI-System verfeinern (dialogische Nutzung).

Da das KI-System in den Online-Dienst implementiert ist, steht es nur Abonnentinnen und Abonnenten nach Anmeldung im Online-Dienst zur Verfügung.

Zur Sicherstellung der Vorgaben des EU-AI-Acts, des Datenschutzes und der Datensicherheit wurden folgende technisch-organisatorische Maßnahmen getroffen:

1. Zweckbindung und Datenminimierung

- Das KI-System dient ausschließlich der Recherche in verlagseigenen, geprüften Inhalten des Online-Dienstes.
- Personenbezogene Daten werden durch das KI-System weder verarbeitet noch gespeichert.
- Nutzeranfragen werden anonymisiert verarbeitet; es erfolgt keine Verknüpfung mit Namen, IP-Adressen oder anderen Identifikationsmerkmalen.

2. Technische Infrastruktur

- Die Datenverarbeitung erfolgt über die Azure-OpenAI-Schnittstelle (API) auf Servern von Microsoft innerhalb der Europäischen Union.
- Es findet keine Übermittlung personenbezogener Daten an Microsoft oder OpenAI statt.
- Die übermittelten Inhalte (Nutzeranfragen) werden nicht zur Weiterentwicklung oder zum Training von Sprachmodellen durch Microsoft oder OpenAI verwendet.

- Microsoft hat sich vertraglich verpflichtet, die über Azure-OpenAI verarbeiteten Daten nicht für Marketing- oder Analysezwecke zu nutzen.

3. Zugriffs- und Zugriffskontrollmanagement

- Der Zugriff auf die technische Schnittstelle (API) ist durch Authentifizierungsmechanismen abgesichert.
- Nur autorisierte Mitarbeiter des Verlages sowie autorisierte Mitarbeiter des technischen Dienstleisters haben Zugriff auf die technische Infrastruktur und die Administrationsbereiche der API-Anbindung.
- Rollen- und Rechtemanagement stellt sicher, dass nur notwendige Personen Zugriff auf die Konfiguration des Systems haben.

4. Vertraulichkeit und Integrität

- Die Kommunikation zwischen dem Online-Dienst und der Azure-OpenAI-API erfolgt verschlüsselt (TLS).
- Nutzeranfragen werden nur anonymisiert protokolliert und dienen der weiteren Verbesserung des Antwortverhaltens. Sie werden ausschließlich vom Verlag verarbeitet und nicht an Dritte weitergegeben.
- Feedback-Bewertungen zum Dienst sind freiwillig, werden ausschließlich vom Verlag verarbeitet und nicht an Dritte weitergegeben.

5. Transparenz und Kontrolle

- Nutzer werden im Online-Dienst transparent über den Einsatz des KI-Systems informiert, inklusive der Datenverarbeitung und ihrer Rechte.
- Die Geschäftsbedingungen von OpenAI sowie ergänzende Informationen zur Datenverarbeitung sind öffentlich einsehbar.
- Die eingesetzten technischen Systeme werden regelmäßig auf Sicherheit und Funktionalität überprüft.

6. Folgeabschätzungen und Auftragsverarbeitung

- Bezüglich der Entwicklung und Betreiben des KI-Systems wurde eine Datenschutzfolgeabschätzung sowie eine KI-Risikoabschätzung durchgeführt.
- Die Datenverarbeitung erfolgt im Rahmen einer vertraglich geregelten Auftragsverarbeitung mit Microsoft (Azure-OpenAI).
- Es besteht ein Auftragsverarbeitungsvertrag mit den eingesetzten Dienstleistern.

Regensburg, 25. Juli 2025