



HESSISCHER LANDTAG

17. 06. 2024

Kleine Anfrage

Oliver Stirböck (Freie Demokraten) vom 22.04.2024**Hessens AI Quality und Testing Hub GmbH als Mitglied im US-amerikanischen Sicherheitskonsortium****und**

Antwort

Ministerin für Digitalisierung und Innovation

Vorbemerkung Fragesteller:

Im April 2024 hat Digitalministerin Kristina Sinemus verkündet, dass der AI Quality und Testing Hub GmbH (AIQ), mit dem Unternehmen die Qualität von Künstlicher Intelligenz messen und verbessern können, Mitglied im neu gegründeten „US AI Safety Institute Consortium“ geworden sei.

Vorbemerkung Ministerin für Digitalisierung und Innovation:

Die Landesregierung hat in der Strategie „Digitales Hessen – Wo Zukunft zuhause ist“ und in der hessischen KI-Zukunftsagenda den Anspruch formuliert, „KI made in Hessen“ zu einem Markenzeichen unseres Landes zu machen. Dafür bedarf es eines starken KI-Ökosystems, für dessen Entwicklung die Landesregierung bereits viel getan hat und weiterhin tut.

Ein besonderer Schwerpunkt wurde dabei stets auf KI-Qualität gelegt, denn diese ist zentral für die Marktfähigkeit von KI-Produkten, aber auch für die öffentliche Akzeptanz dieser Technologie. Damit positionierte sich die Landesregierung frühzeitig zu einem Thema, das auch ein zentrales Anliegen der europäischen KI-Verordnung ist (siehe Antwort auf die Kleine Anfrage, Drucks. 21/200). Die AI Quality und Testing Hub GmbH („der AIQ“), die das Land Hessen im Dezember 2022 gemeinsam mit dem VDE (Verband der Elektrotechnik Elektronik Informations-technik) gründete, ist ein wichtiges Element der hessischen KI-Zukunftsagenda. Der AIQ bietet Dienstleistungen in Beratung und Weiterbildung an und entwickelt Testverfahren und -werkzeuge, um seine Kunden bei der Entwicklung hochqualitativer, vertrauenswürdiger KI-Technologie zu unterstützen. Im April 2024 wurde der AIQ in das AI Safety Institute Consortium des National Institute of Standards and Technology (NIST) aufgenommen, eine nachgeordnete Behörde des US-Handelsministeriums, deren Hauptaufgaben in den Bereichen Normung und Standardisierung liegen. In seiner „Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence“ (EO 14110) vom 30.10.2023 hat US-Präsident Biden das NIST u. a. damit beauftragt, Richtlinien, Standards und Best Practices für KI-Sicherheit zu entwickeln. Anfang November 2023 wurden die Gründung des AI Safety Institutes innerhalb von NIST sowie der Aufbau des US AI Safety Institute Consortiums (US AISIC) verkündet. Das Konsortium ist als öffentlich-private Partnerschaft konzipiert, in welcher Expertinnen und Experten, Unternehmen und Forschungsinstitutionen ihren Input in die Entwicklung von Risikomanagement-Richtlinien geben sollen.

Diese Vorbemerkungen vorangestellt beantworte ich die Kleine Anfrage wie folgt:

Frage 1 Welche Kriterien, Qualifikationen oder sonstigen Eigenschaften musste der AIQ erfüllen, um die Kriterien für die Aufnahme in das US AI Safety Institute Consortium zu erreichen?

Der Bewerbungsprozess lief über einen offenen Aufruf auf dem Internetauftritt des NIST. Interessierte Organisationen hatten 75 Tage Zeit (zwischen dem 02.11.2023 und dem 15.01.2024), um eine Interessenbekundung einzureichen. Das NIST erhielt in dieser ersten Runde über 600 Interessenbekundungen von Organisationen weltweit, v. a. aus den Vereinigten Staaten. Das NIST wählte die Organisationen anhand ihrer Fähigkeiten und Erfahrungen im Bereich AI Safety (KI-Sicherheit) aus. Der AIQ wurde ausgewählt, in den Arbeitsgruppen zu KI-Red-Teaming-Guidelines, Vorschriften für Testroutinen und Infrastrukturanforderungen für das Testen von KI-Anwendungen mitzuarbeiten.

Frage 2 Welche Institutionen und Unternehmen sind ebenfalls Mitglied beim US AI Safety Institute Consortium?

Die vollständige Mitgliederliste findet sich auf der Webseite des NIST:
→ <https://www.nist.gov/artificial-intelligence/artificial-intelligence-safety-institute/aisic-members>. Sie wird regelmäßig aktualisiert. Am 03.05.2024 wurden dort 285 Unternehmen, Forschungseinrichtungen und andere Institutionen als Mitglieder genannt. Dazu gehören namhafte Unternehmen wie z. B. OpenAI, Meta oder NVIDIA, sowie Universitäten wie Princeton oder das MIT.

