

Künstliche Intelligenz im Finanzsektor: Wann braucht ein Institut eine interne KI-Weisung?



Von Dr. Fabian Schmid

Leiter Regulatory & Compliance FS
Grant Thornton Advisory AG, Zürich

Wann braucht ein Finanzinstitut eine interne KI-Weisung?

Am 10. Februar 2026 diskutierten hohe Vertreter von Politik und Wirtschaft letztmals über den zukünftigen Rechtsrahmen der Künstlichen Intelligenz (KI) in der Schweiz. Bundesrat Rösli betonte am «Beiratstreffen Digitale Schweiz», dass es für das Vertrauen der Bevölkerung in KI zentral sei, dass diese Transparenz und Nachvollziehbarkeit gewährleistet. Gleichzeitig müssten alle Akteure Raum zur Entfaltung haben und innovativ tätig sein können. Der Schutz der Grundrechte dürfe aber dabei nicht beeinträchtigt werden. KI hat bekanntlich auch in der Schweizer Finanzbranche längst den Alltag erobert. Anwendungen finden sich heute entlang der gesamten Wertschöpfungskette: von der Kundeninteraktion über Kredit- und Risikoanalysen bis hin zu Betrugsbekämpfung, Marktüberwachung oder internen Sup-

port-Funktionen. KI-Werkzeuge werden von Mitarbeitenden zunehmend selbstverständlich genutzt.

Demgegenüber entwickelt sich der regulatorische Rahmen in der Schweiz vergleichsweise zurückhaltend. In den letzten zwölf Monaten hat sich an der formellen Rechtslage wenig geändert. Die Schweiz kennt – anders als die EU – weiterhin kein spezifisches KI-Gesetz, es existieren bislang weder ein konkreter Gesetzesentwurf noch eine formelle Vernehmlassung. Für Finanzinstitute bleiben damit vor allem die bestehenden finanzmarktrechtlichen Vorgaben sowie die Erwartungen der Finma in den Bereichen Riskmanagement und Organisation massgeblich. Diese Ausgangslage wirft eine zentrale praktische Frage auf: Wann ist der Erlass einer internen KI-Weisung angezeigt – und wann genügt es, bestehende Regelwerke anzuwenden?

Der vorliegende Beitrag beleuchtet diese Frage aus einer praxisorientierten Perspektive und ordnet ein, welche Überlegungen Schweizer Finanzinstitute bei der Steuerung von KI-Risiken und bei der Ausgestaltung ihres internen Weisungswesens anstellen sollten.

Regulatorischer Kontext: Schweiz und internationale Entwicklungen

Die Schweiz verfolgt im Bereich der KI-Regulierung bislang bewusst einen technologieneutralen Ansatz. KI soll grundsätzlich innerhalb des bestehenden Rechtsrahmens adressiert werden, insbesondere über Organisations-, Sorgfalts-, Datenschutz- und aufsichtsrechtliche Pflichten. Für den Finanzsektor bedeutet dies, dass sich der Einsatz von KI weiterhin an den allgemeinen Anforderungen des Finanzmarktrechts, des revidierten Datenschutzgesetzes und der kodifizierten Praxis der Finma messen lassen muss. Hervorzuheben ist dabei die Finma-Aufsichtsmitteilung 8/2024, in welcher die spezifischen Er-

wartungen an die Finanzinstitute beim Einsatz von KI formuliert werden.

Auf politischer Ebene zeichnet sich allerdings mittelfristig eine gewisse Bewegung ab. Die Schweiz hat die KI-Konvention des Europarates unterzeichnet. Deren Ratifizierung gilt als wichtiger Zwischenschritt für eine kohärente gesetzliche Regelung auf Bundesebene. Auf dieser Grundlage dürfte voraussichtlich Ende 2026 ein Gesetzesentwurf in die Vernehmlassung gehen. Der zeitliche Horizont bis zum Inkrafttreten bleibt jedoch offen, und kurzfristig ist nicht mit verbindlichen neuen KI-Spezialnormen zu rechnen.

Anders stellt sich die Situation in der Europäischen Union dar. Mit dem EU AI Act wurde ein umfassender, risikobasierter Regulierungsrahmen geschaffen, der den Einsatz von KI je nach Risikokategorie mit teils weitreichenden Pflichten verbindet. Auch wenn dieser Rechtsakt für Schweizer Finanzinstitute grundsätzlich nicht direkt anwendbar ist, entfaltet er faktische Wirkung, etwa bei grenzüberschreitenden Tätigkeiten, bei EU-Kunden oder bei der Nutzung von in der EU ansässigen KI-Anbietern. In der politischen Diskussion wird dabei zunehmend kritisch angemerkt, dass Europa zwar regulatorisch eine Vorreiterrolle einnimmt, während die technologische Führungsposition im KI-Bereich aber nach wie vor (oder vielleicht gerade deshalb) primär in den USA und in China liege. Für Schweizer Institute bedeutet dies, dass sie sich in einem Spannungsfeld zwischen Innovationsdruck und wachsender regulatorischer Erwartungshaltung bewegen.

