CENTRE DE DROIT
BANCAIRE ET FINANCIER

EU-Verordnung über künstliche Intelligenz

Die ersten Schritte

Par Philipp Fischer, Yannick Caballero Cuevas le 12 Juli 2024

Nach mehr als drei Jahren legislativer Geburtswehen wurde die EU-Verordnung über künstliche Intelligenz endlich im Amtsblatt veröffentlicht. Diese gilt unmittelbar für alle EU-Mitgliedstaaten, ohne dass eine Umsetzung in nationales Recht erforderlich ist. Für bestimmte Akteure und Anforderungen ist eine Übergangsregelung vorgesehen (cf. *timeline*).

Die Verordnung stellt den ersten regulatorischen Rahmen dar, der allgemein für Systeme künstlicher Intelligenz (KIS) gilt. Diese Verordnung markiert einen wichtigen Wendepunkt, auch für Schweizer Finanzdienstleister. Zum einen hat die Verordnung eine extraterritoriale Reichweite, zum anderen könnte sie über die Grenzen der Europäischen Union hinaus als Inspirationsquelle dienen. Obwohl es noch zu früh ist, um festzustellen, ob die Verordnung zu einem neuen ‚internationalen Standard' wird (wie es die DSGVO war), ist es wahrscheinlich, dass sie Auswirkungen auf die Schweiz haben wird.

Die Verordnung verfolgt einen risikobasierten Ansatz, der sowohl für KIS als auch für allgemeine KI-Modelle (General Purpose AI Models, GPAIM) gilt.

Sie unterteilt KIS in vier Kategorien, nämlich (i) KIS mit einem *unannehmbaren* Risiko (Art. 5), (ii) KIS mit einem *hohen* Risiko (Art. 6), (iii) KIS mit einem *begrenzten* Risiko (Art. 50) und (iv) KIS mit einem *minimalen* Risiko.

Für die erste Kategorie verbietet die Verordnung KI-Praktiken wie „Social Credit"-Systeme (kurz gesagt : die Bewertung natürlicher Personen über einen bestimmten Zeitraum hinweg auf der Grundlage ihres Sozialverhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Merkmale) oder biometrische Echtzeitüberwachung.

Die zweite Kategorie zielt insbesondere auf KIS ab, die zur Bewertung der Kreditwürdigkeit natürlicher Personen eingesetzt werden (*Credit Scoring*, vgl. cdbf.ch/1316/ im Zusammenhang mit der DSGVO). Für diese Systeme müssen die Anbieter und Betreiber umfangreiche technische und organisatorische Anforderungen erfüllen (auf die Definition der Begriffe Anbieter und Betreiber wird weiter unten eingegangen). Jedes KIS mit hohem Risiko muss die durch die Verordnung auferlegten Anforderungen erfüllen, bevor es auf dem europäischen Markt in Betrieb genommen wird. Diese Anforderungen müssen nicht nur während des Zulassungsverfahrens vor der zuständigen nationalen Behörde, sondern auch während des gesamten Lebenszyklus des KIS erfüllt werden.

Die dritte Kategorie umfasst KIS, die gemäß der Verordnung weder verboten sind noch ein hohes Risiko darstellen, für die aber bestimmte Transparenzanforderungen gelten.

Die letzte Kategorie schließlich betrifft KI-Anwendungen, die in Videospielen oder Spamfiltern eingesetzt werden und für die die Verordnung keine besonderen regulatorischen Anforderungen vorsieht.

Liegt ein GPAIM vor, muss geprüft werden, ob das Modell ein systemisches Risiko darstellt, das aufgrund seiner Tragweite erhebliche Auswirkungen auf den europäischen Markt haben könnte, oder tatsächliche oder vernünftigerweise vorhersehbare negative Auswirkungen auf die öffentliche Gesundheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft als Ganzes hat, die sich über die gesamte Wertschöpfungskette ausbreiten können (Art. 51).

A. Materieller Anwendungsbereich

Wie bereits erwähnt, gilt die Verordnung für KIS und GPAIM. Die Hinzufügung von GPAIM, die derzeit in die Verordnung aufgenommen wird, erzeugt praktische Herausforderungen bei der Koordinierung der Regeln, die für KIS und GPAIM gelten. In diesem Zusammenhang wird sich auch die Frage stellen, ob GPAIM eine Unterkategorie der KIS sind, in welchem Fall der Anbieter bewerten muss, ob sein Modell ein unannehmbares, hohes oder begrenztes Risiko darstellt.

Die Verordnung definiert ein KIS als „maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“ (Art. 3 Ziff. 1). Aus dieser Definition geht hervor, dass KIS Ergebnisse erzeugen, die physische oder virtuelle Umgebungen beeinflussen können. Darüber hinaus müssen sie einen gewissen Grad an Autonomie sowie Anpassungsfähigkeit besitzen. Diese Elemente erlauben es, Systeme aus der Definition auszuschließen, die auf einer reinen „*if-then*„-Logik basieren, zugunsten von Systemen, die versuchen, in der Eingabe (*input*) *ein* Muster (*pattern*) zu erkennen, das mit den *Mustern* in einem *Trainingsdatensatz (training data set*) verglichen werden kann.

