15 Jahre Deutscher AnwaltSpiegel

KI-Integration im Unternehmen

Eine Reise durch die neue KI-Verordnung

Von Dr. Patrick Grosmann und Jonas Puchelt

© Spot Decor – stock.adobe.com

Die Integration von KI-Systemen wird durch die neue EU-Verordnung stark reglementiert. Unternehmen müssen sich auf umfassende Pflichten und mögliche Sanktionen einstellen.

Dr. Patrick Grosmann, M.A.

FPS Rechtsanwaltsgesellschaft, Frankfurt am Main
Rechtsanwalt, Associate, Zertifizierter Datenschutzbeauftragter (TÜV®), Zertifizierter Datenschutz-Auditor (DGI®)

grosmann@fps-law.de
www.fps-law.de

Jonas Puchelt

FPS Rechtsanwaltsgesellschaft, Frankfurt am Main
Rechtsanwalt, Associate Partner, Fachanwalt für Informationstechnologierecht, Datenschutzbeauftragter (DSC)

puchelt@fps-law.de
www.fps-law.de

Künstliche Intelligenz (KI) ist bereits jetzt aus der freien Wirtschaft nicht mehr wegzudenken. Als Antwort darauf hat die EU eine wegweisende KI-Verordnung auf den Weg gebracht. Die KI-Verordnung befasst sich mit den spezifischen Risiken von KI-Systemen und zielt darauf ab, Überschneidungen mit anderen Gesetzen zu minimieren. Dabei konzentriert sich die Verordnung auf Aspekte wie Transparenz, Sicherheit und Datenschutz bei KI-Systemen mit dem Ziel, bestehende Lücken der Regulatorik zu schließen.

Um die Auswirkungen der neuen KI-Verordnung greifbar zu machen, zeigen wir im Folgenden kurz auf, was es aus Unternehmenssicht bei der Integration von KI im Unternehmen zu beachten gilt.

Überblick über die KI-Verordnung: Was ist ein KI-System?

Die Definition eines KI-Systems in der KI-Verordnung ist weit gefasst. Von den fünf Kriterien sind drei (maschinenbasiertes System; generiert aus Input einen Output; der Output entfaltet Wirkung außerhalb des Systems) auf fast alle IT-Systeme anwendbar. Das vierte Kriterium, die Lernfähigkeit, ist optional. Entscheidend ist das fünfte Merkmal: die Fähigkeit zur teilweisen Autonomie. Dies bedeutet, dass KI-Systeme in der Lage sind, Outputs zu generieren, die nicht ausschließlich auf vorher festgelegten, von Menschen definierten Regeln basieren. Stattdessen nutzen sie datengetriebene Modelle, um Muster zu erkennen und darauf basierend Entscheidungen zu treffen oder Vorhersagen zu machen.

Dabei ist zu beachten, dass die KI-Verordnung nicht nur auf evidente KI-Anwendungen abzielt, sondern auch auf Systeme, die maschinelles Lernen, logikbasierte Ansätze oder statistische Methoden verwenden. Die Verordnung hat einen breiten Anwendungsbereich und kann auch Systeme betreffen, die auf den ersten Blick gar nicht nach KI-Systemen aussehen.

Parallelen und Unterschiede zur DSGVO: Der risikobasierte Ansatz

Die KI-Verordnung folgt, ähnlich wie die Datenschutz-Grundverordnung (DSGVO), einem risikobasierten Ansatz [siehe Art. 24 Abs. 1 Satz 1 DSGVO (Bindung des Verantwortlichen an das Verarbeitungsrisiko), Art. 32 DSGVO (technische und organisatorische Maßnahmen anhand des Verarbeitungsrisikos), Art. 35 DSGVO (Datenschutz-Folgenabschätzung) und Art. 39 Abs. 2 DSGVO (risikobasierte Aufgabenzuweisung des Datenschutzbeauftragten)].

