

Kleine Anfrage

der Abgeordneten Robin Jünger, Ruben Rupp und der Fraktion der AfD

Agentische KI und vollständige Verwaltungsentscheidungsprozesse in der Bundesverwaltung

Die Bundesregierung verknüpft ihre Vorhaben zur Digitalisierung und Staatsmodernisierung mit dem Anspruch, staatliche Entscheidungs-, Prozess- und Organisationsstrukturen grundlegend zu modernisieren. Der Koalitionsvertrag zwischen CDU, CSU und SPD sieht hierfür ausdrücklich eine grundlegende Modernisierung der Verwaltung, Bürokratierückbau, Ziel- und Wirkungsorientierung sowie Effizienzsteigerungen durch Digitalisierung vor (KoaV-2025-Gesamt-final-0424.pdf). Im Koalitionsvertrag zwischen CDU, CSU und SPD wird das Ziel formuliert, Verwaltungsleistungen zu digitalisieren, barrierefrei anzubieten und die Verwaltung vernetzt, effizient, leistungsfähig, niedrigschwellig und nutzerfreundlich auszugestalten. Darüber hinaus soll Deutschland als KI-Nation etabliert werden. Dies umfasst insbesondere massive Investitionen in Cloud- und KI-Infrastruktur sowie in die Verbindung von KI und Robotik (ebd.).

Vor diesem Hintergrund gewinnt der Einsatz agentischer KI-Systeme in der Bundesverwaltung eine besondere Bedeutung. Unter agentischen KI-Systemen werden im fachlichen Diskurs regelmäßig Anwendungen verstanden, die nicht lediglich isolierte Antworten erzeugen, sondern auf Zielvorgaben hin mehrschrittige Handlungsabläufe planen, externe Werkzeuge oder Datenquellen einbeziehen, Informationen beschaffen, Zwischenergebnisse bewerten und komplexe Aufgabenketten mit einem hohen Grad operativer Eigenständigkeit ausführen können (www.ibm.com/de-de/think/topics/agent-ai). Nach Auffassung der Fragesteller eröffnen sich einerseits erhebliche Rationalisierungs-, Beschleunigungs- und Standardisierungspotenziale für die öffentliche Verwaltung. Andererseits entstehen neue rechtsstaatliche und organisatorische Risiken, sofern solche Systeme Verwaltungsvorgänge nicht nur unterstützen, sondern strukturieren, priorisieren, rechtlich vorbereiten oder zum Beispiel Bescheidentwürfe erzeugen. Mit zunehmender funktionaler Tiefe des KI-Einsatzes in der Bundesverwaltung stellen sich daher umso nachdrücklicher Fragen nach Verantwortungszurechnung, menschlicher Kontrolle, tragfähiger Rechtsgrundlage, Datenzugriff, IT-Sicherheit, Fehlerkorrektur, Aktenmäßigkeit, Transparenz, Rechtsschutzfähigkeit und parlamentarischer Nachprüfbarkeit.

Die Bundesregierung hat in ihrer Antwort zu Frage 17 auf Bundestagsdrucksache 21/5842 ausgeführt, Ziel des Agentic AI Hubs sei nicht nur eine Vernetzung von Marktakteuren und Verwaltung, sondern auch die Entwicklung eines Vehikels, das den Einsatz agentischer KI-Systeme skalierbar mache. Ferner erklärte sie, ein Fahrplan für das weitere Vorgehen werde im Rahmen eines laufenden Vorgangs erarbeitet. Für die Pilotierung agentischer KI-Lösungen sei im Rahmen der Beauftragung der DigitalService GmbH ein Sachkostenbudget von maximal 500 000 Euro vereinbart worden. Davon seien 212 849 Euro für die

unmittelbare Pilotierung der Pilotprojekte veranschlagt. Die Bundesregierung erklärte zudem, inwiefern diese Mittel auch für Verstetigung oder Nachnutzung zur Verfügung gestellt werden könnten, sei Gegenstand laufender Überlegungen. Offensichtlich will die Bundesregierung Start-ups und kleine und mittlere Unternehmen (KMU) stärker in staatliche Innovations- und Digitalisierungsprojekte einbeziehen. Der Agentive AI Hub soll offenbar auch als Schnittstelle zwischen Verwaltung und Marktakteuren dienen.

Auf die Schriftliche Frage 120 auf Bundesdrucksache 21/5846 antwortete die Bundesregierung, das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) habe sich zum Ziel gesetzt, moderne, leistungsfähige und innovative Verwaltungsprozesse mit KI zu unterstützen. Derzeit stünden Unterstützungsleistungen unter Beachtung der Maßgabe „Human in the Loop“ im Vordergrund. Ob und wann ein Verwaltungsentscheidungsprozess vollständig von KI durchgeführt werden könne, hänge von verschiedenen Faktoren ab. Genannt wurden technische Umsetzungsmöglichkeit, Rechtsgrundlagen zur Datenverarbeitung, Grundrechtsrelevanz der Entscheidungen, ausreichende menschliche Aufsicht im Sinne des Artikels 14 der Verordnung (EU) 2024/1689, Nachvollziehbarkeit von Entscheidungen und IT-Sicherheit.

