Der Einsatz von KI-Systemen im Finanzsektor

Kaum ein Thema wurde und wird in den letzten Jahren so positiv und zukunftsweisend, aber auch so kritisch diskutiert wie das Thema Künstliche Intelligenz, kurz KI. Unternehmen werben bereits seit geraumer Zeit mit dem Einsatz von KI-Systemen und der damit verbundenen Steigerung der Leistungsfähigkeit oder Produktqualität. Auch in der Finanzwirtschaft werden KI-Systeme bereits eingesetzt, z.B. für Kreditwürdigkeitsprüfungen oder im Vertrieb.

Der positive Nutzen von KI-Systemen ist nicht von der Hand zu weisen, da die Systeme in der Lage sind, sehr große Datenmengen in wenigen Augenblicken zu verarbeiten und eine Entscheidung zu treffen. Im gleichen Fall würde die Verarbeitung der Daten durch einen Menschen mindestens mehrere Stunden in Anspruch nehmen, vor allem wenn man den Aufwand der Dateneingabe und -auswertung berücksichtigt. Die rechtlichen Rahmenbedingungen und Folgen des Einsatzes von KI-Systemen waren in der EU bislang nicht geregelt. Mit dem Inkrafttreten der KI-Verordnung, auch AI-Act genannt, ändert sich dies nun. Die am 13. März 2024 vom Europäischen Parlament verabschiedete Verordnung muss im Wesentlichen innerhalb von 24 Monaten nach Inkrafttreten - also ab 2026 - von den Mitgliedstaaten umgesetzt werden.

Die KI-Verordnung stellt dabei auf einen technologie- und risikobasierten Ansatz ab und richtet sich im Wesentlichen an Entwickler und Anwender der Systeme. Unterschieden wird zwischen vier Risikokategorien:

1. Unannehmbares Risiko, Art. 5 KI-VO
2. Hohes Risiko, Art. 5 KI-VO
3. Beschränktes Risiko, Art. 50 KI-VO
4. Geringes Risiko, Art. 95 KI-VO

Die Entwicklung und Anwendung von KI-Systemen mit unannehmbarem Risiko sind grundsätzlich verboten, da sie eine offensichtliche Bedrohung für Sicherheit, Lebensgrundlagen und Menschenrechte darstellen. Das sind Systeme, die zu einer Diskriminierung führen können oder zum Beispiel flächendeckende Gesichtserkennungssysteme in öffentlichen Räumen. Ihr Einsatz ist nur zur Abwehr schwerer Straftaten legitimiert

Der Einsatz von KI-Systemen mit hohem Risiko, sog. Hochrisiko-KI-Systeme, ist mit umfassenden Anforderungen an das Risikomanagementsystem des Instituts als Systemanwender verbunden. Hierunter fällt insbesondere der Einsatz von KI-Systemen im Rahmen der Kreditwürdigkeitsprüfung oder des sog. Social Scoring. Dabei handelt es sich um solche KI-Systeme, die bestimmungsgemäß zur Kreditwürdigkeitsprüfung und Bonitätsbeurteilung natürlicher Personen eingesetzt werden sollen, mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug eingesetzt werden. Der Wortlaut beschränkt sich eindeutig auf natürliche Personen, so dass Systeme, die ausschließlich zur Kreditwürdigkeitsprüfung juristischer Personen eingesetzt werden, nicht unter die Regelung fallen.

Ein weiterer praxisrelevanter Anknüpfungspunkt der KI-VO kann die Identifizierung von Vertragspartnern mittels eines KI-Systems sein, etwa im Rahmen der Geldwäscheprüfung. Allerdings macht die Verordnung insoweit eine wichtige Ausnahme für solche Systeme, die bestimmungsgemäß zur biometrischen Videoidentifizierung eingesetzt werden und deren einziger Zweck darin besteht, zu bestätigen, dass eine konkrete natürliche Person diejenige ist, für die sie sich ausgibt. Dies betrifft den in der Praxis relevanten Fall der Identitätsüberprüfung natürlicher Personen durch das Videoident-Verfahren.

Der Einsatz von Hochrisiko-KI-Systemen ist naturgemäß auch mit erhöhten Risiken verbunden. So können je nach Entwicklungsstand des Systems die von ihm getroffenen Entscheidungen nicht oder nicht vollständig nachvollzogen werden, das System ist in sich eine Black Box. Diesem sogenannten Black-Box-Problem versucht die KI-VO durch umfassende Transparenzanforderungen an Entwickler und Anwender von Hochrisiko-KI-Systemen zu begegnen. So ist unter anderem eine technische Dokumentation der eingesetzten Systeme zu erstellen, die Aktivitäten der Systeme sind laufend zu protokollieren und einer regelmäßigen Überprüfung zu unterziehen.

