Microsoft

Microsoft-Positionspapier zum KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI- MIG)

Stand: Februar 2026

Kontext

§ 11 KI-MIG überträgt allen nach dem Gesetz benannten deutschen Marktüberwachungsbehörden Durchsetzungsbefugnisse. Während die meisten dieser Befugnisse aus dem EU-Recht *(Verordnung (EU) 2019/1020 und KI-Verordnung)* stammen, trifft das KI-MIG spezifische nationale Umsetzungsentscheidungen, die Bedenken hinsichtlich der Datensicherheit, der betrieblichen Auswirkungen und der Verfahrensgarantien für Anbieter von KI-Systemen, insbesondere cloudbasierten und grenzüberschreitenden Diensten, aufwerfen.

1. Umfang der API-basierten Fernvollstreckung

Bestimmung: § 11 Abs. 2 Satz 2 sieht vor, dass Marktüberwachungsbehörden Befugnisse gemäß Artikel 14 Absatz 4 Buchstaben d und j der Verordnung (EU) 2019/1020 „über Anwendungsprogrammierschnittstellen oder andere technische Mittel, die den Fernzugriff ermöglichen", ausüben können.

- Der Fernzugriff auf aktive KI-Systeme, selbst für eng gefasste Zwecke, wirft Bedenken hinsichtlich Betriebsstörungen bei Echtzeitdiensten und der Möglichkeit einer unbeabsichtigten Offenlegung nicht relevanter Daten auf, wenn die Zugriffskontrollen nicht genau definiert sind.
- **Empfehlung:** Jede API-basierte Durchsetzung sollte einer vorherigen Abstimmung mit dem Betreiber, festgelegten Umfangsbeschränkungen und sicheren Verbindungsprotokollen unterliegen. Der Umfang der Fernvollstreckungsbefugnisse sollte ohne weitere Konsultation der Interessengruppen nicht über den derzeitigen Artikel 14 Absatz 4 Buchstaben d und j hinaus erweitert werden.

2. Umfang der Datenzugriffsbefugnisse

Bestimmung: § 11 Absatz 1 übernimmt Artikel 14 Absatz 4 Buchstabe a der Verordnung (EU) 2019/1020, der den Behörden die Befugnis einräumt, Dokumente, technische

Spezifikationen, Daten und Informationen zur Einhaltung der Vorschriften, einschließlich des Zugriffs auf eingebettete Software, *„in jeder Form und jedem Format und unabhängig vom Speichermedium oder Speicherort solcher Dokumente“,* anzufordern.

Für cloudbasierte KI-Systeme schafft dies eine Rechtsgrundlage für deutsche Behörden, den Zugang zu Daten unabhängig davon zu verlangen, wo diese physisch gehostet werden, was möglicherweise im Widerspruch zu den Datenaufbewahrungsvorschriften in anderen Rechtsordnungen steht.

- In Verbindung mit Artikel 74 Absätze 12 und 13 der KI-Verordnung können Behörden auf Trainingsdaten, Validierungsdaten, Testdatensätze und unter bestimmten Voraussetzungen auch auf Quellcode zugreifen. Das KI-MIG enthält keine spezifischen Verfahrensgarantien für den Umgang mit wirtschaftlich sensiblen oder geschützten Informationen, die durch diese Befugnisse erlangt werden, die über den allgemeinen Vertraulichkeitsrahmen von Artikel 78 der KI-Verordnung hinausgehen.
- **Empfehlung:** Entweder das KI-MIG selbst oder eine Durchführungsrichtlinie sollte Datensicherheitsstandards festlegen, die Behörden beim Zugriff auf cloudbasierte KI-Systeme einhalten müssen, insbesondere in Bezug auf grenzüberschreitende Datenanfragen, sichere Übertragungsprotokolle und die Zweckbindung für Daten, die während der Durchsetzung erhoben werden.

3. Einsatz von dritten Personen als Verwaltungshelfer ohne festgelegte Schutzmaßnahmen

Bestimmung: § 11 Absatz 2 Satz 1 ermächtigt die Marktüberwachungsbehörden, Dritte als Verwaltungshelfer hinzuzuziehen, um sie insbesondere bei der Ausführung technischer Prozesse zu unterstützen.

