



KI im Finanzsektor: Kernaussagen des neuen OECD-Papers für die Aufsicht

Wie Regulierung, DORA und BaFin-Praxis den Einsatz von KI konkret prägen

Sehr geehrte Leser*innen,

der Einsatz von Künstlicher Intelligenz im Finanzsektor stellt Institute und Aufsichtsbehörden vor neue Herausforderungen. Das aktuelle OECD-Paper zeigt, dass bestehende, technologieneutrale Regelwerke grundsätzlich ausreichen – entscheidend ist jedoch deren praktische Umsetzung.

Dieses Whitepaper fasst die Kernaussagen zusammen, beleuchtet aufsichtliche Themen wie Governance, Modellrisiken, Datenqualität und Drittanbietersteuerung und ordnet diese in den europäischen Kontext mit DORA und BaFin-Praxis ein. Sie erhalten eine kompakte Orientierung, wie KI-Systeme regulatorisch belastbar, transparent und aufsichtsfest gestaltet werden können.

Über die Autorin:

Josefine Spengler ist Rechtsanwältin und Fachanwältin für IT-Recht im Berliner Büro von Annerton. Sie verfügt über langjährige Inhouse-Erfahrung als Head of Legal und Datenschutzbeauftragte bei einem Payment Service Provider. Als Expertin im IT- und FinTech-Segment berät Josefine Spengler nationale und internationale Mandanten in allen Fragen an der Schnittstelle zwischen Regulierungsrecht und IT-Recht sowie zu Compliance- und AML-Themen. Josefine Spengler ist regelmäßig Referentin bei Veranstaltungen zum IT-Recht und zu regulatorischen Anforderungen an die IT von Finanzunternehmen.



KI im Finanzsektor – Kernaussagen des neuen OECD-Papers

von **Josefine Spengler** 3. Februar 2026 7 Minuten



Foto: Seerat/Adobestock

Im Finanzsektor nimmt die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) seit Jahren eine zentrale Rolle als Policy- und Thought Leader ein, insbesondere dort, wo technologische Entwicklungen nationale Regulierungsansätze überlagern und internationale Abstimmung erforderlich wird. Mit dem am 27. Januar 2026 veröffentlichten OECD-Paper „Supervision of Artificial Intelligence in Finance – Challenges, Policies and Practices“ liegt nun eine internationale Bestandsaufnahme zur Frage vor, wie die Aufsichtsbehörden den Einsatz von Künstlicher Intelligenz (KI) im Finanzsektor praktisch überwachen. Die OECD nimmt dabei bewusst eine übergeordnete Perspektive ein: Sie geht davon aus, dass die Mitgliedstaaten grundsätzlich über geeignete regulatorische Rahmenwerke verfügen, identifiziert jedoch erhebliche Herausforderungen bei der aufsichtlichen Auslegung und Anwendung dieser Regeln im Kontext zunehmend komplexer KI-Systeme.

Inhaltsverzeichnis

Methodik und Aufbau des OECD-Papiers

Typische Einsatzfelder von KI aus Sicht der Aufsicht

Aufsichtliche Kernprobleme aus OECD-Sicht

Technologieneutralität als Leitprinzip – mit praktischen Grenzen

Herausforderungen bei der praktischen Umsetzung

Aufsicht braucht eigene KI-Kompetenz

Aufsichtsansätze im internationalen Vergleich

Aufsichtspraxis: Mehr Guidance statt neuer Regeln

Einordnung für Europa und Deutschland – Anschluss an DORA und die BaFin-Praxis

Fazit: Von der Regulierung zur aufsichtsrechtlichen Realität

Der besondere Mehrwert des OECD-Papiers liegt darin, dass es die aufsichtliche Praxis in den Mittelpunkt stellt und untersucht, wie Aufsichtsbehörden weltweit versuchen, eine verantwortungsvolle Nutzung von KI mit den zentralen Aufsichtszielen – Finanzmarktstabilität, Marktintegrität und Schutz der Finanzkundinnen und -kunden – in Einklang zu bringen. Das Papier versteht sich damit ausdrücklich nicht als regulatorischer Entwurf, sondern als Leitlinie für Aufsichtsverständnis und -praxis.

