Deloitte.
Legal

KI-Aufsicht im Finanzsektor: Die Bafin wird Marktüberwachungsbehörde

Was Banken, Versicherer und Kapitalverwaltungs-gesellschaften jetzt tun müssen

Stand: August 2026

Regulatorische Einordnung, Auswirkungen und Handlungs-empfehlungen zum Inkrafttreten des KI-Marktüberwachungs- und Innovationsförderungsgesetzes (KI-MIG)

Executive Summary

Kernaussage: Mit dem Inkrafttreten des KI-MIG übernimmt die Bafin im Rahmen des in Deutschland geltenden hybriden Aufsichtsmodells – neben der zentralen Marktüberwachungsbehörde Bundesnetzagentur (BNetzA) - die sektorspezifische Marktüberwachung für KI-Systeme, die in direktem Zusammenhang mit regulierten Finanztätigkeiten stehen. Damit wird die Einhaltung des AI Act (Verordnung (EU) 2024/1689) Teil der praktischen Finanzaufsicht. Geschäftsleitungen sollten KI-Governance deshalb nicht als isoliertes Innovations- oder IT-Thema behandeln, sondern in die bestehende Compliance-, Risiko- und Auslagerungssteuerung integrieren

- **Unmittelbarer Handlungsdruck**: Die Pflichten zu KI-Kompetenz und verbotenen Praktiken gelten bereits; die Transparenzpflichten nach Art. 50 AI Act sind seit dem 2. August 2026 anzuwenden.
- **Dokumentation der Zuständigkeitszuordnung**: Die Bafin ist für KI-Systeme mit unmittelbarem Bezug zu regulierten Finanztätigkeiten zuständig; horizontale Anwendungen können in die Zuständigkeit der Bundesnetzagentur fallen. Diese Zuordnung sollte durch Insitute im KI-Inventar je Anwendung dokumentiert werden.
- **Hochrisiko-Roadmap:** Für erfasste Systeme, insbesondere in der Kreditwürdigkeitsprüfung natürlicher Personen sowie in der Risiko- und Preisbewertung der Lebens- und Krankenversicherung, sind die Anforderungen an Hochrisiko-Systeme, insbesondere Rollen, Klassifizierung und Kontrollanforderungen, bis zum 2. Dezember 2027 belastbar umzusetzen.
- **Prioritäten für die Umsetzung**: Institute sollten kurzfristig ein vollständiges KI-Inventar, klare Verantwortlichkeiten, rollenbasierte Kompetenzprogramme, Transparenzprozesse und risikoadäquate Vertragsstandards für KI-Systeme etablieren und mit DORA, MaRisk, DSGVO sowie dem bestehenden Modellrisikomanagement verzahnen.
- **Unmittelbarer Handlungsdruck**: Die Pflichten zu KI-Kompetenz und verbotenen Praktiken gelten bereits; die Transparenzpflichten nach Art. 50 AI Act sind seit dem 2. August 2026 anzuwenden.

1. Ausgangslage: Ein neues Kapitel der Finanzaufsicht

Mit Inkrafttreten des Gesetzes zur Durchführung der Verordnung (EU) 2024/1689 – des sogenannten KI-Marktüberwachungs- und Innovationsförderungsgesetzes (KI-MIG) – hat der deutsche Gesetzgeber die Bafin am 29. Juli 2026 als Marktüberwachungsbehörde für KI-Systeme im Finanzsektor benannt. Die BaFin überwacht sektorspezifisch die bereits anwendbaren Pflichten des AI Act, soweit KI-Systeme in direktem Zusammenhang mit einer regulierten Finanztätigkeit stehen; die Marktüberwachung der Anforderungen an Hochrisiko-KI-Systeme setzt ab dem 2. Dezember 2027 ein. Damit rückt der AI Act – neben DORA, MiCAR, MaRisk und den sonstigen sektorspezifischen Organisationspflichten – endgültig in den Kernbereich der praktischen Aufsicht über Kreditinstitute, Versicherungsunternehmen und weitere Finanzakteure.

