krz/Microsoft

Große Sprachmodelle für die Verwaltung

[15.08.2023] Große Sprachmodelle – KI-Lösungen wie ChatGPT und Co. – bergen viel Potenzial für den Einsatz bei der öffentlichen Verwaltung. Bestehende Sicherheitsbedenken adressiert nun das Innovation Lab beim Kommunalen Rechenzentrum Minden-Ravensberg/Lippe (krz), an dem sich auch Microsoft beteiligt.

In Zusammenarbeit mit Microsoft Deutschland hat das Kommunale Rechenzentrum Minden-Ravensberg/Lippe (krz) Anfang Juli unter der Leitung von Christian Beermann, dem stellvertretenden Bereichsleiter Digitalisierung und Innovation und Leiter der Softwareentwicklung, ein Innovation Lab ins Leben gerufen. Ziel ist es laut krz, generative Große Sprachmodelle (auch bekannt als Large Language Models – kurz: LLM) auf Basis eigener Unternehmensdaten nutzbar zu machen, ohne diese an Drittanbieter zu übertragen.
Als erster öffentlicher IT-Dienstleister habe das krz Zugriff auf die Azure Cloud Open AI Services von Microsoft erhalten, die beispielsweise ChatGPT, Dall-E und Codex als KI-Modelle beinhalten. Das Datenschutzteam des krz habe bei der Umsetzung erster Prototypen tatkräftige Unterstützung geleistet und erarbeite derzeit Standards, um künftige Anwendungsfälle von Verbandsmitgliedern und Kommunen schnellstmöglich in eigenen Anwendungen nutzbar zu machen.?Die nun entwickelten Prototypen-Apps sollen es den Verwaltungsmitarbeiterinnen und -mitarbeitern ermöglichen, eigene Daten wie Word-, Excel-, PowerPoint- und PDF-Dateien sowie Unternehmens-Wikis und Datenbanken an die großen Sprachmodelle anzuschließen.

Datenschutzkonformer LLM-Einsatz

Die Nutzung großer Sprachmodelle in der öffentlichen Verwaltung eröffne immense Möglichkeiten zur Effizienzsteigerung und zur Verbesserung der Kommunikation mit Bürgerinnen und Bürgern, sagt die krz-Bereichsleiterin für Digitalisierung und Innovation, Michaela Lehnert. Allerdings bestünden häufig Bedenken hinsichtlich des Datenschutzes und der Datenübertragung an Dritte. Das Innovation Lab des krz habe eine wegweisende Lösung entwickelt, um dieser Situation zu begegnen, so Lehnert.?Dabei wurde mit dem Konzept der so genannten Augmented Recommender Systems erstmalig ein hochmoderner Ansatz zur Erprobung großer Sprachmodelle für die öffentliche Verwaltung angewendet. Dieser erlaube es, datenschutzkonform auf Unternehmensdaten zuzugreifen und auf dieser Basis Empfehlungen und Antworten zu generieren.
Die enge Zusammenarbeit zwischen dem krz Lemgo, Microsoft Deutschland, OpenAI und dem Datenschutzteam habe es ermöglicht, eine wegweisende Initiative zur Nutzung großer Sprachmodelle in der öffentlichen Verwaltung zu erproben. Durch den Einsatz von Augmented Recommender Systems und die Einbindung eigener Unternehmensdaten wird der Datenschutz laut krz gewährleistet und die Kontrolle über sensible Informationen bleibt nachweislich in den Händen der Verwaltung.

(sib)

Stichwörter: IT-Infrastruktur,