Positionspapier
Deutschlands Wettbewerbsfähigkeit bei KI sichern

Die IBM begrüßt die KI-Verordnung, im Besonderen ihren risikobasierten Ansatz, die Anerkennung der unterschiedlichen Rollen entlang der KI-Wertschöpfungskette bei der Beurteilung der Haftung, die an die OECD angelehnte Definition von KI und die Würdigung der Rolle von Open Source.

Nicht alle Anwendungen von KI bergen das gleiche Risiko. Während einige harmlos erscheinen mögen, können andere weitreichende Folgen haben, wie etwa die Verbreitung von Fehlinformationen, die Einführung von Voreingenommenheit bei Kreditentscheidungen oder die Beeinträchtigung der Wahlintegrität. Da jede KI-Anwendung einzigartig ist, sind wir der festen Überzeugung, dass die Regulierung den Kontext berücksichtigen muss, in dem KI eingesetzt wird, und sicherstellen muss, dass die risikoreichen Anwendungen von KI strenger reguliert werden („Regulate AI risks, not AI algorithms"). Die Gesetzgebung sollte die unterschiedlichen Rollen von KI-Entwicklern und KI-Anwendern berücksichtigen und sie in dem Kontext, in dem sie KI entwickeln oder einsetzen, zur Verantwortung ziehen („Make AI creators and deployers accountable, not immune to liability").

Die IBM setzt sich für eine offene und pluralistische KI-Landschaft ein. Ein KI-Lizenzierungssystem wäre ein schwerer Schlag für offene Innovationen, würde unbeabsichtigt die Kosten erhöhen, Innovationen behindern, kleinere Akteure und Open-Source-Entwickler benachteiligen und die Marktmacht einiger weniger Akteure festigen. Stattdessen sollte KI von und für viele entwickelt werden, nicht für wenige. Zu diesem Zweck ist ein lebendiges offenes KI-Ökosystem gut für Wettbewerb, Innovation, Qualifizierung und Sicherheit („Support open AI innovation, not an AI licensing regime").

Für eine wirkungsvolle und innovationsfreundliche Umsetzung

IBM begrüßt die Idee, die **Marktüberwachung über die Bundesnetzagentur** zu organisieren. Sie ist etabliert und verfügt über Kernkompetenzen und Erfahrung im Telekommunikationsbereich und bei Hardware. Zudem sollte:

- **das nationale Umsetzungsgesetz die Bundes- und ggf. sektorspezifischen Landeskompetenzen klar regeln;** eine Marktüberwachungs-Kleinstaaterei wie bei der DSGVO sollte unbedingt vermieden werden. Hier sind insbesondere die Vermeidung von Doppelstrukturen und die Verzahnung der diversen Durchführungsakte der Digitalregulierung wichtig;

- der **Schutz von Geschäftsgeheimnissen** bei Offenlegung technischer Spezifika und Quellcodes gegenüber Behörden zum Zwecke der Marktüberwachung gewährleistet werden;

- die Politik eine **ausreichende technische, personelle und finanzielle Ausstattung** aller Marktüberwachungs- und notifizierenden Behörden, Konformitätsbewertungsstellen sowie der zentralen Anlaufstelle sicherstellen. Die Finanzierung des geplanten Durchführungsgesetzes sollte im Haushalt 2025 und in der mittelfristigen Finanzplanung unverzüglich vorangebracht werden.

Für eine internationale Harmonisierung der KI-Governance

Die Politik sollte sich dafür einsetzen, die **G7-Hiroshima-Prinzipien voranzutreiben**, und sich weltweit für risikobasierte KI-Governance einsetzen. Diese sollte in Übereinstimmung mit dem AI Act und der Executive Order der USA ausgestaltet sein. Entscheidend sind hierbei:

- die **Stärkung der Rolle supranationaler Organisationen wie der OECD für die internationale Koordinierung der Digitalpolitik**. Der strukturierte Ansatz der Stakeholder Einbindung der OECD bringt eine Vielzahl an Perspektiven ein und sollte gestärkt werden;

- die **G7 sollte „KI crosswalks“ entwickeln**, ähnlich der von IMDA und NIST, die die nationalen KI-Regulierungssysteme mit den G7-Hiroshima-Prinzipien vergleichen. Diese „KI crosswalks“ würden aufzeigen, wo derzeit Lücken und Unterschiede bestehen;

- **Regulatorische Sandboxes** wie beispielsweise die AI Verify Foundation in Singapur und andere sind wichtige Instrumente zur Förderung iterativer Entwicklungen hin zu risikobasierten Regulierungsrahmen und haben den Vorteil, dass sie flexibel, anpassungsfähig sowie wachstumsorientiert sind;

- **europäische Standards für KI sollten so identisch wie möglich mit ISO-Standards sein**, um eine Marktfragmentierung zu verhindern.

Für eine wissenschaftsorientierte und offene KI

Die wissenschaftliche Bewertung der KI-Modelle auf ihre potenziellen Sicherheitsrisiken steht erst am Anfang. Einige Länder (USA, Großbritannien, Japan) gründeten hierfür KI-Sicherheitsinstitute. Diese

liefern wissenschaftlich fundierte und empirisch abgesicherte Richtlinien und Standards für die Messung der KI.

- Politische Entscheidungsträger sollten **regulatorische Reaktionen auf neuartige Risiken** – die von bestehenden Regulierungsrahmen noch nicht berücksichtigt werden – auch durch die Förderung von grundlagen- und anwendungsorientierter Forschung in KI testen.

- **Offene KI-Modelle** sind der Schlüssel zu neuen technischen Durchbrüchen und verbessern die Sicherheit. Open Source hat in der Vergangenheit bewiesen, dass „viele Augen" starke Sicherheit bieten. Die Bundesregierung sollte sich für stärkeren Einsatz von Open Source KI in der öffentlichen Verwaltung einsetzen – das OZG 2.0 ist hierfür ein erster Schritt.

Kontakt

Government & Regulatory Affairs IBM DACH

Martin Wegele, Director, martin.wegele@ibm.com, +49 173 5769369

Svenja Frerichs, Senior Manager, svenja.frerichs@ibm.com, +49 172 7655429