



Monthly  
Newsletter  
Oct 2024

Bankwesen und  
Finanzen

Schellenberg  
Wittmer



# AI-Regulierung im Finanzsektor

Grégoire Tribolet

## Key Take-aways

- 1.** Die Schweiz hat noch keine KI-spezifischen Regulierungen eingeführt. Finanzinstitute, die KI einsetzen, müssen die allgemeinen rechtlichen Rahmenbedingungen und die aufsichtsrechtlichen Anforderungen der FINMA einhalten.
- 2.** Mit dem EU-KI-Gesetz werden neue Vorschriften für KI-Systeme eingeführt, die nicht nur EU-Institutionen betreffen, sondern auch Schweizer Unternehmen, die KI-Systeme in die EU liefern oder Systeme einsetzen, deren Ergebnisse in der EU verwendet werden.
- 3.** Finanzinstitute und Versicherungsunternehmen müssen KI-Governance-Prozesse einführen und über regulatorische Entwicklungen informiert bleiben, um die Einhaltung der Vorschriften zu gewährleisten.

# 1 Einleitung

Künstliche Intelligenz (**KI**) ist zu einem **wichtigen Innovationsmotor in der Finanzbranche** geworden, wo sie in einer Vielzahl von Anwendungen eingesetzt wird, wie beispielsweise Betrugserkennung, Risikomanagement, Cashflow-Prognosen, Prozessautomatisierung, Kreditrisikoanalyse, Kundenbeziehungsmanagement, Handelsalgorithmen, IT-Entwicklung und Informationsanalyse. Die jüngsten Entwicklungen im Bereich der generativen KI bieten zwar beträchtliche Chancen, bergen aber auch Risiken. Daher verstärken die Finanzaufsichtsbehörden weltweit ihre Aufsicht über KI-Anwendungen, die von Finanzinstituten eingesetzt werden.

Dieser Newsletter gibt einen Überblick über den aktuellen Stand des Schweizer Regulierungsrahmens für Finanzinstitute, die KI-Anwendungen einsetzen, sowie über das EU-KI-Gesetz. Diese EU Regulierung ist relevant für Finanzinstitute, die KI-Systeme an in der EU ansässige Unternehmen liefern oder KI-Systeme einsetzen, deren Ergebnisse in der EU verwendet werden.

## 2 Schweizerischer Rechtsrahmen

Die Schweiz hat noch keine KI-spezifischen Regulierungen verabschiedet. Im Jahr 2020 hat der Bundesrat die [Richtlinien zur Künstlichen Intelligenz für die Eidgenossenschaft](#) in Kraft gesetzt, die nur für die Bundesverwaltung gelten. Für den Privatsektor hat das Staatssekretariat für Bildung, Forschung und Innovation (**SBFI**) im Jahr 2019 einen [Bericht](#) an den Bundesrat veröffentlicht, worin es zum Schluss kommt, dass keine unmittelbare Notwendigkeit für die Einführung einer schweizerischen Gesetzgebung im Bereich der KI besteht.

---

# Schweizer Finanzinstitute müssen die aufsichtsrechtlichen Erwartungen der FINMA erfüllen.

---

Im Jahr 2023 hat der Bundesrat jedoch die wachsende globale Dynamik in Richtung KI-Regulierung erkannt und das Departement für Umwelt, Verkehr, Energie und Kommunikation (**UVEK**) beauftragt, bis Ende 2024 einen Bericht über mögliche Regulierungsansätze zu verfassen. Dieser Bericht wird als Grundlage für einen **möglichen Vorschlag für eine Schweizer KI-Regulierung im Jahr 2025** dienen.