Die KI-Verordnung geht jedoch noch einen Schritt weiter und definiert konkrete Risikoklassen (siehe hierzu auch den **FPS-KI-Check**):

1. Unannehmbares Risiko: Bestimmte KI-Systeme, wie soziales Scoring oder manipulative Techniken, werden vollständig verboten.
2. Hochrisiko-KI-Systeme: Die Regelungen zur Einstufung eines KI-Systems als hochriskant sind komplex. So können KI-Systeme z.B. hochriskant sein, weil sie in bestimmten Sektoren, regulierten Produkten (Medizin) oder bestimmten Use-Cases, wie der biometrischen Identifizierung, zum Einsatz kommen. Details dazu sind in den Anlagen der KI-Verordnung festgehalten. Für hochriskante Systeme gelten umfassende Pflichten (siehe unten).
3. General Purpose AI (GPAI): Dies sind Modelle, die aus Sicht des Gesetzgebers ein besonderes Risikoprofil aufweisen, weil sie für eine Vielzahl von Use-Cases ohne weiteres anwendbar sind. Es gelten insbesondere erweiterte Transparenzpflichten, z.B. für KI-basierte Chatbots.
4. Ohne spezifisches Risiko: Für KI-Systeme ohne spezifisches Risiko gelten lediglich allgemeine Sicherheits- und Transparenzregeln.

Einordnung als Hochrisiko-KI-System

Die KI-Verordnung definiert grundsätzlich zwei Szenarien für Hochrisiko-KI-Systeme. Einerseits fallen darunter KI-Systeme, die selbst Produkte sind oder als Sicherheitsfeatures in Produkten dienen, die laut EU-Recht eine Konformitätsbewertung benötigen (siehe Anhang 2). Hochrisiko-KI-Systeme sind auch solche Systeme, die für bestimmte Anwendungsszenarien eingesetzt werden (siehe Anhang 3) – dies betrifft beispielsweise die Bereiche Bildung, Beschäftigung, Strafverfolgung und KI-Systeme zum Einsatz bei kritischen Infrastrukturen.

Die Einstufung in eine Risikoklasse ist nicht statisch. Wenn ein System erweitert wird oder dessen Einsatzbereich geändert wird, kann eine andere Risikoeinstufung gelten.

Adressaten und Pflichten der KI-Verordnung

Die KI-Verordnung richtet sich an verschiedene Akteure im KI-Ökosystem, wobei die Rollen des Providers, Deployers und Distributors praxisrelevant sind. Diese Rollen sind an spezifische Verantwortlichkeiten und Anforderungen geknüpft, um einen sicheren, ethischen und rechtskonformen Einsatz von KI-Technologien zu gewährleisten. Unternehmen können dabei eine oder mehrere Rollen gleichzeitig einnehmen.

> „Verstöße gegen die KI-Verordnung können für Unternehmen schwerwiegende Folgen haben."

Als Provider gilt, wer ein KI-System entwickelt und in der EU auf den Markt bringt oder in Betrieb nimmt. Deployer sind Anwender, die KI-Systeme unter eigener Aufsicht verwenden, während Distributoren KI-Systeme vertreiben oder verkaufen, ohne sie selbst entwickelt zu haben.

Wer ein KI-System für seine Unternehmensprozesse einsetzt, wird in der Regel als Deployer eingestuft. Die folgenden Deployer-Pflichten müssen dann umgesetzt werden:

- Überwachung des Systems durch qualifiziertes Personal;
- Aufbewahrung von Systemlogs für sechs Monate;
- Nutzung des Systems gemäß den Nutzungsanweisungen des Providers;
- Inputdaten müssen für den konkreten Zweck geeignet, repräsentativ und nicht voreingenommen sein (non-bias);
- Bereitstellung von Informationen über den Betrieb des Systems an den Provider;
- es müssen notwendige Meldungen über Zwischenfälle und Risiken für natürliche Personen an den Provider und die zuständige Aufsichtsbehörde erfolgen.

An dieser Stelle ist jedoch Vorsicht geboten: Ein Unternehmen kann bei dem Einsatz von KI-Systemen schnell (zusätzlich) in eine Providerstellung rutschen. Beispielsweise, weil das KI-System auf eigene Bedürfnisse angepasst oder einer anderen Konzerngesellschaft zur Nutzung überlassen wird.

