Management Summary: Die KI-Verordnung

Einleitung

Die Europäische Union hat das Gesetz über Künstliche Intelligenz (KI-Verordnung oder KI-VO) verabschiedet, das den Einsatz von KI innerhalb der EU reguliert. Es schafft einen rechtlichen Rahmen für die Entwicklung, Vermarktung und Nutzung von KI in der EU. Ziel ist es sicherzustellen, dass KI-Technologien sicher sind und grundlegende Rechte einhalten. Zudem soll ein einheitlicher Markt für vertrauenswürdige KI-Anwendungen in Europa gefördert werden. Das Gesetz trat am 1. August 2024 in Kraft, wobei die Einhaltung über drei Jahre schrittweise erfolgt. Die Frist für die Einhaltung der meisten Verpflichtungen ist der 2. August 2026. Bei Nichtbeachtung drohen Geldbußen von bis zu 7 % des weltweiten Jahresumsatzes oder 35 Millionen Euro pro Verstoß.

Ausgangslage

Die KI-Verordnung reguliert die Entwicklung, Nutzung und den Handel von KI-Technologie, um Menschen vor den Auswirkungen von KI zu schützen. Die KI-Verordnung verpflichtet uns, Risikobewertungen durchzuführen und Maßnahmen wie Prüf-, Überwachungs- und Dokumentationsprozesse zu ergreifen, wenn wir KI-Technologie nutzen oder entwickeln wollen. Um Transparenz zu gewährleisten, müssen Beschäftigte, Kunden und Geschäftspartner informiert werden, wenn KI-gestützte Systeme zum Einsatz kommen. Hat die Organisation bereits KI-gestützte Systeme in Geschäftsbereiche integriert, um Unternehmensabläufe zu optimieren, könnten die neuen Regulierungen bereits getätigte Investitionen gefährden. Die frühzeitige Evaluierung nötiger Anpassungen und Maßnahmen hilft, diese Investitionen abzusichern, Werte sowie Vorteile langfristig zu erhalten und Bußgeldrisiken zu vermeiden.

Herausforderungen

Die KI-Verordnung ist bereits in Kraft getreten. In den nächsten Monaten muss die Organisation sicherstellen, die umfangreichen Anforderungen der KI-Verordnung erfüllen zu können. Die KI-Verordnung setzt voraus, dass wir KI-Technologie verstehen, Risiken beim Einsatz von KI-Technologien bewerten, Maßnahmen zur Risikominderung identifizieren und festlegen sowie die Umsetzung dieser Maßnahmen überwachen. Hierfür ist es erforderlich, dass die Organisation die notwendige KI-Kompetenz bei allen involvierten Mitarbeitern sicherstellt. Dies betrifft alle Unternehmensbereiche, die mit der Entwicklung, dem Einkauf oder dem Betrieb bzw. der Nutzung von KI-gestützten Systemen befasst sind. Neue Rollen und Zuständigkeiten müssen im Rahmen eines (erweiterten) Managementsystems festgelegt werden. Dabei sollten nach Möglichkeit bestehende Managementsysteme genutzt und Synergien genutzt werden.

Nächste Schritte

Wir empfehlen, die notwendigen Maßnahmen zur Erfüllung der Anforderungen der KI-Verordnung schrittweise umzusetzen. Hierbei sollten wir bereits bestehende Managementprozesse nutzen. Einen finalen Maßnahmenplan können wir zum jetzigen Zeitpunkt noch nicht vorlegen, da erst nach dem Erfassen der bereits genutzten KI-Technologie eine Risikobewertung vorgenommen werden kann. Anschließend können Maßnahmen definiert und der entsprechende Umfang neuer Managementprozesse festgelegt werden.

Nach einem ersten Abgleich der Anforderungen aus der KI-Verordnung mit bereits bestehenden Anforderungen aus anderen Gesetzen (unter anderem aus dem Datenschutzrecht) haben wir viele Parallelen festgestellt, wie beispielsweise die Risikobewertung, die Meldeprozesse sowie die Betroffenenkommunikation. Vor diesem Hintergrund empfehlen wir, im Rahmen der vorgenannten Feststellungen auf bereits bestehende Prozesse zurückzugreifen.