Darüber hinaus obliegen den Entwicklern und Anwendern von Hochrisiko-KI-Systemen umfangreiche Pflichten zur Sicherstellung der Integrität und Robustheit der Trainings-, Validierungs- und Testdaten. So muss sichergestellt werden, dass die Qualität der Daten, mit denen das eingesetzte System (weiter-)lernt, welche Faktoren für die Entscheidung im Einzelfall wichtig sein könnten, nicht „verunreinigt“ oder „verzerrt“ ist. Denn das System kann nur die ihm zur Verfügung stehenden Datenmengen als Grundlage für aktuelle und zukünftige Entscheidungen heranziehen. Handelt es sich dabei um einseitige Daten, führt dies unweigerlich dazu, dass das KI-System - trotz aller Automatisierung und Autonomiebestrebungen - eine ebenfalls einseitige Entscheidung trifft, die im Einzelfall nicht richtig sein kann und von einem Menschen in der gleichen Situation trotz desselben Datensatzes vermutlich anders getroffen worden wäre. Daher müssen Hochrisiko-KI-Systeme einer menschlichen Aufsicht unterliegen, die je nach Risikoneigung des Instituts weniger streng bis sehr streng ausfallen kann.

Zu den aufsichtsrechtlichen Anforderungen hat die BaFin ein Positionspapier „Big Data und Künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen“ veröffentlicht. Hatte die BaFin die Verwendung von Systemen, die als Black Box agieren, zuvor vollständig angelehnt, soll dies nun unter bestimmten Voraussetzungen möglich sein. Zudem stellt die BaFin unter anderem die Strategie und Risikoeinschätzung des Einsatzes von KI-Systemen sowie die Auslagerung einzelner Überwachungs- und Wartungsmaßnahmen an Dritte in den Verantwortungsbereich der Geschäftsleitung.

Auch dürfen Hochrisiko-KI-Systeme nicht wie herkömmliche KI-Systeme unmittelbar nach dem Erwerb von den Anwendern in Betrieb genommen werden. Die Anwender müssen vor Inbetriebnahme des Systems ein sogenanntes Konformitätsverfahren durchlaufen, bei dem insbesondere interne Kontrollen festgelegt und das im Institut

bestehende Qualitätsmanagementverfahren bewertet und eigenständig dokumentiert werden muss.

Auch für KI-Systeme mit begrenztem Risiko sieht die KI-Verordnung die Einhaltung bestimmter Transparenzpflichten vor. Darunter kann beispielsweise der Einsatz von Chatbots durch Finanzinstitute im Rahmen der Kundenkommunikation fallen. So müssen die Institute bei der Verwendung von Chatbots die Kunden vorab darüber informieren, dass sie mit einem System kommunizieren und auf der Gegenseite keine natürliche Person agiert.

Beim Einsatz von KI-Systemen mit geringem Risiko werden den Anwendern durch die KI-VO keine besonderen Transparenzpflichten auferlegt. In diese Risikokategorie fallen beispielsweise interne Spamfilter, die in der Firewall eingesetzt werden. Es steht den Anwendern jedoch frei, freiwillig von bestimmten Anforderungen Gebrauch zu machen und institutsinterne Kodizes zu erstellen.

Neben der Kategorisierung von KI-Systemen in die verschiedenen Risikoklassen gibt es KI-Systeme mit sog. allgemeinem Verwendungszweck. Darunter fällt z.B. die Verwendung großer Sprachmodelle wie Google Gemini oder GPT-4. Für einige dieser Systeme sieht die KI-VO ein sog. systemisches Risiko, während ein solches für andere Systeme gänzlich fehlen soll. Die Folge dieser Unterscheidung sind auch hier unterschiedliche Transparenz- und Dokumentationspflichten, die von den Anwendern zu beachten sind.

Bei Verstößen gegen die Pflichten, die die KI-VO Entwicklern und Anwendern von KI-Systemen auferlegt, drohen zum Teil exorbitante Bußgelder. Die Höhe der Bußgelder richtet sich nach der Art des Verstoßes, aber auch nach dem Jahresumsatz des verstoßenden Unternehmens. Diese können bei schwerwiegenden Verstößen von bis zu 7 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres bis zu 35 Mio. Euro reichen.

Die KI-Verordnung und der konforme Einsatz bzw. Weiterbetrieb von KI-Systemen stellt die Finanzbranche vor einige Herausforderungen. Dies umso mehr, da neben den Anforderungen der KI-Verordnung beim Einsatz von KI-Systemen auch die Grundsätze der DS-GVO, des EU-Urheberrechts und der Verordnung über die digitale operationelle Resilienz im Finanzsektor (DORA) zu beachten sind (hierüber hatten wir im Newsletter aus Mai 2024 informiert).

Mit den besten Grüßen
Ihr

Dr. Christian Waigel
Rechtsanwalt