Vor diesem Hintergrund lässt sich auch die jüngst veröffentlichte BaFin-Orientierungshilfe zu IKT-Risiken beim Einsatz von KI einordnen. Sie stellt ein nationales Beispiel dafür dar, wie die im OECD-Paper beschriebenen Herausforderungen aufsichtspraktisch operationalisiert werden können. Während der OECD-Beitrag den internationalen Rahmen absteckt, zeigt die BaFin-Orientierungshilfe, wie bestehende europäische Vorgaben, insbesondere DORA, konkret auf KI-Systeme angewendet werden (siehe hierzu auch: „KI im Finanzsektor: Einordnung und praktische Bedeutung der neuen BaFin-Orientierungshilfe zum Einsatz von KI“ vom 18.12.2025 auf PayTechLaw.com <https://paytechlaw.com/einsatz-von-ki-im-finanzenzsektor/>).

Der folgende Beitrag stellt zunächst die zentralen Aussagen des OECD-Papiers dar und ordnet diese anschließend anhand der deutschen Aufsichtspraxis ein.

Methodik und Aufbau des OECD-Papiers

Das OECD-Paper basiert auf einer qualitativen Erhebung unter Finanzaufsichtsbehörden aus OECD-Mitgliedstaaten sowie ausgewählten Nichtmitgliedern. Im Mittelpunkt stehen die Erfahrungen der Aufsichtsbehörden mit dem konkreten Einsatz von KI-Systemen in beaufsichtigten Instituten, insbesondere in

den Bereichen Kreditvergabe, Betrugsprävention, Marktüberwachung, Handel, Compliance und Kundeninteraktion. Die OECD analysiert dabei keine einzelnen Institute, sondern aggregiert aufsichtliche Erfahrungswerte, die aus Prüfungen, Meldungen, Dialogformaten und Aufsichtspraxis stammen.

Strukturell gliedert sich das Paper in drei zentrale Analyseebenen:

- den Einsatz von KI im Finanzsektor,
- die aufsichtlichen Herausforderungen bei der Überwachung dieser Systeme sowie
- die Aufsichtsansätze und Instrumente, die zur Bewältigung dieser Herausforderungen eingesetzt werden.

Ziel ist es nicht, Best Practices im Sinne verbindlicher Vorgaben zu formulieren, sondern wiederkehrende Muster und Problemlagen sichtbar zu machen.

Typische Einsatzfelder von KI aus Sicht der Aufsicht

Das OECD-Paper zeigt, dass KI im Finanzsektor bereits heute breit eingesetzt wird, allerdings mit sehr unterschiedlicher Risikointensität. Während klassische Machine-Learning-Modelle seit Jahren fester Bestandteil etwa der Betrugsbekämpfung oder des Kredit-Scorings sind, rücken zunehmend generative KI-Anwendungen in den Fokus der Aufsicht, etwa bei Kundenkommunikation, internen Analyse- und Entscheidungsunterstützungssystemen oder im Compliance-Umfeld.

Die OECD hebt hervor, dass viele Aufsichtsbehörden weniger Probleme mit klar abgegrenzten, eng kontrollierten KI-Anwendungen haben, sondern mit solchen Systemen, die

- mehrere Geschäftsprozesse gleichzeitig beeinflussen,
- sich dynamisch weiterentwickeln oder
- stark von externen Datenquellen und Drittanbietern abhängen.

Gerade diese Eigenschaften erschweren aus aufsichtsrechtlicher Sicht eine klare Verantwortungszuordnung und eine belastbare Risikoabschätzung.

Aufsichtliche Kernprobleme aus OECD-Sicht

Besonders instruktiv ist die Darstellung derjenigen Aspekte, die von Aufsichtsbehörden wiederholt als problematisch benannt werden. Dazu zählen vor allem:

Die Begrenztheit klassischer Prüfungsansätze: Viele bestehende Aufsichts- und Prüfmechanismen sind auf deterministische Systeme ausgelegt. KI-Modelle, deren Ergebnisse probabilistisch sind oder sich im Zeitverlauf verändern, lassen sich damit nur eingeschränkt erfassen.