Gerade im Bereich von Hochrisiko-KI erweitert sich der Pflichtenkreis des Unternehmens dann drastisch:

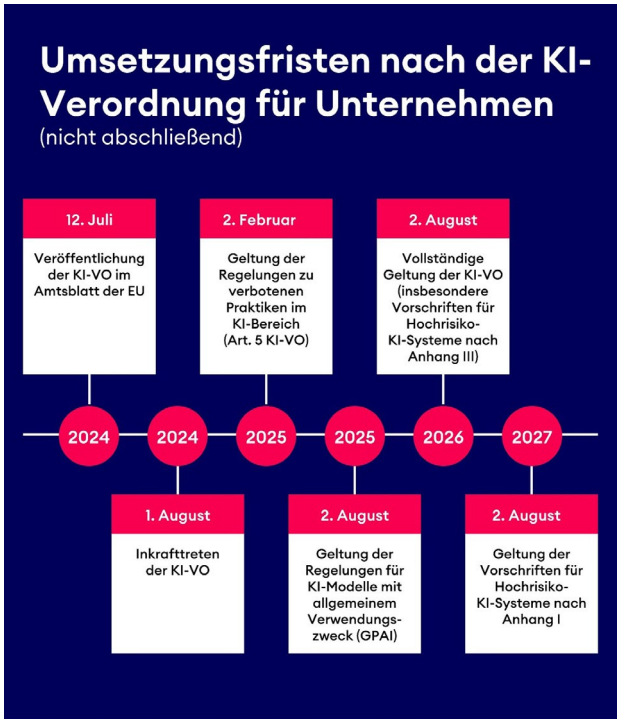
- Es ist ein Risikomanagementsystem zu unterhalten, das die Risiken des Systems identifiziert und mittels wirksamer Maßnahmen mitigiert.
- Es sind Qualitätskriterien für die Inputdaten des Systems sicherzustellen (Test-, Trainings- und Produktivdaten).
- Es sind eine technische Dokumentation des Systems und für den Anwender verständliche Nutzungsanweisungen bereitzustellen.
- Der Betrieb des Systems ist mittels Logs fortlaufend zu protokollieren.
- Die Genauigkeit und Zuverlässigkeit sowie die angemessene Fehlertoleranz des Systems sind sicherzustellen.
- Angemessene Sicherheitsstandards sind zu implementieren, die das System vor Angriffen Dritter schützen.

Konsequenzen bei Nichteinhaltung

Verstöße gegen die KI-Verordnung können für Unternehmen schwerwiegende Folgen haben. Bei Verstößen gegen Bestimmungen zu verbotenen KI-Systemen drohen Geldbußen von bis zu 7% des weltweiten Jahresumsatzes oder 35 Millionen Euro. Sonstige Verstöße können mit bis zu 3% oder 15 Millionen Euro sanktioniert werden. Aufsichtsbehörden haben zudem weitere Befugnisse, um auf Verstöße zu reagieren. Hierzu zählen die Anordnung zur Anpassung oder Einstellung des KI-Systems, die Herausgabe des Quellcodes, die Auferlegung von Korrekturmaßnahmen oder Marktzugangsbeschränkungen.

Neben möglichen Bußgeldern müssen auch Reputationsschäden und der Verlust des Kundenvertrauens berücksichtigt werden.

Abbildung 1: Umsetzungsfristen nach der KI-Verordnung



Quelle: FPS Rechtsanwaltsgesellschaft

Wie geht es jetzt weiter?

Die KI-Verordnung ist am 01.08.2024 in Kraft getreten, wobei die Regelungen erst 24 Monate später vollständig anwendbar sein werden (siehe Abbildung 1). Für verbotene KI-Systeme gilt eine kürzere Frist von sechs Monaten nach Inkrafttreten. Bestimmungen zu General-Purpose-Modellen und Konformitätserklärungen greifen nach zwölf Monaten; Regelungen zu Hochrisiko-KI-Systemen, die auf bestehenden EU-Produktregulierungen basieren, werden erst 36 Monate nach der Veröffentlichung anwendbar. Diese gestaffelte Einführung ermöglicht eine sukzessive Umsetzung der Verordnung – dabei sollten besonders kritische Bereiche priorisiert werden. ←