Diese Antwort benennt zwar einzelne relevante Prüffaktoren, lässt aber den Kern der Frage offen. Nicht mitgeteilt wurde, ob die Bundesregierung konkrete Vorhaben plant, prüft oder ausschließt, bei denen KI-Systeme vollständige Verwaltungsentscheidungsprozesse übernehmen sollen. Ebenfalls offen blieb, ob es bereits eine Roadmap, Projektliste, ressortübergreifende Abstimmung, technische Architektur, rechtliche Bewertung oder Evaluation für agentische KI in der Bundesverwaltung gibt. Auch wurde nicht beantwortet, ob die Bundesregierung einen Zeitpunkt oder jedenfalls Meilensteine erwartet, zu denen agentische KI-Systeme über bloße Unterstützungsleistungen hinausgehen könnten.

Agentische KI im Verwaltungskontext unterscheidet sich qualitativ von einfachen Assistenzsystemen. Ein KI-System, das nur Textbausteine vorschlägt, wirft andere Fragen auf als ein System, das selbstständig Akten durchsucht, externe Datenquellen abfragt, Rechtsnormen zuordnet, Ermessenskriterien gewichtet, Entscheidungsvorschläge erstellt oder Bescheide generiert. Gerade wenn der Staat solche Systeme im Kontakt mit Bürgern und Unternehmen einsetzt, muss frühzeitig geklärt werden, ob menschliche Verantwortung tatsächlich wirksam bleibt oder lediglich nachträglich formalisiert wird.

Wir fragen die Bundesregierung:

1. Welche Definition von „agentischer KI“ oder „Agentive AI“ verwendet die Bundesregierung im Zusammenhang mit dem Agentive AI Hub und vergleichbaren Vorhaben der Bundesverwaltung?
2. Welche konkreten Funktionen, Fähigkeiten oder Autonomiegrade müssen nach Auffassung der Bundesregierung vorliegen, damit ein KI-System als agentisch gilt?
3. Welche konkreten Vorhaben, Pilotprojekte, Marktdialoge, Tests, Prototypen oder Konzeptstudien zum Einsatz agentischer KI in der Bundesverwaltung gibt es derzeit?
4. Welche dieser Vorhaben betreffen ausschließlich unterstützende Tätigkeiten, und welche betreffen Verfahrensschritte mit unmittelbarer Relevanz für Verwaltungsentscheidungen?
5. Welche Bundesministerien, Bundesbehörden, bundeseigenen Unternehmen, Projektträger oder sonstigen Stellen sind am Agentive AI Hub beteiligt?

6. Welche Rolle nimmt das BMDS beim Agentic AI Hub ein, und welche Aufgaben wurden der DigitalService GmbH des Bundes konkret übertragen?
7. Welche Verträge, Verwaltungsvereinbarungen, Leistungsbeschreibungen, Projektaufträge oder sonstigen Beauftragungsdokumente liegen dem Agentic AI Hub zugrunde?
8. Welche Gesamtkosten sind für den Agentic AI Hub für die Jahre 2025, 2026, 2027 und 2028 jeweils geplant, veranschlagt, gebunden oder bereits verausgabt?
9. Aus welchen Haushaltstiteln werden der Agentic AI Hub und vergleichbare Vorhaben agentischer KI finanziert?
10. Welche Mittel des in der Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 21/5842 genannten Sachkostenbudgets von maximal 500 000 Euro wurden bisher konkret wofür verausgabt, und welche konkreten Leistungen wurden für die in der Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 21/5842 genannten 212 849 Euro zur unmittelbaren Pilotierung konkret beauftragt oder erbracht?
11. Welche Kriterien verwendet die Bundesregierung, um Start-ups, KMU, Forschungseinrichtungen oder sonstige Anbieter für eine Beteiligung am Agentic AI Hub auszuwählen, welche konkreten vergaberechtlichen Verfahren wurden für Leistungen im Zusammenhang mit dem Agentic AI Hub durchgeführt, und welche Auftragswerte, Zuschlagsempfänger und Leistungsgegenstände ergaben sich jeweils?
12. Welche Anforderungen stellt die Bundesregierung beim Agentic AI Hub an Open Source, offene Standards, Portabilität, Interoperabilität und Vermeidung von Anbieterabhängigkeiten, und welche konkreten Datenbestände der Bundesverwaltung werden oder sollen im Rahmen des Agentic AI Hub für Training, Test, Evaluation, Prompting, Retrieval-Augmented Generation oder sonstige Systemfunktionen genutzt werden?
13. Welche personenbezogenen, vertraulichen, sicherheitsrelevanten oder VS (Verschlusssache)-eingestuften Daten sind von Vorhaben des Agentic AI Hub ausgeschlossen, und welche Datenschutzfolgenabschätzungen, IT-Sicherheitskonzepte, Bedrohungsanalysen oder Grundrechtefolgenabschätzungen wurden für Vorhaben agentischer KI erstellt?
14. Welche Rolle spielen das Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, das Informationstechnikzentrum Bund (ITZBund) und die Rechtsabteilungen der Ressorts bei der Prüfung agentischer KI-Vorhaben?
15. Welche konkreten Bewertungskriterien werden in der von der Bundesregierung genannten Evaluation des Agentic AI Hub verwendet?
16. Welche messbaren Zielwerte bestehen für technische Leistungsfähigkeit, fachliche Leistungsfähigkeit, Rechtskonformität, Skalierbarkeit, Wirtschaftlichkeit, Bearbeitungsdauer, Fehlerquote und Nutzerzufriedenheit?
17. Wann soll der in der Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 21/5842 erwähnte Fahrplan für das weitere Vorgehen beim Agentic AI Hub abgeschlossen werden?
18. Welche Meilensteine enthält oder soll dieser Fahrplan nach dem aktuellen Planungsstand enthalten?