- Die Bestimmung legt keine Qualifikationsanforderungen, Sicherheitsüberprüfungsvorschriften oder verbindliche Standards für den Umgang mit Daten für externe Verwaltungshelfer fest, die während technischer Durchsetzungsprozesse Zugang zu proprietären KI-Modellarchitekturen, Kundendaten oder Geschäftsgeheimnissen erhalten können.
- Die Einbeziehung externer Parteien in die Durchsetzung schafft zusätzliche Angriffsflächen, die die Cybersicherheit gefährden könen und kann im Widerspruch zu den vertraglichen Verpflichtungen stehen, die KI-Anbieter gegenüber ihren Kunden hinsichtlich der Beschränkung des Datenzugriffs haben.
- **Empfehlung:** Das KI-MIG oder etwaige Durchführungsleitlinien sollten vorschreiben, dass dritte Personen, die als Verwaltungshelfer eingesetzt werden, verbindlichen Vertraulichkeitsverpflichtungen, angemessenen Sicherheitsüberprüfungen und festgelegten Datenverarbeitungsprotokollen unterliegen, die denen entsprechen, die für die eigenen Mitarbeiter der Behörde gelten.

Microsoft

4. Überschneidungen zwischen den Befugnissen mehrerer Marktüberwachungsbehörden

Bestimmung: § 11 Abs. 1 überträgt allen gemäß § 2 Abs. 1 bis 8 benannten Marktüberwachungsbehörden, darunter der BNetzA, der BaFin, der KI-Marktaufsichtskammer, Landesbehörden und bestehenden sektoralen Behörden, die vollständigen Durchsetzungsbefugnisse.

- Ein Anbieter, der KI-Systeme in mehreren Sektoren in Deutschland betreibt (z. B. Finanzdienstleistungen, Behörden, Produkte, die unter die EU-Harmonisierungsvorschriften fallen), könnte mit parallelen oder sich überschneidenden Durchsetzungsmaßnahmen verschiedener Behörden konfrontiert sein, die jeweils die gleichen maximalen Befugnisse ausüben, aber möglicherweise unterschiedliche Ansätze in Bezug auf Datensicherheit, Qualifikationen der Inspektoren und operative Koordination verfolgen.
- Das Koordinierungs- und Kompetenzzentrum (§ 5) soll zwar die Zusammenarbeit erleichtern, hat jedoch eher eine beratende als eine verbindliche Funktion und kann doppelte oder inkonsistente Durchsetzungsmaßnahmen nicht verhindern.
- **Empfehlung:** In den operativen Leitlinien sollte ein „Leitbehördenprinzip" für die Durchsetzung bei branchenübergreifenden KI-Anbietern festgelegt werden, um doppelte Datenanfragen und Inspektionen zu vermeiden. Das Koordinierungszentrum sollte über einen formellen Mechanismus verfügen, um Zuständigkeitsüberschneidungen zu klären, bevor Durchsetzungsmaßnahmen eingeleitet werden.

5. Sofortige Vollstreckbarkeit von BaFin-Entscheidungen ohne aufschiebende Wirkung

Bestimmung: § 11 Abs. 7 Satz 2 sieht vor, dass Widersprüche und Klagen gegen alle Entscheidungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) als Marktaufsichtsbehörde, einschließlich der Androhung und Verhängung von Zwangsmaßnahmen, keine aufschiebende Wirkung haben.

- Das bedeutet, dass eine Anordnung der BaFin, ein in Finanzdienstleistungen eingesetztes KI-System zurückzuziehen oder einzuschränken, sofort wirksam wird, selbst wenn der Anbieter sie vor Gericht anficht. Für KI-Systeme, die in kritische Finanzinfrastrukturen eingebettet sind und mehrere Kunden bedienen, birgt die sofortige Vollstreckung ohne vorläufigen Rechtsschutz erhebliche operative und Reputationsrisiken.
- Dies schränkt auch die praktische Fähigkeit der betroffenen Unternehmen ein, die für eine verantwortungsvolle Compliance erforderlichen „strengen Sicherheitsmaßnahmen, präzisen Zugangsbeschränkungen und klaren

Verantwortlichkeiten" umzusetzen, da es vor Inkrafttreten der Vollstreckung keinen Verfahrensspielraum gibt.

- **Empfehlung:** Der Umfang der sofortigen Vollstreckbarkeit sollte auf Fälle beschränkt sein, die echte und unmittelbare Risiken für die Gesundheit, Sicherheit oder Grundrechte darstellen. Für andere Vollstreckungsmaßnahmen sollten die üblichen verwaltungsrechtlichen Schutzmaßnahmen, einschließlich der aufschiebenden Wirkung von Rechtsbehelfen, gelten, um eine ordnungsgemäße Einhaltung und gerichtliche Überprüfung zu ermöglichen.

Ihre Ansprechpartnerin bei Microsoft:

Rebekka Weiss, Head of Regulatory Policy Germany

Tel.: +49 30 39097368| Mobil: +49 160 58 92732 | E-Mail: rebekka.weiss@microsoft.com

Microsoft Berlin | Unter den Linden 17 | D-10117 Berlin | www.microsoft-berlin.de