Die Definition von GPIAMs ist noch weiter gefasst als die von KIS. Ein KI-Modell wird zu einem GPIAM, wenn es „erhebliche allgemeine Verwendbarkeit aufweist“ und „in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen“ (Art. 3 Ziff. 63). Diese Präzisierungen beziehen sich implizit auf die sogenannte generative KI. GPIAMs sind weniger streng geregelt als KIS und werden in einem separaten Abschnitt der Verordnung behandelt, da sie erst nach dem ersten Entwurf der Europäischen Kommission in die Verordnung aufgenommen wurden (vgl. cdbf.ch/1181/). ChatGPT ist ein Beispiel für GPIAM.

B. Persönlicher Anwendungsbereich

Der persönliche Anwendungsbereich der Verordnung beruht auf einer Unterscheidung zwischen denjenigen, die auf künstlicher Intelligenz basierende Systeme anbieten (Anbieter, Art. 3 Ziff. 3), und denjenigen, die sie für kommerzielle Zwecke nutzen (Betreiber, Art. 3 Ziff. 4) :

- Ein Anbieter ist derjenige, der ein KIS entwickelt oder auf dem EU-Markt zur Verfügung stellt, unabhängig davon, ob er auf entgeltlicher oder unentgeltlicher Basis handelt. Ein Lieferant muss eindeutig identifiziert werden, da er die Hauptverantwortung für die Einhaltung der Vorschriften trägt. Das Konzept des Anbieters schließt Unternehmen ein, die ein KIS wesentlich verändern oder KIS in einer nicht vorgesehenen Weise verwenden und es so in ein KIS mit *hohem* Risiko verwandeln.
- Betreiber sind kommerzielle Nutzer von KIS, die diese Systeme unter ihrer eigenen Autorität betreiben. Damit wird die private Nutzung in einem nicht beruflichen Kontext ausgeschlossen.

Die Verordnung sieht auch Verpflichtungen für Importeure und Händler vor, wobei letztere in bestimmten Fällen auch als Anbieter eingestuft werden können.

C. Territorialer Anwendungsbereich

Die Verordnung hat einen breiten territorialen Anwendungsbereich, der nicht nur Akteure innerhalb der EU, sondern auch außerhalb der EU umfasst, wenn ihre KIS Personen in der EU betreffen oder wenn Ergebnisse, die von außerhalb der EU angesiedelten KIS erzeugt wurden, in der EU verwendet werden (Art. 2). Das Ziel des europäischen Gesetzgebers war es, die Umgehung der Verordnung durch Aktivitäten außerhalb der EU zu verhindern, die den europäischen Binnenmarkt beeinflussen würden. Daher kann die Verordnung auch extraterritorial angewendet werden.

Schweizer Unternehmen müssen den Transparenz- und Compliance-Verpflichtungen besondere Aufmerksamkeit schenken, wenn ihre Aktivitäten oder Produkte, die künstliche Intelligenz beinhalten, Nutzer innerhalb der EU betreffen. Auch ohne direkt auf dem EU-Markt tätig zu sein, könnte die Verordnung auf diese Unternehmen angewendet werden, beispielsweise wenn das Ergebnis (*Output*) ihrer KI absichtlich in der EU verwendet wird.

D. Schlussfolgerung

Die Verordnung legt den Grundstein für einen neuen Regulierungsrahmen, den es zu erkunden gilt. Sie ist für Schweizer Finanzdienstleister in mehrfacher Hinsicht von Bedeutung : (i) Einige Finanzdienstleister verfügen über Niederlassungen in der EU, auf die die neuen Regeln anwendbar sind, (ii) einige Bestimmungen der Verordnung haben extraterritoriale Auswirkungen und (iii) die Verordnung ist einer der Regulierungsansätze, die das UVEK bei der Erfüllung des Auftrags des Bundesrats, bis Ende 2024 „mögliche Regulierungsansätze im Bereich der künstlichen Intelligenz“ aufzuzeigen, wahrscheinlich heranziehen wird. Künstliche Intelligenz hat auch Eingang in das „Risk Monitoring“ 2023 der FINMA gefunden.

Die EU-Verordnung über KI wird erhebliche Auswirkungen auf die Finanzindustrie haben. Das Zentrum für Bank- und Finanzrecht wird eine Reihe von Kommentaren zu diesem Thema veröffentlichen. Darüber hinaus wird dieses Thema im Rahmen des Journée 2024 de droit bancaire et financier vorgestellt werden.

Reproduction autorisée avec la référence suivante: Philipp Fischer, Yannick Caballero Cuevas, Die ersten Schritte, publié le 12 Juli 2024 par le Centre de droit bancaire et financier, https://cdbf.ch/de/1359/