In der Zwischenzeit müssen Schweizer Unternehmen bei der Entwicklung oder dem Einsatz von KI-Anwendungen den **allgemeinen Rechtsrahmen** einhalten wie das Datenschutzgesetz (**DSG**; siehe Ziffer 2.1) und die Persönlichkeitsrechte nach Schweizer Recht, die

einschlägigen Gesetze zum Schutz des geistigen Eigentums, insbesondere das Urheberrechtsgesetz (**URG**), sowie das Gesetz gegen den unlauteren Wettbewerb (**UWG**), im Einklang mit dem prinzipienbasierten und technologieneutralen Ansatz der Schweiz.

Darüber hinaus müssen Schweizer Finanzinstitute, die KI einsetzen, die **aufsichtsrechtlichen Anforderungen der FINMA** erfüllen (siehe Ziffer 2.2) und weitere relevante Vorschriften wie das Bankgeheimnis im Bankengesetz, das FINMA-Rundschreiben 2018/3 (Outsourcing) und das FINMA-Rundschreiben 2023/1 (Operationelle Risiken und Resilienz) einhalten.

### 2.1. Datenschutzgesetz

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (**EDÖB**) hat im November 2023 eine [Stellungnahme](#) publiziert, in der er betont, dass **die schweizerische Datenschutzgesetzgebung direkt auf die KI-gesteuerte Datenbearbeitung anwendbar ist**. Die Stellungnahme erinnert Hersteller, Anbieter und Betreiber von KI-Anwendungen daran, dass sie Transparenz über Zweck, Funktionsweise und Datenquellen der KI-gesteuerten Datenbearbeitung sicherstellen und ein Höchstmass an digitaler Selbstbestimmung der betroffenen Personen gewährleisten müssen.

Die Anforderungen der schweizerischen Datenschutzgesetzgebung gelten für die meisten KI-Anwendungen, die von Finanzinstituten eingesetzt werden. Finanzinstitute müssen insbesondere prüfen, ob eine KI-Anwendung **automatisierte Einzelentscheidungen** im Sinne von Artikel 21 DSG trifft. Diese Prüfung ist insbesondere für KI-Anwendungen relevant, die bei der Kreditwürdigkeitsprüfung, dem digitalen Onboarding, der Kundensegmentierung oder der Filterung von Bewerbungen eingesetzt werden.

Der EDÖB wies zudem darauf hin, dass gewisse KI-Anwendungen **eine Datenschutz-Folgenabschätzung** nach Artikel 22 DSG erfordern. Dies gilt insbesondere in Fällen, in denen (i) grosse Mengen sensibler Personendaten verarbeitet werden, (ii) Personendaten systematisch für die KI-Verarbeitung erhoben werden (ausser für statistische oder nicht-personenbezogene Zwecke) oder (iii) der Output der KI-Anwendung erhebliche Auswirkungen auf die betroffenen Personen hat.

### 2.2. Aufsichtsrechtliche Anforderungen der FINMA

Die FINMA beobachtet die Entwicklung und den Einsatz von KI bereits seit mehreren Jahren. In den Jahren 2021 und 2022 führte sie Erhebungen zum Einsatz von KI im Versicherungs-, Banken- und Vermögensverwaltungssektor durch, erstellte ein Inventar der Bereiche, in denen KI-Anwendungen eingesetzt werden, und richtete eine spezialisierte KI-Dienststelle ein. In ihrem [Risikomonitor 2023](#) hat die FINMA ihre **aufsichtsrechtlichen Anforderungen an Finanzinstitute, die KI einsetzen**, dargelegt und sich dabei auf **vier kritische Bereiche** konzentriert:

- **Governance und Verantwortung:** Die Finanzinstitute müssen die Rollen und Verantwortlichkeiten für KI-bezogene Entscheidungen klar definieren und sicherstellen, dass die Verantwortung bei den menschlichen Akteuren und nicht bei den KI-Systemen selbst liegt. Dies ist besonders wichtig, wenn KI-Fehler unbemerkt bleiben können, wenn Prozesse

zu komplex werden oder wenn es innerhalb des Instituts an Fachwissen mangelt.