Bafin-Präsident Mark Branson hat in seiner begleitenden Erklärung deutlich gemacht, dass die Verantwortung für den Einsatz von KI bei den beaufsichtigten Unternehmen und ihren Geschäftsleitungen liegt. Für die Institute bedeutet das: KI ist nicht länger ein Innovations- oder IT-Thema, sondern eine Compliance-, Governance- und Vorstandsverantwortung.

2. Regulatorischer Rahmen und Zuständigkeitsabgrenzung

Der AI Act ist als produktsicherheitsrechtlich geprägte, unmittelbar geltende EU-Verordnung konzipiert. Die Mitgliedstaaten müssen für die Durchsetzung Marktüberwachungsbehörden benennen. Das KI-MIG begründet in Deutschland ein hybrides Aufsichtsmodell. Die Bafin ersetzt die allgemeine KI-Aufsicht nicht, sondern tritt für den Finanzsektor neben die allgemeine Marktüberwachungsstruktur. Dementsprechend regelt § 2

Abs. 3 KI-MIG die sektorale Zuständigkeit der Bafin. Erfasst sind insbesondere:

- Kreditinstitute und Finanzdienstleistungsinstitute und in Deutschland errichtete Zweigstellen unter Aufsicht der Bafin und der EZB (SSM-VO);
- Versicherungs- und Rückversicherungsunternehmen sowie Pensionsfonds;
- Kapitalverwaltungsgesellschaften, Wertpapierinstitute und Zahlungsdienstleister;
- Emittenten signifikanter vermögenswertreferenzierter Token (Art. 43 ff. MiCAR);
- die Versorgungsanstalt des Bundes und der Länder (VBL).

Wichtig ist die Abgrenzung: Die Bafin wird nur tätig, soweit das KI-System in unmittelbarem Zusammenhang mit einer regulierten Finanztätigkeit steht. Für horizontale Anwendungen – etwa KI-gestütztes Recruiting, HR-Analytics oder allgemeine interne Verwaltungssoftware – bleibt gemäß Verlautbarung der BaFin die Bundesnetzagentur als zentrale nationale Marktaufsichtsbehörde und Koordinierungsstelle zuständig. In der Praxis führt dies zu einem Zuständigkeits-Splitting innerhalb ein und desselben Instituts, das im KI-Inventar sauber dokumentiert werden muss. Der AI Act sieht für die Europäische Zentralbank keine Marktüberwachungs-aufgaben vor. Diese Aufgabe soll grundsätzlich von nationalen Behörden übernommen werden, vgl. Artikel 70 Absatz 1 Satz 1 AI Act.

3. Gestaffelte Anwendbarkeit – die relevanten Stichtage

Die Pflichten des AI Act greifen zeitlich gestaffelt. Für Finanzunternehmen sind vor allem folgende Termine maßgeblich:

- **2. Februar 2025** – Anwendbarkeit der verbotenen KI-Praktiken nach Art. 5 AI Act sowie der KI-Kompetenzpflicht nach Art. 4 AI Act.
- **2. August 2025** – Anwendbarkeit der Vorschriften zu KI-Modellen mit allgemeinem Verwendungszweck (GPAI, Art. 51 ff.) und der Sanktionsvorschriften.
- **2. August 2026** – Wirksamwerden der Transparenzpflichten nach Art. 50 AI Act (u. a. für Chatbots, synthetische Inhalte, Deepfakes, Emotionserkennung) sowie der überwiegenden Governance-Regeln.

- **2. Dezember 2027** – Anwendbarkeit der Anforderungen an Hochrisiko-KI-Systeme nach Anhang III Nr. 5 lit. b) und c) AI Act (Kreditwürdigkeits- und Bonitätsprüfung natürlicher Personen sowie Risikobewertung und Preisbildung in der Lebens- und Krankenversicherung).

Hinweis: In der öffentlichen Kommunikation zum KI-MIG kursiert vereinzelt der 2. Dezember 2026 als Stichtag für Hochrisiko-Systeme. Maßgeblich ist jedoch der von der BaFin genannte 2. Dezember 2027. Die Verschiebung beruht auf der Verordnung (EU) 2026/1744 (Digital-Omnibus-Verordnung zur KI), welche die Verordnung (EU) 2024/1689 geändert und die Übergangsfrist für die einschlägigen Hochrisiko-KI-Systeme nach Anhang III verlängert hat.