KI-Technologie erfassen

Schritt 1: Erfassen bereits genutzter KI-Technologie

Im ersten Schritt erfassen wir alle KI-Technologien, die wir im Unternehmen nutzen. Hierfür muss ein sogenanntes KI-Register erstellt werden. Zu jeder KI-Technologie werden Fragen technischer, aber auch organisatorischer Natur gestellt. Es ist notwendig zu wissen, zu welchem Zweck und in welchem Kontext die Technologie eingesetzt wird oder eingesetzt werden soll. Zudem sind technische Informationen erforderlich, einschließlich der Komponenten, aus denen die Technologie besteht, der genutzten Datenquellen und des verwendeten Frameworks.

Risikoeinordnung Rollenzuweisung

Schritt 2: Risikoeinordnung und Rollenzuweisung

Im zweiten Schritt sind die erfassten KI-Technologien nach der KI-Verordnung zu klassifizieren. Hierzu müssen wir einen Abgleich durchführen, inwieweit die Anwendungsszenarien, die wir mit der KI-Technologie vorhaben, unter eine verbotene Praktik oder ein Hochrisiko-Szenario fallen. Je nachdem, welche der Kategorien hier zutrifft, ist auch unsere Rolle in der KI-Wertschöpfungskette für jede dieser KI-Technologien festzulegen. Sind wir lediglich Anwender oder auch Entwickler dieser Technologien?

Ressourcen- und Budgetplanung

Schritt 3: Ressourcen- und Budgetplanung

Wenn wir ermittelt haben, wie die KI-Technologie nach der KI-Verordnung klassifiziert werden muss, legen wir den Umfang des notwendigen Managementsystems fest. Dies kann von einem einfachen Risikomanagementsystem (Art. 9 KI-VO) bis hin zu einem aufwendigen Qualitätsmanagementsystem (Art. 17 KI-VO) reichen. Hier sind die einzelnen notwendigen Prozesse aufzulisten und auf der einen Seite die dafür notwendigen Personal-, Verwaltungs-, Rechts- sowie IT-Kosten im Rahmen einer Budgetplanung festzuhalten. Am Ende erfolgt die Vorstellung an die Geschäftsleitung, um identifizierte Risiken und geplante Maßnahmen vorzustellen. Ebenso erfolgt eine Darstellung des erforderlichen Budgets für die geplanten Maßnahmen. Die Geschäftsleitung muss über Budget und Maßnahmen entscheiden.

Implementierung der KI-Governance

Schritt 4: Implementierung der KI-Governance

Basierend auf den Ergebnissen der Risikoanalyse, Einordnung und Rollenzuweisung sowie dem festgelegten Ressourcen- und Budgetplan sind die Anforderungen der KI-Verordnung in die bereits bestehenden Managementsysteme zu implementieren. Hierzu sind die zuvor festgelegten Rollen und Zuständigkeiten zu übertragen und den Überwachungs- und Steuerungsfunktionen des Managementsystems zuzuordnen. Wenn erforderlich, empfehlen wir, die Organisationsstruktur entsprechend anzupassen. Sollten Anpassungen an der Organisationsstruktur erforderlich sein, muss die Geschäftsleitung über diese Anpassung entscheiden.

Überwachungs-Kontrollmaßnahmen

Schritt 5: PDCA-Zyklus

Das KI-Managementsystem muss, wie bei anderen Managementsystemen, ebenfalls kontinuierlich überprüft und an aktuelle Gegebenheiten angepasst werden. Hierzu müssen unter anderem die Gesetzgebung und die Rechtsprechung zur KI-Verordnung laufend beobachtet werden. Die Europäische Kommission kann delegierte Rechtsakte und Durchführungsakte erlassen und Richtlinien entwickeln, um den Anwendungsbereich und die Anforderungen der KI-Verordnung anzupassen. Es ist entscheidend, diese Änderungen zu verfolgen und zu berücksichtigen. Auch technologische Entwicklungen können es erforderlich machen, dass das KI-Managementsystem angepasst werden muss. Eine kontinuierliche KI-Kompetenz ist aufzubauen, um möglichst unabhängig von externer Beratung Rechtssicherheit zu gewährleisten sowie Chancen und Risiken beim Einsatz von KI-Technologie sorgfältig abwägen zu können.