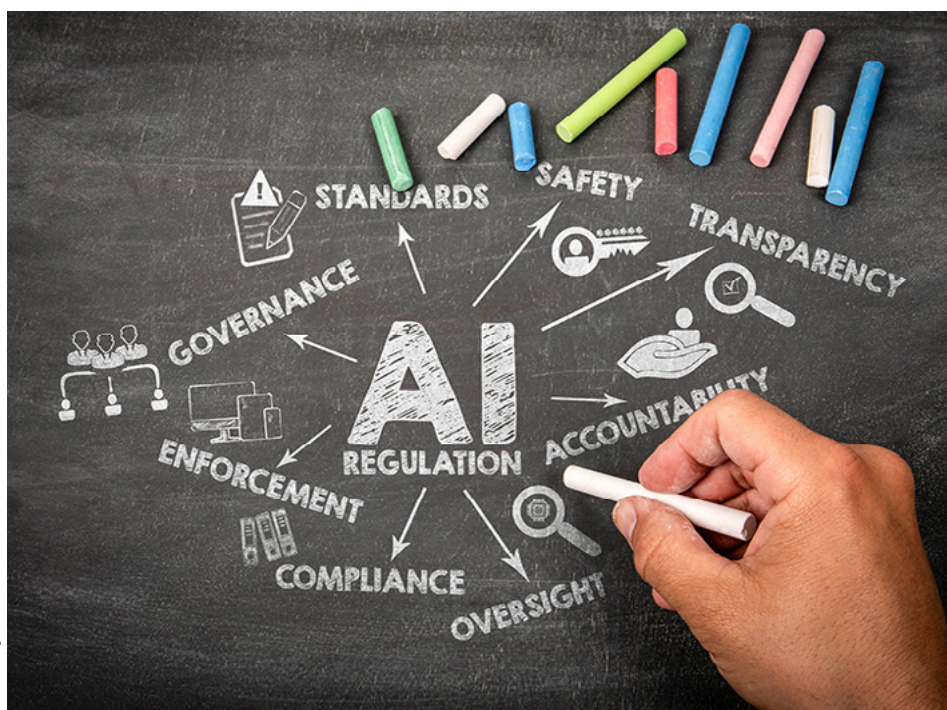


EU AI Act: KI wird in Standardsoftware zum Compliance-Risiko

Der EU AI Act wird für deutlich mehr deutsche Unternehmen relevant, als bislang angenommen. Diejenigen, die Standardsoftware mit integrierten KI-Funktionen einsetzen – etwa in den Bereichen Biometrie, Leistungsbewertung oder Lernanwendungen –, können unter die Vorschriften für Hochrisiko-KI-Systeme fallen. Verschobene Fristen verschärfen die Unsicherheit bei der Umsetzung der Compliance-Anforderungen.



AI Regulation: Compliance-Anforderungen müssen rechtzeitig in Prozesse, Verantwortlichkeiten und Kontrollmechanismen überführt werden.

Der EU AI Act gilt nicht nur für künstliche Intelligenz (KI), die Unternehmen selbst entwickeln, sondern auch für den Einsatz von Unternehmenssoftware, in die KI integriert ist. Auch die Nutzung von KI-Software von Drittanbietern begründet konkrete Dokumentations-, Kontroll- und Nachweispflichten. Das größte Missverständnis rund um den EU AI Act besteht darin, dass er in erster Linie KI-Entwickler und Technologieanbieter betreffe. Tatsächlich gilt das Gesetz für alle Organisationen, die KI-Systeme einsetzen. Das Problem: KI hat sich in Unternehmen längst etabliert, wird jedoch häufig nicht als regulatorisches Risiko wahrgenommen.

In vielen Fällen wird KI nicht als eigenständiges Projekt eingeführt, sondern ergänzt bestehende HR-, Rechts- oder Finanzsysteme um zusätzliche Funktionen. Genau hier besteht Nachholbedarf: Unternehmen müssen sich des tatsächlichen Anwendungsbereichs des EU AI Acts bewusst werden, um die Anforderungen rechtzeitig in Prozesse, Verantwortlichkeiten und Kontrollmechanismen zu überführen.

