

# KI-Verordnung der EU setzt neue Anforderungen

Gute Vorbereitung schützt vor empfindlichen Sanktionen – Hohe Bußgelder auch wegen geringer Verstöße

Von Tim Wybitul \*)

Börsen-Zeitung, 15.6.2024

Die Europäische Union hat mit der EU-Verordnung zur Regelung künstlicher Intelligenz (KI) ein System geschaffen, das den Einsatz von KI in Unternehmen streng reguliert. Die Verordnung soll Risiken minimieren, die Sicherheit sowie die Grundrechte der Bürger schützen und Innovation fördern.

Doch mit diesen Regeln kommen auch erhebliche Risiken auf Unternehmen zu. Denn viele Bestimmungen sind unpräzise formuliert und lassen sich in der Praxis nur schwer rechtssicher anwenden. Beispielsweise sind die nach der Verordnung verbotenen KI-Praktiken nur schwer vom erlaubten Einsatz künstlicher Intelligenz abzugrenzen. Zudem dürften viele Unternehmen die Anforderungen an Betreiber von Hochrisiko-KI-Systemen übersehen oder unterschätzen. Gerade beim Einsatz von KI am Arbeitsplatz oder beim sogenannten Profiling gelten teilweise weitgehende Anforderungen.

## Gestaffeltes System

Die KI-Verordnung sieht ein gestaffeltes Bußgeldsystem vor, das sich nach der Schwere des Verstoßes richtet. Die meisten Verstöße werden von Marktaufsichtsbehörden auf nationaler Ebene geahndet. Die höchsten Strafen drohen bei der Nutzung verbotener KI-Praktiken, wie etwa der manipulativen Beeinflussung von Personen. Hier drohen Geldbußen von bis zu 35 Mill. Euro. Bei Unternehmen mit globalen Umsätzen von mehr als 500 Mill. Euro kommen noch höhere Geldbußen von bis zu 7% ihres weltweiten Jahresumsatzes in Betracht.

Dieser Mechanismus ist bereits aus einem anderen EU-Digitalrechtsakt bekannt, der EU Datenschutz-Grundverordnung (DSGVO). Dort verhängen die Aufsichtsbehörden bereits jetzt regelmäßig Geldbußen in dreistelliger Millionenhöhe – und auch die Milliardengrenze haben die Aufsichtsbehörden bereits deutlich überschritten. Nach derzeitigem Stand spricht übrigens viel dafür, dass die Daten-

schutzaufsichtsbehörden in Deutschland und vielen anderen EU-Staaten als Marktaufsichtsbehörden auch für die Kontrolle der Einhaltung der KI-Verordnung zuständig werden.

## Aus der DSGVO lernen

Es steht zu hoffen, dass Kommission und nationale Gesetzgeber aus dem Beispiel der DSGVO lernen und den Behörden klare rechtliche Vorgaben machen. Denn die europäischen Datenschutzaufsichtsbehörden haben sich in der Vergangenheit nicht immer durch hinreichendes Verständnis für wirtschaftliche Belange hervorgetan.

Sogar bei scheinbar geringfügigen Vergehen, wie der Bereitstellung unvollständiger oder irreführender Informationen auf behördliche Anfragen, drohen Unternehmen Geldbußen von bis zu 7,5 Mill. Euro oder 1% des weltweiten Jahresumsatzes konfrontiert werden. Diese Regelung dürfte in der Praxis eine erhebliche Sprengkraft haben. Denn sie macht die Reaktion auf entsprechende Anforderungen von Aufsichtsbehörden ausgesprochen riskant. Einerseits drohen Risiken, wenn man der Behörde zu transparent die eigenen KI-Systeme und Prozesse offenlegt. Andererseits drohen erhebliche Risiken, wenn man die Behörde unvollständig oder wenig transparent informiert.

In der Praxis läuft diese Regelung auf eine ausgesprochen weitgehende Pflicht zur Kooperation oder sogar zu Selbstbeziehung wegen möglicher Verstöße gegen die KI-Verordnung hinaus.

## Flexibel geplante Strategie

Unternehmen stehen nun vor der Herausforderung, die Anforderungen der KI-Verordnung effektiv und mit vertretbaren Kosten in ihre Geschäftsprozesse zu integrieren. Eine gründliche Vorbereitung ist entscheidend, um Bußgeldrisiken zu minimieren und die Vorteile von KI-Technologien sicher und mit vertretbaren rechtlichen Risiken zu nutzen.

Der sinn- und verantwortungsvolle Einsatz von KI im Unternehmen braucht eine

gut und flexibel geplante Strategie. Dabei gilt es, die Vorgaben der KI-VO „mitzudenken“ und bei der Planung und kontinuierlichen Anpassung der eigenen KI-Strategie zu kennen und zu beachten. So sollte man etwa darauf achten, möglichst auf bereits bestehenden Strukturen aufzusetzen, etwa im Rahmen der Erfüllung von Vorgaben der DSGVO oder anderer EU-Digitalrechtsakte.