19. Welche Entscheidungskriterien gelten für die Überführung einzelner Pilotprojekte in eine breitere Pilotierung, einen Wirkbetrieb oder einen Regelbetrieb?
20. Welche Stellen entscheiden jeweils über Fortführung, Skalierung, Abbruch oder Regelbetrieb agentischer KI-Projekte, und welche konkreten Verwaltungsentscheidungsprozesse hält die Bundesregierung für geeignet, künftig vollständig oder weitgehend durch KI-Systeme durchgeführt zu werden?
21. Welche Verwaltungsentscheidungsprozesse hält die Bundesregierung wegen Grundrechtsrelevanz, Ermessensausübung, hoher Fehlerfolgen, fehlender Nachvollziehbarkeit oder besonderer Schutzbedürftigkeit Betroffener für ungeeignet?
22. Plant, prüft oder erprobt die Bundesregierung derzeit Systeme, die Sachverhaltsermittlung, rechtliche Bewertung, Ermessensvorbereitung, Ermessensausübung und Bescheiderstellung in einem integrierten KI-gestützten Prozess verbinden?
 - a) Wenn ja, welche Ressorts, Behörden, Fachverfahren und Rechtsbereiche sind betroffen?
 - b) Wenn nein, weshalb hat die Bundesregierung in ihrer Antwort auf die Schriftliche Frage 120 auf Bundestagsdrucksache 21/5846 nicht ausdrücklich klargestellt, dass entsprechende Vorhaben derzeit nicht bestehen?
23. Wie stellt die Bundesregierung sicher, dass „Human in the Loop“ bei agentischen KI-Systemen nicht lediglich eine nachträgliche Bestätigung eines faktisch bereits durch KI vorentschiedenen Ergebnisses bedeutet, und welche konkreten organisatorischen Vorgaben bestehen für Beschäftigte der Bundesverwaltung, die Ergebnisse agentischer KI-Systeme prüfen, ändern, verwerfen oder freigeben sollen?
24. Welche Qualifikations-, Schulungs- und Fortbildungsanforderungen gelten für Beschäftigte, die agentische KI-Systeme in Bundesverwaltungsverfahren einsetzen, und welche Protokollierungs-, Dokumentations- und Aktenführungspflichten gelten für Zwischenschritte agentischer KI-Systeme?
25. Wie wird sichergestellt, dass bei agentischen KI-Systemen sämtliche relevanten Eingaben, Zwischenschritte, Tool-Nutzungen, Datenabrufe, Modellversionen und Ausgaben nachträglich überprüfbar bleiben, und welche Rechtsgrundlagen hält die Bundesregierung für erforderlich, bevor agentische KI-Systeme Verwaltungsentscheidungen vollständig oder weitgehend übernehmen können?
26. Plant die Bundesregierung Änderungen des Verwaltungsverfahrensgesetzes, des E-Government-Gesetzes, fachgesetzlicher Regelungen oder haushaltsrechtlicher Vorgaben, um agentische KI in Verwaltungsverfahren zu ermöglichen oder zu begrenzen?
27. Welche Haftungs-, Verantwortungs- und Zurechnungsfragen hat die Bundesregierung für den Fall geprüft, dass ein agentisches KI-System fehlerhafte, rechtswidrige oder diskriminierende Ergebnisse erzeugt?
28. Welche Melde- und Abhilfeverfahren sind vorgesehen, wenn agentische KI-Systeme in Pilotierung oder Betrieb Fehlentscheidungen, Sicherheitsvorfälle, Datenschutzverstöße oder systematische Verzerrungen verursachen?

29. Welche Rolle soll der Agentic AI Hub für Start-ups und KMU konkret spielen, und wie verhindert die Bundesregierung, dass nur wenige große Anbieter mit bestehender Marktmacht von staatlichen KI-Projekten profitieren?
30. Weshalb hat die Bundesregierung in ihrer Antwort auf die Schriftliche Frage 120 auf Bundesdrucksache 21/5846 weder einen konkreten Planungsstand einzelner Vorhaben noch einen belastbaren Zeitplan für vollständige KI-gestützte Verwaltungsentscheidungsprozesse benannt?

Berlin, den 24. Juli 2026

Dr. Alice Weidel, Tino Chrupalla und Fraktion

