EU KI-VO ("AI Act") mit Fokus auf Banken

Forum für Bankrecht

BWG – Österreichische Bankwissenschaftliche Gesellschaft

Christoph Herbst

5. November 2024

KI-Anwendungen bei Kreditinstituten und verbundene Risiken

- Kreditprüfung
- Betrugserkennung
- Verhinderung von Geldwäsche und Terrorismusfinanzierung
- Chat- und Talkbots
- Risikomanagement
- Compliance
- ….

Aufsichtsrechtliche Implikationen

- Verantwortung für alle Entscheidungen, die ein KI-System trifft, liegt bei der Geschäftsleitung (§ 39 BWG)

- Erklär- und Kontrollierbarkeit der grundlegenden Aufgabenbeschreibungen und maßgebenden Entscheidungsparameter (§ 39 BWG)

Ansatz der KI-VO

- Bereichsübergreifend
- in erster Linie ein produktsicherheitsrechtlicher Ansatz (vgl New Legal Framework)
- keine umfassende Regulierung von KI-Systemen – sektorspezifische Regelungen ?
- strukturelle Herausforderungen bereits bei Konzeption, Modellierung, Training von KI-Systemen
- Abweichungen vom produktsicherheitsrechtlichen Ansatz: verbotene Praktiken gemäß Art 5 und GPAI-Modelle
- Kritik an der KI-VO

Zeitlicher und örtlicher Geltungsbereich

- Abgestuftes zeitliches Inkrafttreten von Bestimmungen der VO

- Örtlicher Geltungsbereich:
  - ❖ Niederlassungsprinzip
  - ❖ Marktortprinzip – extraterritoriale Wirkung

Sachlicher Geltungsbereich

- "KI-System" ist gemäß Art 3 Nr 1
  (i) ein maschinengestütztes System
  (ii) das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und
  (iii) das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben
  (iv) für explizite oder in implizite Ziele
  (v) ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden,
  (vi) die physische oder virtuelle Umgebungen beeinflussen können

- GPAI-Modell ("KI-Modell mit allgemeinem Verwendungszweck")

Persönlicher Geltungsbereich

- Verpflichtete
  - ❖ Anbieter
  - ❖ Betreiber
  - ❖ Einführer, Händler, Produkthersteller und sog Bevollmächtigte

- Geschützte Personen

Geschützte Rechtsgüter / Risikobasierter Ansatz

- hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und Grundrechte der GRC, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz (Art 1 Abs 1)
- sektorübergreifende Regelung → risikobasierter Ansatz
- vier Risikostufen
  - ❖ verbotene Praktiken (Art 5)
  - ❖ Hochrisiko-KI-Systeme
  - ❖ KI-Anwendungen mit Transparenzrisiko
  - ❖ Einfache KI-Systeme

Hochrisiko-KI-System als "Kern" der KI-VO

- Klassifizierung (Einstufung)
  - ❖ Produktsicherheitsrechtliche Einstufung (Art 6 Abs 1)
  - ❖ "eigenständige" Einstufung nach Einsatzfeld (Art 6 Abs 2 iVm Anhang III) – ua Kreditwürdigkeitsprüfung und Bonitätsprüfung natürlicher Personen

- Änderungs- und Ergänzungsmöglichkeiten für Europäische Kommission

Anforderungen an Hochrisiko-KI-Systeme

- Risikomanagementsystem (Art 9)
- Daten-Governance (Art 10)
- technische Dokumentation (Art 11)
- automatische Aufzeichnung von Ereignissen (Art 12)
- Transparenzanforderungen und Betriebsanleitungen (Art 13)
- menschliche Aufsicht (Art 14)
- Genauigkeit, Robustheit und Cybersicherheit (Art 15)

Pflichten bei Hochrisiko-Systemen

- Anbieter
  - ❖ Compliance-by-design-Ansatz (Art 13-15)
  - ❖ Qualitätsmanagement (Art 17)
  - ❖ Aufbewahrung der Dokumentation (Art 18, 19)
  - ❖ Korrekturmaßnahmen und Informationspflicht (Art 20)
  - ❖ Zusammenarbeit mit Behörden (Art 21)
- Betreiber (Art 26)
  - ❖ Anwendung entsprechend der Betriebsanleitung
  - ❖ Meldung bei schwerwiegendem Vorfall
  - ❖ menschliche Aufsicht
  - ❖ Aufbewahrung automatisierter Protokolle
  - ❖ weitere Pflichten

Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme (Art 27)

- Sachlicher Anwendungsbereich
- Persönlicher Anwendungsbereich
- Zeitpunkt
- Prognoseentscheidung / Prüfungsmaßstab
- Inhalt
- Dokumentation
- Mitteilungspflicht
- (in Kombination mit) Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO
- Fragebogenmuster

Harmonisierte Normen und gemeinsame Spezifikationen (Art 40 ff)

- Europäische Normung
- Bedeutung der Standardisierung in KI-VO
- Harmonisierte Normen und Normungsdokumente (Art 40)
- Gemeinsame Spezifikation (Art 41)
- Legitimationsdefizit der harmonisierten Normen?
- Eignung des produktsicherheitsrechtlichen Ansatzes für die Regulierung der KI ?

KI-Systeme mit besonderen Transparenzpflichten für Anbieter und Betreiber

- Chatbots
- Deepfakes
- Ausnahmen

Haftung

- Entwurf der Änderung der Produkthaftungsrichtlinie
  - ❖ Offenlegungspflichten
  - ❖ Kausalitätsvermutung

- Entwurf einer Richtlinie zur Anpassung von Vorschriften über außervertragliche zivilrechtliche Haftung
  - ❖ Offenlegungspflichten
  - ❖ Vermutung der Verletzung der Sorgfaltspflichten
  - ❖ Kausalitätsvermutung

Verhältnis zu anderen Rechtsgebieten, insb DSGVO

- (Weitestgehende) Parallele Anwendbarkeit der DSGVO und der KI-VO
- Begriff der KI in DSGVO
- Verpflichtungen nach DSGVO und KI-VO zu erfüllen
- Sonderfall: Verbot der automatisierten Einzelfallentscheidung gemäß Art 22 DSGVO
- Zusammenspiel von Art 22 DSGVO und KI-VO

Aufsichtsgremien

- Europäische Kommission (Amt für Künstliche Intelligenz) – Art 64ff
- Europäischer Ausschuss für Künstliche Intelligenz – Art 65, 66
- Beratungsforum – Art 67
- Wissenschaftliches Gremium unabhängiger Sachverständiger – Art 68, 69
- Europäischer Datenschutzbeauftragter
- Nationale Behörden
  - ❖ notifizierende Behörde
  - ❖ Marktüberwachungsbehörde(n)

Nationale Regulierungsmöglichkeiten

- Wenige Öffnungsklauseln in KI-VO
- KI-VO enthält keine Aussage über Rechtmäßigkeit des Einsatzes von KI-Systemen
- Nationaler Gesetzgeber kann den Einsatz von KI-Systemen – ungeachtet des Verbotskatalogs in Art 5 KI-VO – verbieten oder einschränken

Rechtsbehelfe - Sanktionen

- (Popular-)Beschwerde bei Marktüberwachungsbehörde – Art 85
- (Betroffenen-)Recht auf Erläuterungen zur Rolle des KI-Systems im Entscheidungsverfahren – Art 86
- hohe Geldbußen – Art 99 Abs 3 und 4 (vergleichbar den einschlägigen Regelungen im Finanzmarktaufsichtsrecht und in der DSGVO)