Die Asymmetrie zwischen Institut und Aufsicht: Das Paper betont, dass Aufsichtsbehörden häufig weniger technischen Einblick in KI-Systeme haben als die beaufsichtigten Unternehmen oder deren Technologieanbieter. Dies verschärft Abhängigkeits- und Informationsrisiken.

Die Verschiebung von Risiken entlang der Wertschöpfungskette: Risiken entstehen nicht nur im Institut selbst, sondern häufig bereits bei Modelltraining, Datenbeschaffung oder durch Entscheidungen externer Anbieter – ohne dass die Aufsicht hier unmittelbar ansetzen kann.

Diese Befunde erklären, warum die OECD weniger neue Regulierung fordert, sondern eine Weiterentwicklung der Aufsichtsinstrumente.

Technologieneutralität als Leitprinzip – mit praktischen Grenzen

Ein zentrales Ergebnis des OECD-Papiers ist die Feststellung, dass die überwiegende Mehrheit der OECD-Staaten davon ausgeht, bereits über ausreichende regulatorische Rahmenwerke für den Einsatz von KI im Finanzsektor zu verfügen. Diese beruhen auf dem Grundsatz der Technologieneutralität: Bestehende Anforderungen an Governance, Risikomanagement, Verbraucherschutz, IT-Sicherheit und Auslagerungen gelten unabhängig davon, ob Entscheidungen durch Menschen, klassische statistische Modelle oder KI-Systeme getroffen werden.

Gleichzeitig macht die OECD deutlich, dass diese Technologieneutralität in der aufsichtlichen Praxis zunehmend an Grenzen stößt. Je komplexer, dynamischer und

weniger erklärbar KI-Modelle werden, desto schwieriger wird ihre Einordnung in klassische Kontroll- und Prüfmechanismen.

Herausforderungen bei der praktischen Umsetzung

Das OECD-Paper identifiziert eine Reihe wiederkehrender Problemfelder, die sich in nahezu allen untersuchten Jurisdiktionen zeigen.

Im Mittelpunkt stehen zunächst **Modellrisiken und Validierungsfragen**. Zwar gelten bestehende Modellrisiko-Frameworks grundsätzlich auch für KI-Modelle. In der Praxis bestehen jedoch erhebliche Unsicherheiten, wie Validierung, laufende Überwachung und Governance bei selbstlernenden oder nur eingeschränkt erklärbaren Systemen auszugestalten sind.

Eng damit verbunden ist das Thema **Erklärbarkeit und Fairness**. Die eingeschränkte Nachvollziehbarkeit vieler KI-Entscheidungen erschwert nicht nur interne Kontrollprozesse, sondern auch die Erfüllung aufsichtsrechtlicher Transparenz- und Begründungspflichten gegenüber Aufsichtsbehörden und Kundinnen und Kunden.

Hinzu treten **Daten- und Governance-Fragen**. Die Qualität, Herkunft und laufende Steuerung der für KI verwendeten Daten rücken stärker in den Fokus, ebenso die konkrete Ausgestaltung von „Human-in-the-Loop“-Konzepten und Verantwortlichkeiten.

Schließlich verweist die OECD auf die wachsende **Abhängigkeit von Drittanbietern**. Der Einsatz externer KI-Modelle, Cloud-Infrastrukturen und spezialisierter Technologieanbieter führt zu neuen Konzentrations-, Kontroll- und Resilienzrisiken, die sich nicht immer allein über die klassische Aufsicht über das einzelne Institut erfassen lassen.

Aufsicht braucht eigene KI-Kompetenz

Ein weiterer Schwerpunkt des OECD-Papiers liegt auf der institutionellen Leistungsfähigkeit der Aufsichtsbehörden selbst. Effektive KI-Aufsicht setzt voraus, dass Aufsichten über ausreichende technische Expertise verfügen und zunehmend KI-gestützte SupTech-Instrumente einsetzen. Investitionen in Personal, Schulung und internationale Zusammenarbeit werden als zwingende Voraussetzungen beschrieben, um mit der Geschwindigkeit der technologischen Entwicklung Schritt zu halten.