4. Materielle Kern-pflichten und ihre Be-deutung für die Praxis

4.1 KI-Kompetenz (Art. 4 AI Act)

Anbieter und Betreiber müssen unter Berücksichtigung ihrer technischen Kenntnisse, ihrer Erfahrung, ihrer Ausbildung und Schulung sowie des Einsatzkontexts Maßnahmen ergreifen, um bei ihrem Personal und sonstigen in ihrem Auftrag mit Betrieb und Nutzung befassten Personen ein ausreichendes Maß an KI-Kompetenz sicherzustellen. Ein bestimmtes Kompetenzniveau jeder einzelnen Person muss nach der Aufsichtskommunikation der Bafin nicht garantiert werden. Bestehende Schulungskonzepte sollten deshalb risikoorientiert und adressatengerecht erweitert werden; einzubeziehen sind diejenigen Funktionen, deren Aufgaben durch Entwicklung, Beschaffung, Freigabe, Nutzung, Kontrolle oder Prüfung von KI-Systemen berührt werden.

4.2 Verbotene Praktiken (Art. 5 AI Act)

Art. 5 AI Act enthält einen abschließenden Katalog verbotener KI-Praktiken. Für den Finanzsektor besonders relevant sind insbesondere die Verbote manipulativer oder täuschender Techniken, der Ausnutzung bestimmter Vulnerabilitäten und des Social Scoring. Die Verbote für

bestimmte Formen der Emotionserkennung und biometrischen Kategorisierung knüpfen dagegen an spezifische Verfahren und Einsatzkontexte an; klassische Betrugserkennung ist nicht ohne Weiteres hierunter zu fassen. Verstöße können mit Geldbußen von bis zu 35 Mio. EUR oder – bei Unternehmen – 7 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden, je nachdem, welcher Betrag höher ist.

4.3 Transparenzpflichten (Art. 50 AI Act)

Ab dem 2. August 2026 gelten die rollen- und anwendungsbezogenen Transparenzpflichten des Art. 50 AI Act. Anbieter von Systemen, die unmittelbar mit natürlichen Personen interagieren, müssen diese grundsätzlich über den KI-Einsatz informieren; dies gilt nicht, wenn die KI-Natur aus Sicht einer hinreichend informierten, aufmerksamen und verständigen Person offensichtlich ist (z.B. bei offensichtlich KI-basierten Chatbots oder digitalen Assistenten). Weitere Pflichten betreffen insbesondere synthetische Audio-, Bild-, Video- oder Textinhalte sowie Deepfakes und unterscheiden zwischen Anbieter- und Betreiber-pflichten. Für Finanzunternehmen sind vor allem Chatbots und Voice-Bots in der Kundenkommunikation sowie KI-generierte Marketing- und Kundeninhalte relevant (z.B. durch Hinweise bei KI-gestützter Kundenkommunikation und die Kennzeichnung bestimmter KI-generierter Marketinginhalte)

4.4 Hochrisiko-KI-Systeme (Art. 6 ff. AI Act)

Ab dem 2. Dezember 2027 gelten die umfangreichen materiellen Anforderungen für die erfassten Hochrisiko-Systeme. Welche Pflichten das Finanzunternehmen treffen, hängt zunächst von seiner Rolle ab: Die Anforderungen an Risikomanagement, Daten und Daten-Governance, technische Dokumentation, Aufzeichnungen, Transparenz gegenüber Betreibern, menschliche Aufsicht, Genauigkeit, Robustheit, Cyber-sicherheit und Qualitätsmanagement richten sich weitgehend an Anbieter; Betreiber unterliegen insbesondere den Vorgaben des Art. 26 AI Act. Ein Finanzunternehmen kann jedoch etwa durch Eigenentwicklung, wesentliche Veränderung oder Zweckänderung eingesetzter KI-Systeme selbst zum Anbieter werden. Ausdrücklich erfasst sind KI-Systeme zur Bewertung der Kreditwürdigkeit natürlicher Personen oder zur Ermittlung ihres Kreditscores – mit Ausnahme reiner Betrugserkennung – sowie zur Risikobewertung und Preisbildung in der Lebens- und Kranken-versicherung. Kfz-Tarifierung, Sachversicherung und gewerbliche Kreditvergabe werden von Anhang III Nr. 5 lit. b) und c) nicht erfasst; eine Hochrisikoeinstufung nach anderen Tatbeständen des Art. 6 und der Anhänge ist im Einzelfall gesondert zu prüfen.

