

## Künstliche Intelligenz

# Erwartungen der FINMA in Bezug auf Governance und Risikomanagement

Par Yannick Caballero Cuevas le 19 Dezember 2024

Banken und Finanzinstitute integrieren zunehmend künstliche Intelligenz (KI) in ihre Dienstleistungen und internen Prozesse (vgl. not. Jotterand, [cdbf.ch/1377](https://www.cdbf.ch/1377)). Diese Nutzung kann insbesondere operative, rechtliche und Reputationsrisiken mit sich bringen (vgl. not. Levis, [cdbf.ch/1380](https://www.cdbf.ch/1380)). Auch eine zunehmende Abhängigkeit von Drittanbietern, insbesondere bei KI-Modellen und *Cloud-Diensten*, ist die Folge. Hinzu kommt die Schwierigkeit, klare Verantwortlichkeiten für Fehler des Systems oder des KI-Modells zuzuweisen. Der Einsatz von KI durch Banken und Finanzinstitute stellt eine grosse Herausforderung für die Aufsicht dar. Zu diesem Zweck hat die FINMA die [Aufsichtsmitteilung 08/2024](#) über Governance und Risikomanagement beim Einsatz von KI veröffentlicht, in der sie die Erkenntnisse aus ihrer Aufsicht beschreibt.

Jeder Beaufsichtigte muss die Auswirkungen des Einsatzes von KI auf sein Risikoprofil im Hinblick auf den geltenden regulatorischen Rahmen überdenken und seine Governance, sein Risikomanagement sowie sein Kontrollsystem anpassen (vgl. not. de Cannière, [cdbf.ch/1376](https://www.cdbf.ch/1376)). Neben Datenschutzfragen lenkt die FINMA die Aufmerksamkeit der Beaufsichtigten auf die Robustheit und Genauigkeit von KI-Modellen sowie auf die Notwendigkeit, sicherzustellen, dass die Ergebnisse korrekt, erklärbar und frei von Verzerrungen sind. Sie konzentriert ihre Aufsicht auf sieben Themenbereiche : (i) Governance, (ii) Risikoinventarisierung und -klassifizierung, (iii) Datenqualität, (iv) Tests und laufende Überwachung, (v) Dokumentation, (vi) Erklärbarkeit und (vii) unabhängige Überprüfung. Einige Themenbereiche finden sich im Übrigen auch in der europäischen KI-Verordnung (KI-VO), insbesondere in den [Art. 9](#) bis [15 KI-VO](#) zu den Anforderungen an KI-Systeme mit hohem Risiko.

Für die FINMA ist die Governance im Bereich der KI von entscheidender Bedeutung. Sie muss anhand der Risiken, die von den Beaufsichtigten identifiziert wurden, aufgebaut werden. Die FINMA muss die Zuständigkeiten und Verantwortlichkeiten im Zusammenhang mit der Entwicklung, Implementierung, Überwachung und Nutzung von KI klar definieren und Vorgaben für Modelltests, Hilfskontrollen des Systems, Dokumentationsstandards und Schulungen machen. Wenn Steuerpflichtige KI-Lösungen von Drittanbietern erwerben, müssen sie auch feststellen, welche Daten und Methoden verwendet werden und ob insbesondere eine Sorgfaltspflicht seitens des Drittanbieters besteht. Im Falle eines Outsourcings müssen Tests und Kontrollen eingerichtet werden. Darüber hinaus müssen Vertragsklauseln die Zuständigkeiten und Haftungsfragen regeln. Darüber hinaus stellen die Steuerpflichtigen sicher, dass die Drittanbieter über die erforderlichen Kompetenzen und Erfahrungen verfügen. Unserer

Ansicht nach ist Governance ganzheitlich zu betrachten, da sie das Risikomanagement, die internen und externen Kompetenzen, die Zuweisung von Verantwortlichkeiten sowie den rechtlichen und vertraglichen Rahmen umfasst.

Um die Risiken zu inventarisieren und zu klassifizieren, müssen die Steuerpflichtigen feststellen, ob die geplante Anwendung unter ihre Definition von KI fällt. Diese muss ausreichend weit gefasst sein, da das Risikoinventar ansonsten nicht vollständig sein kann. Die Definition eines KI-Systems oder -Modells stellt für die Steuerpflichtigen bereits eine Herausforderung dar, da es im Schweizer Recht keine spezifische Gesetzgebung zur KI gibt. Unserer Ansicht nach kann der KI-VO als Inspirationsquelle dienen (vgl. Caballero Cuevas, [cdbf.ch/1382](https://www.cdbf.ch/1382)). Zweitens müssen die Steuerpflichtigen die Risiken nach ihrer Bedeutung, ihrer Spezifität und der Wahrscheinlichkeit des Eintretens der identifizierten Risiken klassifizieren. Hier sei daran erinnert, dass auch die KI-VO diesen risikobasierten Ansatz verfolgt (vgl. Caballero Cuevas, [cdbf.ch/1390](https://www.cdbf.ch/1390)). Darüber hinaus sollten die Verpflichteten systematische Kriterien festlegen, anhand derer sie wichtige KI-Anwendungen identifizieren können, die besonderer Aufmerksamkeit bedürfen.