Aufsichtsansätze im internationalen Vergleich

Das OECD-Paper zeigt, dass Aufsichtsbehörden weltweit sehr unterschiedliche Wege wählen, um mit KI umzugehen. Während einige Aufsichten primär auf ex-post-Prüfung und klassische Aufsichtsinstrumente setzen, experimentieren andere mit dialogorientierten und iterativen Formaten, etwa:

- strukturierte Vorgespräche zu KI-Use-Cases,
- themenspezifische Prüfungen (z. B. Fairness, Bias, Datenqualität),
- Aufsichtssandboxes und kontrollierte Testumgebungen.

Auffällig ist, dass Aufsichtsbehörden, die frühzeitig in fachliche Kompetenz und interne Spezialisierung investiert haben, KI weniger als regulatorisches Risiko, sondern stärker als aufsichtliches Steuerungsproblem behandeln.

Aufsichtspraxis: Mehr Guidance statt neuer Regeln

Bemerkenswert ist, dass die OECD ausdrücklich nicht für eine umfassende Neuregulierung plädiert. Stattdessen empfiehlt sie gezielte aufsichtliche Klarstellungen und Guidance, wo bestehende Regeln in der Praxis als unklar oder schwer anwendbar empfunden werden. Solche Leitlinien sollen rechtliche Sicherheit schaffen, ohne die Innovationsfähigkeit des Finanzsektors durch übermäßig detaillierte Vorgaben zu beeinträchtigen.

Zugleich betont das Paper die Bedeutung eines intensiven Dialogs zwischen Aufsicht und Markt. Sandboxes, Modelltests oder strukturierte Austauschformate werden als geeignete Instrumente beschrieben, um neue Bewertungs- und Überwachungsansätze gemeinsam zu entwickeln. Als Beispiel wird unter anderem das von der UK Financial Conduct Authority angebotene „[AI Live Testing](#)“ angeführt.

Einordnung für Europa und Deutschland – Anschluss an DORA und die BaFin-Praxis

Für den europäischen Kontext ist das OECD-Paper insbesondere vor dem Hintergrund des EU AI Act, von DORA und der bestehenden sektoralen Finanzregulierung relevant. Die OECD warnt ausdrücklich davor, neue KI-spezifische Anforderungen unkoordiniert „über“ bestehende Aufsichtsregime zu legen. Stattdessen müsse die Aufsicht darauf achten, Überschneidungen, Widersprüche und Doppelanforderungen zu vermeiden und bestehende Rahmenwerke konsistent weiterzuentwickeln.

Genau an diesem Punkt setzt die BaFin-Orientierungshilfe an. Sie übersetzt die im OECD-Paper beschriebenen abstrakten Herausforderungen in konkrete aufsichtspraktische Erwartungen und ordnet KI-Systeme als IKT-Assets vollständig in die DORA-Struktur ein. Damit wird deutlich: KI ist kein regulatorischer Sonderfall, sondern eine besonders anspruchsvolle Ausprägung bestehender Risiken, die mit den bekannten Instrumenten von Governance, Risikomanagement und Aufsicht zu steuern ist.

Fazit: Von der Regulierung zur aufsichtsrechtlichen Realität

Das OECD-Paper macht deutlich, dass die eigentliche Herausforderung beim Einsatz von Künstlicher Intelligenz im Finanzsektor nicht auf der Ebene der Normsetzung, sondern auf der Ebene der aufsichtlichen und unternehmerischen Umsetzung liegt. Anders als in früheren Phasen der Finanzmarktregulierung steht heute nicht die Frage im Vordergrund, *ob* KI reguliert ist, sondern *wie* bestehende, überwiegend technologie-neutral ausgestaltete Regelwerke auf KI-gestützte Geschäftsprozesse praktisch angewendet, überwacht und durchgesetzt werden können.