5. Auswirkungen auf beaufsichtigte Unternehmen

Der AI Act tritt nicht in ein regulatorisches Vakuum ein. Er ergänzt die bestehenden Anforderungen insbesondere aus MaRisk – einschließlich AT 4.3.4 zur Verwendung von Modellen und AT 9 zu Auslagerungen –, DORA, DSGVO und bei Kreditvergaben den EBA-Leitlinien zur Kreditvergabe und -überwachung (EBA/GL/2020/06). Die VAIT, KAIT und ZAIT wurden mit Ablauf des 16. Januar 2025 aufgehoben. Die BAIT gelten seit dem 17. Januar 2025 nur noch für einen eingeschränkten Restanwenderkreis und werden mit Ablauf des 31. Dezember 2026 vollständig aufgehoben. Daraus resultieren drei zentrale Effekte:

- **Doppelte Aufsichtsperspektive**: Dieselbe KI-Anwendung kann gleichzeitig Gegenstand der laufenden Institutsaufsicht (z. B. § 25a KWG, § 23 VAG) und der neuen Marktüberwachung sein. Die BaFin hat angekündigt, beide Perspektiven organisatorisch eng zu verzahnen.
- **Drittanbieter- und Auslagerungsperspektive**: Je nach Funktion, Leistungsinhalt und Einbindung können externe KI-Dienste als Auslagerung nach AT 9 MaRisk oder als Bezug einer IKT-Dienstleistung nach DORA einzuordnen sein. Verträge sollten risikoadäquate Informations-, Dokumentations-, Prüf-, Protokollierungs-, Kooperations- und Änderungsrechte sowie gegebenenfalls Anforderungen an Konformitätsnachweise und laufende Überwachung vorsehen.
- **Verschärfte Sanktionsarchitektur**: Neben den Bußgeldern des AI Act (bis 35 Mio. EUR / 7 %) kann die BaFin flankierend aufsichtsrechtliche Maßnahmen nach KWG/VAG ergreifen, einschließlich der Untersagung des KI-Einsatzes und der Anordnung von Nachbesserungen gegenüber der Geschäftsleitung.

6. Praktische Handlungsempfehlungen

Aus unserer Beratungspraxis ergeben sich sechs Prioritäten für die kommenden 12 bis 18 Monate:

- **KI-Inventar aufbauen oder erweitern**: Das Inventar sollte strukturell mit dem DORA-Inventar der Informations- und IKT-Assets abgestimmt oder technisch verknüpft werden, ohne seine eigenständige regulatorische Funktion zu verlieren. Jedes KI-System ist nach einschlägiger Risikokategorie, Rolle des Instituts – etwa Anbieter, Betreiber oder nachgelagerter Anbieter – und zuständiger Marktüberwachungsbehörde zu klassifizieren.
- **AI-Governance-Framework verankern und Compliance-Synergien bilden**: Verantwortlichkeiten entlang der drei Verteidigungslinien klar festlegen, das Modell- und IKT-Risikomanagement anbinden und einen risikoadäquaten Freigabeprozess für neue KI-Systeme und -Anwendungsfälle etablieren. Eine spezialisierte AI-Risk-Function kann hierfür eine sinnvolle Gestaltungsoption sein, ist aber nicht als solche gesetzlich vorgeschrieben.
- **KI-Kompetenzprogramm ausrollen**: Rollenbasierte Curricula für Geschäftsleitung Verwaltungs- oder Aufsichtsorgan, Fachbereiche, Entwicklung, Compliance, Datenschutz und Interne Revision vorsehen. Maßnahmen, Zielgruppen, Inhalte und Aktualisierungszyklen sollten nachvollziehbar dokumentiert und risikoadäquat ausgestaltet werden.
- **Transparenzprozesse ab 2. August 2026 anwenden**: Für jeden KI-Anwendungsfall prüfen, ob und welche Anbieter- oder Betreiberpflicht des Art. 50 AI Act greift. Erforderliche Nutzerhinweise, maschinenlesbare Kennzeichnungen oder Offenlegungen für synthetische Inhalte und Deepfakes sind rollen- und medienbezogen umzusetzen; pauschale Wasserzeichenpflichten bestehen nicht für jede KI-gestützte Kommunikation.
- **Hochrisiko-Roadmap bis 2. Dezember 2027**: Zunächst Rolle und Risikoeinstufung je System bestimmen; anschließend die jeweils einschlägigen Anbieter- und Betreiberpflichten analysieren. Für eigene oder übernommene Anbieterrollen sind insbesondere Risikomanagement, Daten-Governance, technische Dokumentation, Qualitätsmanagement und gegebenenfalls Post-Market-Monitoring sowie Vorfallmeldungen aufzubauen; Betreiber müssen insbesondere die Anforderungen an ordnungsgemäße Nutzung, menschliche Aufsicht, Protokolle und Überwachung abbilden.
- **Lieferanten- und Auslagerungsverträge risikoadäquat überprüfen**: Abhängig von Rolle, Risikoklasse und Leistungsmodell sind insbesondere Informations-, Dokumentations-, Audit-,

Protokollierungs-, Änderungs- und Kooperationsrechte vorzusehen. Bei proprietären Modellen sollten abgestufte Nachweise und angemessene Zugangsrechte vereinbart werden; ein uneingeschränkter Zugriff auf Modell- oder Trainingsdaten ist weder stets erforderlich noch praktisch durchsetzbar.

7. Fazit

Die Benennung der Bafin als sektorspezifische Marktüberwachungsbehörde ist mehr als eine Zuständigkeitsergänzung: Sie markiert den Übergang von einer bislang überwiegend grundsatzorientierten, zentralen KI-Aufsicht zu einer eigenständigen Marktüberwachung mit spezifischen Eingriffsbefugnissen und Sanktionen. Unternehmen, die ihre KI-Governance bereits konsequent an DORA, MaRisk und den einschlägigen sektorspezifischen Organisationspflichten ausrichten, verfügen über eine belastbare Grundlage, müssen jedoch die rollen- und risikobezogenen Pflichten des AI Act ergänzend abbilden und sollten hierbei Synergien zu bereits bestehenden Pflichten diesbezüglichen Prozessen prüfen und realisieren. Die bereits geltenden Vorgaben zu KI-Kompetenz und verbotenen Praktiken sowie die ab dem 2. August 2026 einschlägigen Transparenzpflichten verlangen kurzfristig belastbare Prozesse. Für Hochrisiko-KI-Systeme bleibt bis zum 2. Dezember 2027 Zeit, Rollen, Klassifizierung und Kontrollrahmen systematisch umzusetzen. Dabei gilt der von Bafin-Präsident Mark Branson formulierte Verantwortungsmaßstab: „Die Verantwortung für den Einsatz von KI liegt bei den beaufsichtigten Unternehmen und ihren Geschäftsleitungen.“

Kontaktieren Sie uns

Felix Brandes

Partner | Banking & Finance

fbrandes@deloitte.de
+49 511 30755 9316

Dr. Söntje J. Hilberg

Partnerin | Co-Lead Digital Law

shilberg@deloitte.de
+49 170 766 3353

Deloitte.
Legal

Deloitte Legal bezieht sich auf die Rechtsberatungspraxen der Mitgliedsunternehmen von Deloitte Touche Tohmatsu Limited, deren verbundene Unternehmen oder Partnerfirmen, die Rechtsdienstleistungen erbringen.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation"). DTTL (auch „Deloitte Global" genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter www.deloitte.com/de/UeberUns.

Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeitenden liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 460.000 Mitarbeitenden von Deloitte das Leitbild „making an impact that matters" täglich leben: www.deloitte.com/de.

MAKING AN IMPACT THAT MATTERS since 1845