Frage 3 Welche finanziellen Verpflichtungen ergeben sich aus der Mitgliedschaft des AIQ für das Land Hessen?

Es ergeben sich keine finanziellen Verpflichtungen für das Land Hessen.

Frage 4 In welcher Form wird die Effizienz der Mitgliedschaft überprüft?

Das intendierte Ziel der Mitgliedschaft ist eine enge Vernetzung des AIQ mit der US-amerikanischen Industrie und den dortigen Behörden. Als weltweit stärkste KI-Nation könnten sich die USA zu einem wichtigen Markt für den AIQ entwickeln. Als Gradmesser für die Effizienz der Mitgliedschaft sind daher Kontakte, Kooperationsbeziehungen und Aufträge zu sehen, die in diesem Kontext entstehen.

Frage 5 Welchen konkreten Einfluss hat der AIQ auf die Formulierung von Politiken und Richtlinien im Konsortium?

Das Konsortium ist als Forschungspartnerschaft konzipiert, in der die beteiligten Akteure in fachbezogenen Arbeitsgruppen Teilaspekte von AI Safety behandeln. Die Forschungsergebnisse fließen in die Entwicklung von Politiken, Standards und Richtlinien ein. Der Einfluss des AIQ beschränkt sich dabei auf die Mitarbeit in ausgewählten Arbeitsgruppen.

Frage 6 Wie sollen die hessischen Interessen im amerikanischen Konsortium konkret vertreten werden?

Die Landesregierung steht für verantwortungsbewusste KI-Innovation, wie es u. a. in der hessischen Digitalstrategie und in der KI-Zukunftsagenda ausgeführt wurde. Internationale Zusammenarbeit und innovationsfreundliche Regulierung sind wesentliche Eckpunkte der hessischen KI-Strategie. Der AIQ handelt auf Basis dieser Werte und wird entsprechende Positionen in das Konsortium einbringen.

Frage 7 In welcher Weise soll sichergestellt werden, dass die deutschen und europäischen Datenschutzvorschriften, die sich von den amerikanischen Vorschriften deutlich unterscheiden, innerhalb des Konsortiums beachtet werden?

Der AIQ wird in den Arbeitsgruppen, in denen er mitwirkt, sachgerecht die deutsche und europäische Perspektive zum Datenschutz einbringen.

Frage 8 In welcher Weise soll Hessen durch welchen konkreten Projekte, Initiativen oder Verbesserungen von der Mitgliedschaft profitieren?

Die Mitgliedschaft im US AISIC ist eine Auszeichnung für die Expertise des AIQ und kann von diesem für die Außendarstellung genutzt werden. Ferner baut der AIQ durch die im AISIC gewonnenen Kontakte sein internationales Netzwerk aus. Auf diese Weise positioniert sich der AIQ frühzeitig zur Debatte um KI-Sicherheit, die auch in Deutschland weiter an Dynamik gewinnen wird. Letztlich kann der AIQ die im Rahmen der Zusammenarbeit gewonnenen Erfahrungen auch für die Weiterentwicklung seiner Produkte bzw. die weitere Verbesserung der KI-Qualität nutzen.

Frage 9 In welcher Weise soll die Öffentlichkeit über die Tätigkeiten des AIQ im Rahmen des Konsortiums informiert werden?

Der AIQ informiert über seine Tätigkeit im US AISIC im Rahmen seiner Öffentlichkeitsarbeit, insbesondere über die eigene Webseite sowie auf LinkedIn. Außerdem informiert der AIQ das HMD im Rahmen seiner üblichen Berichtspflichten.

Frage 10 Welche langfristigen Ziele verfolgt die Landesregierung mit der Teilnahme am Konsortium?

Die Landesregierung hat mit dem AIQ einen wichtigen Eckpfeiler des hessischen KI-Ökosystems geschaffen. Die internationale Vernetzung, wie sie im Rahmen der Teilnahme am US AISIC erfolgt, ist dabei als normaler Bestandteil der unternehmerischen Tätigkeit des AIQ zu betrachten. Langfristig sollen aus der US AISIC-Mitgliedschaft Geschäftsbeziehungen sowie Kooperationen entstehen, die der AIQ zur Verfolgung der von den Gesellschaftern gesteckten Zielen nutzen kann. Ferner kann der AIQ im US AISIC einen Beitrag zur Entwicklung von Standards zu KI-Sicherheit leisten, welche auch außerhalb der Vereinigten Staaten sichtbar und wirksam werden.

Wiesbaden, 24. Mai 2024

Prof. Dr. Kristina Sinemus