- **Robustheit und Verlässlichkeit:** KI-Systeme müssen auf ihre Genauigkeit und Zuverlässigkeit geprüft werden, insbesondere in Anbetracht des Risikos eines "Drifts" bei selbstlernenden Modellen. Diese Systeme sollten strengen Tests unterzogen werden, insbesondere in Bereichen des Risikomanagements. KI-Systeme bergen auch Risiken für die Cybersicherheit, die angegangen werden müssen.
- **Transparenz und Erklärbarkeit:** Die Institute müssen sicherstellen, dass KI-Systeme, insbesondere solche, die sich auf kundenbezogene Ergebnisse auswirken, transparent sind und dass die von diesen Systemen getroffenen Entscheidungen den Benutzern erklärt und von diesen verstanden werden können.
- **Gleichbehandlung:** KI-Systeme, die in Finanzdienstleistungen eingesetzt werden, wie z.B. Kreditscoring, müssen Vorurteile oder diskriminierende Praktiken vermeiden. Die FINMA verlangt von Instituten, ihre KI-Systeme zu überwachen, um jede Form der Ungleichbehandlung zu verhindern.

Diese Anforderungen der FINMA sind vergleichbar mit denjenigen anderer Finanzmarktaufsichtsbehörden. Jüngste Beispiele von Regulierungen ausländischer Behörden sind die [Stellungnahme](#) der Europäischen Wertpapier- und Marktaufsichtsbehörde (**ESMA**), die eine erste Orientierungshilfe für Unternehmen bietet, die KI bei der Erbringung von Wertpapierdienstleistungen für Kleinanleger einsetzen (Mai 2024), der [expert Fachartikel](#) der deutschen Bundesanstalt für Finanzdienstleistungsaufsicht (**BaFIN**) über das Risiko der Diskriminierung beim Einsatz von KI (August 2024) und das [KI-Update](#) der britischen Finanzaufsichtsbehörde (Financial Conduct Authority) (April 2024).

### 3 EU-KI-Gesetz

Das [EU-KI-Gesetz](#) trat am 1. August 2024 in Kraft und stellt die **bisher umfassendste KI-spezifische Regelung** dar. Das Gesetz verfolgt einen risikobasierten Ansatz und kategorisiert KI-Systeme auf der Grundlage ihrer potenziellen Auswirkungen auf Sicherheit und Grundrechte.

#### 3.1 Zeitplan

Die Bestimmungen des EU-KI-Gesetzes werden schrittweise über mehrere Jahre eingeführt. Zu den wichtigsten Umsetzungsfristen gehören:

|                       |   |
|-----------------------|---|
| <b>2 Februar 2025</b> | Verbot von KI-Praktiken mit inakzeptablen Risiken und Anforderungen an die KI-Kompetenz   |
| <b>2 August 2025</b>  | Universell einsetzbare KI-Modelle und Bestimmungen über Sanktionen der Mitgliedstaaten  |
| <b>2 August 2026</b>  | Die meisten Vorschriften des Gesetzes, einschliesslich derjenigen über KI-Systeme mit hohem Risiko und die Transparenzbestimmungen, werden in Kraft treten. |
| <b>2 August 2027</b>  | KI mit hohem Risiko im Rahmen spezifischer sektoraler Rechtsvorschriften; Universell einsetzbare KI-Modelle bereits auf dem Markt                           |

Diese Übergangsfristen geben den Unternehmen Zeit, die verschiedenen Bestimmungen des Gesetzes zu erfüllen, obwohl eine frühzeitige Planung von entscheidender Bedeutung ist, insbesondere für Unternehmen, die mit risikoreichen KI-Systemen arbeiten.

#### 3.2 Territorialer Geltungsbereich

Der **territoriale Geltungsbereich des EU-KI-Gesetzes ist ausserordentlich weit gefasst** und gilt für:

- Anbieter von KI-Systemen, die in der EU in Betrieb genommen oder auf den Markt gebracht werden;
- in der EU niedergelassene Anbieter von KI-Systemen; und
- Anbieter oder Betreiber von KI-Systemen, deren Ergebnisse in der EU verwendet werden.

