

ANFRAGE von Gabriel Mäder (GLP, Adliswil), Michael Biber (FDP, Bachenbülach) und Roman Schmid (SVP, Opfikon)

Betreffend Verwaltungsdaten für KI sicher und zuverlässig nutzbar machen

Mit «SynerKI» baut der Kanton Zürich eine zentrale KI-Serviceplattform auf, die künftig auch den Einsatz von KI mit schützenswerten Daten ermöglichen soll. Bisherige Pilotprojekte zeigen jedoch Grenzen. Beim Rechercheassistenten des Gemeindeamtes (GAZ) durfte nur auf Informationen ohne Schutzbedarf zugegriffen werden, was die verfügbare Wissensbasis und teilweise die Qualität der Antworten einschränkte. Auch beim Projekt «KI bei Baubewilligungen» werden Fehlauskünfte aufgrund falsch interpretierter Daten oder Halluzinationen als Risiko bezeichnet.

Einen möglichen Ansatz bieten Retrieval-Augmented-Generation-Systeme (RAG). Sie stützen Antworten auf definierte Wissensbestände, können Halluzinationen reduzieren und erlauben eine rollenbasierte Steuerung des Zugriffs. Der Kanton Zug setzt dies seit August 2026 beim öffentlichen Voicebot «Nick 2.0» des Strassenverkehrsamts ein.

Damit stellt sich die Frage, wann KI lediglich ein neues technisches Hilfsmittel für eine bereits zulässige Datenbearbeitung darstellt und wann zusätzliche Rechtsgrundlagen erforderlich sind. Davon zu unterscheiden ist die Nutzung von Verwaltungsdaten zum Training von KI-Modellen sowie für Bewertungen und Entscheidungsunterstützung.

Der Regierungsrat wird deshalb um die Beantwortung folgender Fragen gebeten:

1. Reichen die bestehenden Rechtsgrundlagen für den Einsatz von RAG und vergleichbaren KI-Systemen durch öffentliche Organe zur Erfüllung ihrer gesetzlichen Aufgaben aus? Wo sieht der Regierungsrat zusätzlichen Regelungsbedarf?
2. Unter welchen Voraussetzungen dürfen bestehende Verwaltungsdaten, einschliesslich Personendaten und besonderen Personendaten, für Training, Fine-Tuning, Evaluation und Weiterentwicklung von KI-Systemen genutzt werden? Sind dafür einheitliche kantonale Rechtsgrundlagen möglich?
3. Welche technischen und organisatorischen Massnahmen sind erforderlich, damit RAG-basierte Chatbots analog zu «Nick 2.0» auch gegenüber Bevölkerung und Unternehmen eingesetzt werden können und Fehlauskünfte bzw. Halluzinationen ausreichend begrenzt werden?

Gabriel Mäder
Michael Biber
Roman Schmid