Die OECD bestätigt damit einen Paradigmenwechsel in der Finanzaufsicht: KI wird nicht als eigenständiger Regulierungsgegenstand behandelt, sondern als Querschnittstechnologie, die bekannte Risikoarten – etwa Modell-, IT-, Auslagerungs-, Governance- und Verbraucherschutzrisiken – in neuer Intensität und Komplexität bündelt. Für Aufsichtsbehörden bedeutet dies, dass klassische Prüf- und Kontrollmechanismen weiterentwickelt werden müssen, ohne dabei den Grundsatz der Technologieneutralität aufzugeben.

Für Finanzinstitute ergibt sich hieraus ein klarer Befund. Der rechtssichere Einsatz von KI ist weniger eine Frage der formalen Compliance mit neuen Einzelvorschriften als vielmehr eine Frage der aufsichtsfesten Ausgestaltung interner Strukturen. Institute müssen in der Lage sein, den Einsatz von KI nicht nur technisch, sondern auch organisatorisch, prozessual und rechtlich zu erklären, zu steuern und zu verantworten. Governance-Strukturen, Verantwortlichkeiten, Modellvalidierung, Datenqualität,

Dokumentation und Drittanbietersteuerung werden damit zu zentralen Compliance-Themen.

Besonders deutlich wird dies im europäischen Kontext. Mit dem EU AI Act, DORA und der bestehenden sektoralen Finanzregulierung entsteht kein neues, in sich geschlossenes KI-Aufsichtsregime, sondern ein vielschichtiges Zusammenspiel bestehender Regelwerke, das konsistent umgesetzt werden muss. Das OECD-Paper warnt zu Recht davor, KI-spezifische Anforderungen isoliert oder additiv zu betrachten. Entscheidend ist vielmehr die Fähigkeit der Aufsicht – und der Institute –, diese Regelwerke kohärent anzuwenden und Widersprüche, Doppelanforderungen und blinde Flecken zu vermeiden.

Die BaFin-Orientierungshilfe zu Einsatz von KI zeigt exemplarisch, wie eine solche Operationalisierung aussehen kann. Sie verdeutlicht, dass KI aus aufsichtsrechtlicher Sicht kein Innovationsfreiraum außerhalb etablierter Kontrollmechanismen ist, sondern integraler Bestandteil des bestehenden IKT- und Risikomanagements. Gleichzeitig wird deutlich, dass sich die Aufsicht weniger auf abstrakte Verbote konzentriert, sondern auf die Qualität der Umsetzung und Steuerung im Einzelfall.

Vor diesem Hintergrund lässt sich das OECD-Paper auch als implizite Handlungsanleitung lesen – sowohl für Aufsichtsbehörden als auch für Marktteilnehmer. Erfolgreiche KI-Nutzung im Finanzsektor wird künftig dort stattfinden, wo Institute frühzeitig in robuste Governance, fachliche Erklärbarkeit, klare Verantwortlichkeiten und einen offenen Aufsichtsdialog investieren. KI wird damit nicht primär zum rechtlichen Risiko, sondern zu einem Stresstest für die Reife bestehender Compliance- und Risikostrukturen.

Letztlich zeigt das OECD-Paper: Die Zukunft der KI im Finanzsektor entscheidet sich nicht in neuen Gesetzestexten, sondern in der aufsichtsrechtlichen Praxis. Wer KI heute bereits als regulierten Bestandteil seines Geschäftsmodells versteht – und nicht als technisches Add-on –, wird regulatorisch besser positioniert sein, wenn sich die aufsichtsrechtlichen Erwartungen weiter verdichten.

TAGS: DORA Finanzsektor KI OECD-Papers

Praxiswissen für Ihren Erfolg im Job

Seminare zu IT, Digitalisierung und Künstlicher Intelligenz

Erhalten Sie in unseren Weiterbildungen fundiertes und praxisnahes Know-how zur digitalen Transformation und IT-Compliance im Bankensektor unter Berücksichtigung der aufsichtsrechtlichen Anforderungen aus DORA, MaRisk, DSGVO, IT-Sicherheitsgesetz und den EBA-ICT-Guidelines. [Jetzt informieren.](#)

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen. [Jetzt unverbindlich testen.](#)

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training. Jetzt individuelles [Angebot anfordern.](#)