---

## Das EU-KI-Gesetz wirkt sich sowohl auf EU- als auch auf Nicht-EU-KI-Anbieter und -Bereitsteller aus.

---

**Schweizer Finanzinstitute**, die KI-Systeme entwickeln oder einsetzen, können daher **dem EU-KI-Gesetz unterliegen**, selbst wenn sie keine physische Präsenz in der EU haben, insbesondere wenn sie (i) KI-Systeme entwickeln und sie an in der EU ansässige Unternehmen liefern oder (ii) KI-Systeme einsetzen, deren Ergebnisse in der EU genutzt werden (z. B. von Kunden mit Wohnsitz in der EU).

Während die EU Datenschutz-Grundverordnung für Einrichtungen ausserhalb der EU gilt, wenn ihre Tätigkeiten zumindest teilweise auf die EU ausgerichtet sind, ist **unklar**, ob das EU-KI-Gesetz in Fällen gilt, in denen der ausserhalb der EU niedergelassene Anbieter oder Bereitsteller **keinen Versuch unternommen hat, auf den EU-Markt abzielen**. In Erwägungsgrund 11 heisst es, dass ein Anbieter oder Bereitsteller ausserhalb der EU dem Gesetz unterliegt, wenn der Output des KI-Systems für die Verwendung in der EU bestimmt ist. Artikel 2 Absatz 1 Buchstabe c des KI-Gesetzes enthält jedoch nicht das Element der Absicht und besagt stattdessen, dass ein Anbieter oder Bereitsteller dem Gesetz unterliegt, wenn die Ergebnisse seiner KI-Systeme in der EU verwendet werden.

Es ist auch ungewiss, wie der **Begriff "Output"** interpretiert werden wird, aber das Gesetz nennt als Beispiele "Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen". So können beispielsweise von einem KI-System generierte Anlageempfehlungen, die ein Schweizer Finanzinstitut an Kunden in der EU richtet, die Anwendbarkeit des EU-KI-Gesetzes auslösen.

Wenn der Anbieter eines Hochrisiko-KI-Systems in einem Drittland ansässig ist, muss er ausserdem einen **bevollmächtigten Vertreter** in der EU benennen.

### 3.3 Risikobasierte Einstufung von KI-Systemen

Das EU-KI-Gesetz kategorisiert KI-Systeme in vier

#### Hauptrisikostufen:

- **Verbotene KI-Systeme:** Dazu gehören KI-Systeme, die unannehmbare Risiken darstellen, wie die Manipulation von Personen durch unterschwellige Techniken, die Ausnutzung von Schwachstellen (z.B. Alter oder Behinderung) oder die Schaffung von sozialen Bewertungssystemen, die aufgrund des persönlichen Verhaltens diskriminieren. Solche KI-Systeme sind nach dem EU-KI-Gesetz bis auf sehr begrenzte Ausnahmen verboten.
- **Hochriskante KI-Systeme:** Diese KI-Systeme unterliegen strengen Vorschriften. Für Finanzinstitute können die folgenden hochriskanten KI-Systeme besonders relevant sein:
  - KI-Systeme, die zur Bewertung der Kreditwürdigkeit natürlicher Personen oder für das Kredit-Scoring eingesetzt werden (ausser zur Aufdeckung von Finanzbetrug);
  - KI-Systeme für die Risikobewertung und Preisgestaltung in der Lebens- und Krankenversicherung;
  - KI-Systeme, die für die Rekrutierung oder Auswahl von Personen eingesetzt werden, einschliesslich der Schaltung gezielter Stellenanzeigen, der Analyse und Filterung von Bewerbungen und der Bewertung von Kandidaten.
- **AI-Systeme mit begrenztem Risiko:** Für diese Systeme gelten Transparenzanforderungen. So müssen beispielsweise KI-Systeme, die direkt mit Verbrauchern interagieren (z. B. Chatbots), die Nutzer darüber informieren, dass sie mit KI interagieren. Ebenso müssen KI-generierte Inhalte (z.B. synthetische Medien oder Deep Fakes) als solche gekennzeichnet werden, um Täuschungen zu verhindern.
- **KI-Systeme mit minimalem Risiko:** Für diese Systeme gibt es keine zwingenden rechtlichen Anforderungen, aber die Unternehmen werden ermutigt, Verhaltenskodizes zu verabschieden, um die ethische Nutzung von KI zu fördern.