Zunächst ist es wichtig, dass Unternehmen die Tragweite der KI-Verordnung erfassen und zu verstehen, welche Aspekte ihres Geschäftsbetriebs betroffen sind. Dazu gehört die Identifikation aller relevanten KI-Systeme im Einsatz und die Bewertung, ob diese unter die KI-Verordnung fallen und in welche der dort vorgegebenen Risikokategorien. Aus dieser Einstufung leitet sich dann ab, welche Maßnahmen man in Bezug auf das jeweilige KI-System treffen muss.

## Priorisierung wichtig

Ein weiterer wesentlicher Schritt ist die Integration der neuen rechtlichen Vorgaben in die KI-Strategie des Unternehmens. Dies umfasst etwa die Identifikation ein-

schlägiger Pflichten nach der KI-Verordnung, die entsprechende Anpassung interner Richtlinien, die Schulung von Mitarbeitern und die Implementierung von Prozessen zur Risikobewertung und Dokumentation.

Auch die richtige Priorisierung von Maßnahmen ist wichtig. Unternehmen sollten die Bereiche identifizieren, in denen das Risiko eines Verstoßes gegen die KI-Verordnung am größten ist, und dort mit der Umsetzung der nötigen Schritte beginnen.

Typische Maßnahmen sind das Sicherstellen menschlicher Kontrolle von KI-gestützten Entscheidungen, interne Regeln zum Einsatz von KI-Anwendungen, Konformitätsbewertungen, das Erstellen gesetzlich geforderter Dokumentation, aber auch die Stärkung der Datensicherheit oder die Verbesserung der Transparenz.

## Dokumentation unerlässlich

Eine sorgfältige Dokumentation aller Schritte zur Einhaltung der KI-Verordnung ist ebenfalls unerlässlich. Im Falle einer Überprüfung müssen Unternehmen nachweisen können, dass sie die Anforderungen der Verordnung erfüllen. Dies beinhaltet die Dokumentation von Risikoanalysen, Entscheidungsprozessen und der Einhaltung technischer Standards. Diese Dokumentation sollte in einer Weise gestaltet sein, die später hilft, Behörden und Gerichte zu überzeugen.

Die Verordnung sieht Umsetzungsfristen von sechs 36 Monaten ab ihrem Inkrafttreten in voraussichtlich wenigen Wochen vor. Das ist angesichts der vielen und weitreichenden Anforderungen der KI-VO ein relativ knapp bemessener Zeitrahmen. Unternehmen und andere KI-Akteure sind daher gut beraten, die Vorgaben der Verordnung in ihrer KI-Strategie zeitnah zu berücksichtigen und umzusetzen. Ein wichtiger Aspekt sollte dabei die erfolgreiche Verteidigung gegen Bußgelder der KI-VO sein.

Gerade bei der Priorisierung einzelner Prozesse und Strukturen sowie bei der Dokumentation der Einhaltung der Anforderungen der Verordnung lassen sich

so mögliche Fehler und unnötiger Aufwand vermeiden. Wegen der vielen Parallelen und Überschneidungen zur DSGVO kann man diese bei der Implementierung der KI-VO teilweise als Blaupause nehmen. Häufig werden sich Prozesse zur Einhaltung der DSGVO so anpassen und erweitern lassen, dass sie auch Anforderungen der KI-VO abdecken können. Ein solches Vorgehen spart erfahrungsgemäß Zeit und Kosten.

## Noch viel zu tun

Die KI-Verordnung stellt Unternehmen vor große Herausforderungen, bietet aber auch die Chance, KI-Technologien verantwortungsvoll und im Einklang mit europäischen Werten zu nutzen. Eine frühzeitige und umfassende Vorbereitung ist der Schlüssel, um die Vorteile von KI zu nutzen und gleichzeitig Bußgeldrisiken zu vermeiden. Bislang sind die vom Gesetzgeber gemachten Vorgaben der KI-VO teilweise noch sehr unbestimmt. Sowohl die konkreten Anforderungen an den Umgang mit KI-Systemen, aber auch die Bußgeldvorschriften der Verordnung sind weitreichend, komplex und teilweise sehr unbestimmt. Wohl auch aus diesem Grund weist die Verordnung vor allem der EU-Kommission, aber auch den Mitgliedstaaten wichtige Regelungskompetenzen zu.

## Im Sinne der Praxis

Es steht zu hoffen, dass sie hiervon in einer Weise Gebrauch machen, die sich an der Praxis orientiert. Entsprechende konkretisierende Regeln sollten realistisch umsetzbar sein und auch die Interessen einer wettbewerbsfähigen KI-Wirtschaft in der EU hinreichend berücksichtigen.

Dies entspräche auch der klaren Zielsetzung der Verordnung, die auf die Unterstützung von Innovation, das Funktionieren des Binnenmarkts und die Förderung einer auf den Menschen ausgerichteten und vertrauenswürdigen KI ausdrücklich als Ziele nennt.

\*) Tim Wybitul ist Partner von Latham & Watkins in Frankfurt.