Die unzureichende Vorbereitung auf den EU AI Act führt schnell zu einem erheblichen Haftungsrisiko. Dabei ist vor allem der Faktor Zeit entscheidend, da in den kommenden zwei Jahren mehrere Fristen greifen. Für Verunsicherung sorgt zudem die EU-Digital-Omnibus-Gesetzgebung, die einige – jedoch keineswegs alle – Fristen der ursprünglichen Verordnung angepasst hat. Viele deutsche Organisationen ordnen die Fristen des AI Acts falsch ein. Sie gehen davon aus, dass sämtliche Verpflichtungen durch den Omnibus verschoben wurden. Das ist jedoch nicht der Fall. Die Trans-

parenzpflichten gelten seit dem 2. August 2026 und wurden nicht verschoben. Der Omnibus hat lediglich die Anforderungen für Hochrisiko-KI-Systeme nach hinten verlegt – und selbst das nicht einheitlich. Für eigenständige Systeme, beispielsweise KI-Tools zur Bewerberauswahl, gilt derzeit voraussichtlich eine Frist bis Dezember 2027. KI, die Bestandteil regulierter Produkte wie Medizinprodukte oder Maschinen ist, muss die entsprechenden Anforderungen hingegen erst bis August 2028 erfüllen.

Bei schwerwiegenden Verstößen drohen Bußgelder von bis zu 35 Mio. EUR oder sieben Prozent des weltweiten Jahresumsatzes. Schwerer als finanzielle Sanktionen dürfte für Unternehmen der Reputationsschaden wiegen. Diskriminierende Entscheidungen bei der Bewerberauswahl oder intransparente KI-gestützte Leistungsbewertungen können als öffentlich bekannt gewordener Compliance-Verstoß schnell erhebliche geschäftliche Risiken nach sich ziehen und die wirtschaftliche Handlungsfähigkeit eines Unternehmens erheblich einschränken. Für Vorstände schafft der AI Act deshalb klare Erwartungen: AI Governance gehört künftig auf die Agenda aller Risiko- und Compliance-Gremien. Dazu gehören regelmäßige Bewertungen des Einsatzes von KI-Systemen, um die erforderlichen Risikobewertungen durchführen zu können, Berichte über Hochrisiko-KI-Systeme, die Überprüfung veröffentlichter KI-generierter Inhalte im Hinblick auf die Transparenzanforderungen sowie eine lückenlose Dokumentation zum Nachweis der Compliance.

Unternehmen sollten die regulatorischen Anforderungen proaktiv angehen und frühzeitig kontinuierliche Prozesse etablieren. Sie sollten zunächst erfassen, welche KI-Systeme sie einsetzen, zu welchen Zwecken diese genutzt werden und welche Ergebnisse sie erzeugen. Daraus sollte ein vollständiges KI-Inventar entstehen, das nicht nur selbst entwickelte Anwendungen, sondern auch KI-Funktionen in eingekaufter Software umfasst. Anschließend können die einzelnen Systeme entsprechend ihrer Risikokategorie gemäß EU AI Act eingeordnet werden, um einen Überblick über die jeweiligen Fristen und Verpflichtungen zu erhalten. Voraussetzung dafür sind klar definierte Verantwortlichkeiten. Unternehmen sollten frühzeitig festlegen, wer für die AI Governance verantwortlich ist, und geeignete Systeme schaffen, über die Mitarbeitende potenzielle Probleme unkompliziert melden können. Zwar hat die EU ein zentrales Meldeportal speziell für Verstöße gegen den EU AI Act eingerichtet. Unternehmen, die bereits heute eigene Hinweisgebersysteme etablieren, ermöglichen ihren Mitarbeitenden jedoch eine geschützte interne Meldung und können potenzielle Probleme frühzeitig intern erkennen und beheben. Ebenso sollten Unternehmen eine kontinuierliche Dokumentation und Überwachung ihrer KI-Systeme etablieren.



Erena Langley, Director of Regulatory Solutions, NAVEX.

Erena Langley