### 3.4 Besondere Anforderungen an KI-Systeme mit hohem Risiko

Anbieter und Betreiber von KI-Systemen mit hohem Risiko müssen umfangreiche Anforderungen erfüllen, darunter:

- **Risikomanagement:** Es sind umfassende Risikomanagementsysteme einzuführen, um potenziellen Risiken während des gesamten Lebenszyklus des KI-Systems zu begegnen. Diese Systeme müssen vorhersehbare Risiken für die Gesundheit, die Sicherheit und die Grundrechte ermitteln und sicherstellen, dass geeignete Abhilfemassnahmen ergriffen werden.
- **Datenverwaltung:** Das EU-KI-Gesetz verlangt, dass die Trainings-, Validierungs- und Testdatensätze für KI-Systeme mit hohem Risiko repräsentativ, relevant und fehlerfrei sind. Besonderes Augenmerk muss auf die Vermeidung von Verzerrungen in Datensätzen gelegt werden, insbesondere bei Systemen, die Grundrechte betreffen, wie z.B. solche, die für Anstellungen oder Kreditwürdigkeitsprüfungen verwendet werden.

- **Transparenz und menschliche Aufsicht:** KI-Systeme mit hohem Risiko müssen so konzipiert sein, dass eine wirksame menschliche Aufsicht möglich ist, und es müssen Mechanismen vorhanden sein, um den Betrieb bei Bedarf zu stoppen. Menschliche Bediener müssen in der Lage sein, die Ergebnisse des Systems zu interpretieren, seine Grenzen zu verstehen und KI-Entscheidungen bei Bedarf ausser Kraft zu setzen.
- **Konformitätsbeurteilungen:** Bevor ein KI-System mit hohem Risiko auf den Markt gebracht wird, müssen die Anbieter eine Konformitätsbewertung durchführen, um sicherzustellen, dass das System den gesetzlichen Normen entspricht. Je nach System kann eine Bewertung durch Dritte erforderlich sein.

Das EU-KI-Gesetz zielt darauf ab, mögliche Überschneidungen zwischen einigen seiner Anforderungen und solchen, die Finanzdienstleistungsunternehmen durch das bestehende EU-Finanzdienstleistungsrecht auferlegt werden, zu vermeiden. Infolgedessen gelten für Finanzdienstleister, die KI-Systeme mit hohem Risiko anbieten oder einsetzen, in bestimmten Bereichen begrenzte Ausnahmeregelungen.

---

## Für KI-Systeme mit hohem Risiko gelten nach dem EU-KI-Gesetz strenge Anforderungen.

---

### 3.5 Mechanismen zur Einhaltung und Durchsetzung der Vorschriften

Mit dem EU-KI-Gesetz wird eine **mehrstufige Aufsichts- und Durchsetzungsstruktur** geschaffen. Auf EU-Ebene wird der Europäische Ausschuss für künstliche Intelligenz die Umsetzung des Gesetzes überwachen, während jeder Mitgliedstaat nationale Behörden zur Durchsetzung des Gesetzes in seinem Zuständigkeitsbereich benennen muss. Diese Behörden werden befugt sein, den Markt zu überwachen, Verstösse zu untersuchen und Sanktionen zu verhängen. Für den Finanzsektor wird erwartet, dass die für die Beaufsichtigung der Finanzinstitute nach den Finanzmarktgesetzen zuständigen Behörden auch die Einhaltung des EU-KI-Gesetzes überwachen.