Die Qualität der Ergebnisse von KI-Anwendungen hängt in hohem Maße von der Qualität der Daten ab. Je nachdem, welche Daten in den verschiedenen Phasen verwendet werden, können die Ergebnisse fehlerhaft, inkonsistent, unvollständig, nicht repräsentativ, veraltet oder verzerrt sein. Die Steuerpflichtigen müssen daher in ihren internen Richtlinien und Anweisungen Vorgaben machen, um die Vollständigkeit, Korrektheit und Integrität der Daten zu gewährleisten und sicherzustellen, dass die Daten verfügbar und zugänglich sind. Diese Erwartung erscheint uns jedoch hoch, wenn die Beaufsichtigten KI-Systeme oder -Modelle von Drittanbietern verwenden. Im Übrigen räumt die FINMA ein, dass die Beaufsichtigten oftmals keinen Einfluss auf die zugrunde liegenden Daten haben oder diese gar nicht kennen. Um die Compliance zu gewährleisten, sollten die Beaufsichtigten unserer Ansicht nach Vertragsklauseln vorsehen, die es ihnen ermöglichen, dem Anbieter Fälle zu melden, in denen die Datenqualität beeinträchtigt ist, und eine Korrektur der zugrunde liegenden Daten sicherstellen. Unserer Ansicht nach entbindet diese Schwierigkeit die Steuerpflichtigen nicht von ihrer Verantwortung, die Qualität der Eingabedaten zu gewährleisten, weshalb es wichtig ist, interne Richtlinien zur Data Governance und zur Verwendung von Daten in KI-Systemen vorzusehen.

Um sicherzustellen, dass das KI-System oder -Modell ordnungsgemäß funktioniert, sind regelmäßige Tests sowie eine kontinuierliche Überwachung von entscheidender Bedeutung. Die FINMA beurteilt, ob die Beaufsichtigten regelmässige Prüfungen der Genauigkeit, Robustheit und Stabilität des KI-Systems oder -Modells vorsehen. Diese Tests helfen zu überprüfen, ob die Anwendung nicht verzerrt ist. Die FINMA erwartet, dass Leistungsindikatoren verwendet werden, um zu beurteilen, inwieweit das System die gesetzten Ziele erreicht. Die Beaufsichtigten stellen zudem sicher, dass Änderungen der Eingabedaten das der KI-Anwendung zugrunde liegende KI-Modell nicht beeinträchtigen. Darüber hinaus sollten die Steuerpflichtigen Fälle analysieren, in denen Ergebnisse von den Nutzern ignoriert oder verändert wurden, da diese Situationen auf eine Schwäche des Systems oder des KI-Modells hindeuten können. Daher müssen sie eine Überwachung der KI-Anwendungen während ihrer gesamten Nutzungsdauer einrichten.

Die FINMA hebt die Bedeutung der Dokumentation hervor. Die Beaufsichtigten sollten über eine detaillierte und adressatenorientierte Dokumentation verfügen (z. B. Berater, Sekretariat, *Compliance* usw.). Bei wichtigen Anwendungen soll diese Dokumentation auf den Zweck der

Anwendung, die Auswahl und Aufbereitung der Daten, die Wahl des Modells, Leistungsmessungen, Annahmen, Einschränkungen, Tests und Kontrollen sowie Rückfallmöglichkeiten eingehen.

Die Erklärbarkeit der Ergebnisse und ihr Verständnis durch die Mitarbeiter von Banken und Finanzinstituten sind entscheidend für eine kritische Bewertung von KI-Systemen und -Modellen. Dies gilt umso mehr, wenn Ergebnisse gegenüber Investoren, Kunden, Mitarbeitern (vgl. Hirsch, [cdbf.ch/1384](https://cdbf.ch/1384)), der Aufsicht oder der Prüfgesellschaft begründet werden müssen. Die FINMA stellte jedoch fest, dass die Ergebnisse oft nicht verstanden oder erklärt wurden und nicht kritisch beurteilt werden konnten, was ein Problem für die Gewährleistung der Robustheit und Genauigkeit des KI-Systems oder -Modells darstellt.

Zusammenfassend lässt sich sagen, dass die Aufsichtsmitteilung 08/2024 uns über die Erwartungen der FINMA in Bezug auf KI informiert. Es bleiben jedoch zahlreiche Fragen offen, insbesondere in Bezug auf die konkrete Umsetzung dieser Erwartungen durch die Beaufsichtigten. Die FINMA plant zudem, diese weiterzuentwickeln und auf transparente Weise zu kommunizieren. Abgesehen davon müssen Beaufsichtigte, die KI einsetzen möchten, bei der Analyse des regulatorischen Rahmens, der Identifizierung und dem Management von Risiken sowie bei der Schulung ihrer Mitarbeiter proaktiv vorgehen. In diesem Zusammenhang sollten sich die Steuerpflichtigen für Initiativen interessieren, die auf internationaler Ebene ergriffen werden. Ein Beispiel hierfür ist die [Erklärung](#) der ESMA zum Einsatz von KI bei Wertpapierdienstleistungen.

*Die in diesem Kommentar angesprochenen Themen werden in dem für den 21. Januar 2025 geplanten [Webinar über künstliche Intelligenz](#) diskutiert und im Rahmen des [CAS Digital Finance Law](#) weiter vertieft.*

---

Reproduction autorisée avec la référence suivante: Yannick Caballero Cuevas, Erwartungen der FINMA in Bezug auf Governance und Risikomanagement, publié le 19 Dezember 2024 par le Centre de droit bancaire et financier, <https://cdbf.ch/de/1392/>