Die Nichteinhaltung des EU-KI-Gesetzes kann **erhebliche Strafen** nach sich ziehen. Unternehmen, die verbotene KI-Praktiken anwenden, können mit Geldbussen von bis zu 35 Mio. EUR oder 7 % des gesamten weltweiten Jahresumsatzes belegt werden, je nachdem, welcher Betrag höher ist. Bei Verstössen im Zusammenhang mit hochriskanten und bestimmten anderen KI-Systemen können die Geldbussen bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes betragen.

## 4 Fazit

Die Schweiz hat zwar noch keinen umfassenden KI-spezifischen Rechtsrahmen eingeführt, aber die Finanzinstitute müssen sich an der bestehenden allgemeinen Rechtslandschaft orientieren, insbesondere in Bereichen wie Persönlichkeitsrechte und Datenschutz, und die aufsichtsrechtlichen Anforderungen der FINMA erfüllen. Diese Verpflichtungen sind prinzipienbasiert und betreffen in erster Linie Transparenz und Rechenschaftspflicht beim Einsatz von KI. Sie sind auch für andere Sektoren, wie z.B. Versicherungsunternehmen, relevant. Im Gegensatz dazu legt das EU-KI-Gesetz einen detaillierteren und weiterreichenden Regulierungsrahmen fest, der nicht nur für in der EU ansässige Unternehmen gilt, sondern auch für Anbieter oder Betreiber von KI-Systemen aus Drittländern, deren Ergebnisse in der EU genutzt werden – was sich auch auf Schweizer Finanzinstitute und Versicherungsunternehmen auswirken kann. Um konform zu bleiben, sollten sie in dem Masse, in dem sie KI nutzen, bereits mit der Einführung eines KI-Governance-Rahmens beginnen und sich über zukünftige regulatorische Entwicklungen informieren.



**Grégoire Tribolet**  
Partner  
[gregoire.tribolet@swlegal.ch](mailto:gregoire.tribolet@swlegal.ch)



**Stéphanie Chuffart-Finsterwald**  
Partner  
[stephanie.chuffart@swlegal.ch](mailto:stephanie.chuffart@swlegal.ch)



**Roland Mathys**  
Partner  
[roland.mathys@swlegal.ch](mailto:roland.mathys@swlegal.ch)



**Olivier Favre**  
Partner  
[olivier.favre@swlegal.ch](mailto:olivier.favre@swlegal.ch)

The content of this Newsletter does not constitute legal or tax advice and may not be relied upon as such. Should you seek advice with regard to your specific circumstances, please contact your Schellenberg Wittmer liaison or one of the persons mentioned above.

Schellenberg Wittmer Ltd is your leading Swiss business law firm with more than 150 lawyers in Zurich and Geneva, and an office in Singapore. We take care of all your legal needs – transactions, advisory, disputes.



Schellenberg Wittmer Ltd



Schellenberg Wittmer Ltd



**Schellenberg Wittmer Ltd**  
Attorneys at Law

**Zurich**  
Löwenstrasse 19  
P.O. Box 2201  
8021 Zurich / Switzerland  
T +41 44 215 5252  
[www.swlegal.com](http://www.swlegal.com)

**Geneva**  
15bis, rue des Alpes  
P.O. Box 2088  
1211 Geneva 1 / Switzerland  
T +41 22 707 8000  
[www.swlegal.com](http://www.swlegal.com)

**Singapore**  
Schellenberg Wittmer Pte Ltd  
6 Battery Road, #37-02  
Singapore 049909  
T +65 6580 2240  
[www.swlegal.sg](http://www.swlegal.sg)