Pflicht zur Risikoanalyse – auch ohne KI-Spezialgesetz

Unabhängig von der Frage künftiger Gesetzgebung sind regulierte Finanzinstitute bereits heute verpflichtet, die Risiken im Zusammenhang mit dem

Einsatz von KI systematisch zu identifizieren, zu analysieren und geeignete Massnahmen zu implementieren. Der Einsatz von KI ist dabei nicht isoliert zu betrachten, sondern unter Berücksichtigung des Geschäftsmodells und der Grösse des Instituts als Teil der Gesamtorganisation und der bestehenden Kontrolllandschaft.

In der Praxis bedeutet dies, dass sich Institute ein klares Bild davon verschaffen müssen, wo und in welcher Form KI bei ihnen eingesetzt wird – sei es produktiv, unterstützend oder experimentell. Ebenso relevant ist, ob KI-Systeme Entscheidungen lediglich vorbereiten oder ob sie faktisch zu einer (teil) automatisierten Entscheidungsfindung führen. Hinzu kommen Fragen zur Art der verarbeiteten Daten, zu möglichen Abhängigkeiten von externen Anbietern sowie zur Nachvollziehbarkeit der Ergebnisse. Erst auf dieser Grundlage lässt sich sachgerecht beurteilen, ob und welche internen Regelungen erforderlich sind. Eine KI-Weisung «um der Weisung willen» schafft demgegenüber wenig Mehrwert.

Typische KI-Risiken für Finanzinstitute

Die konkreten Risiken sind stark vom Einzelfall abhängig. Gleichwohl zeigen sich in der Praxis wiederkehrende Risikokategorien, die für Finanzinstitute besonders relevant sind. Dazu zählen zunächst Governance- und Organisationsrisiken, etwa wenn Zuständigkeiten unklar sind oder Kontroll- und Eskalationsmechanismen fehlen. Von besonderer Bedeutung sind zudem Datenschutz- und Persönlichkeitsrisiken, namentlich bei automatisierten Einzelentscheidungen oder bei der Verarbeitung sensibler Personendaten. Verwandt, aber nicht deckungsgleich sind KI-bezogene Risiken im Bereich der Vertraulichkeit, namentlich das Risiko, dass Mitarbeitende bei unsachgemässer Nutzung von KI-Tools Geschäftsgeheimnisse verletzen. Hinzu kommen Outsourcing- und Drittparteirisiken beim Einsatz externer KI-Lösungen, etwa cloudbasierter Modelle, die erhöhte Anforderungen an Vertragsgestaltung und Überwachung stellen. Schliesslich sind auch Reputations- und Haftungsrisiken nicht zu unterschätzen: Intransparente oder als

unfair wahrgenommene KI-Entscheidungen können das Vertrauen von Kunden und Öffentlichkeit nachhaltig beeinträchtigen.

Wann stellt sich die Frage einer internen KI-Weisung?

Vor diesem Hintergrund stellt sich die Frage, ab welchem Punkt eine formalisierte interne KI-Weisung sinnvoll oder notwendig ist. In der Praxis zeigt sich, dass insbesondere grössere Banken und Versicherungen die KI-Thematik längst in ihrem Weisungs- und Kontrollsystem abgebildet haben, sei es in Form eigenständiger KI-Richtlinien oder als integraler Bestandteil bestehender IT-, Risiko- oder Outsourcing-Weisungen. Zunehmend befassen sich jedoch auch kleine und mittlere Finanzinstitute wie Fondsleitungen, Vermögensverwalter und übrige Finanzintermediäre mit diesem Schritt.

Ein erhöhter interner Regelungsbedarf besteht insbesondere dann, wenn KI in regulierten Kernprozessen eingesetzt wird, wenn Entscheidungen mit rechtlichen oder faktischen Auswirkungen für Kunden automatisiert oder vorselektiert werden, wenn KI-Tools institutsweit oder durch eine Vielzahl von Mitarbeitenden genutzt werden oder wenn externe, insbesondere generative KI-Systeme zum Einsatz kommen. Je näher KI an entscheidungsrelevante Prozesse heranrückt, desto weniger genügt eine rein informelle Steuerung.

Inhalt und Ausgestaltung einer internen KI-Weisung

Eine interne KI-Weisung muss weder hochkomplex noch technisch überladen sein. Entscheidend ist, dass sie die wesentlichen Risiken adressiert und sinnvoll in die bestehende Governance eingebettet ist. Idealerweise regelt sie, welche KI-Anwendungen erfasst sind, wie Zuständigkeiten und Verantwortlichkeiten verteilt werden und nach welchen Kriterien KI-Systeme risikobasiert eingestuft werden. Ebenfalls relevant sind Verhaltensregeln im Umgang mit KI-Tools, Vorgaben zum Einsatz externer Lösungen, zur Transparenz und Dokumentation von KI-gestützten Entscheidungen sowie zur Schulung und Sensibilisierung der Mitarbeitenden.

Wesentlich ist, dass Umfang und Detaillierungsgrad der Weisung zur Grösse, Komplexität und Risikolage des Instituts passen. Eine schlanke, klar verständliche Regelung ist in der Praxis oft wirksamer als ein umfangreiches, aber kaum gelebtes Dokument.

Umsetzung in der Praxis

In der Umsetzung hat sich ein schrittweiser Ansatz bewährt. Ausgangspunkt bildet eine strukturierte Erhebung der bestehenden und geplanten KI-Nutzung. Darauf aufbauend können bestehende Weisungen gezielt ergänzt oder – wo sachgerecht – eine eigenständige KI-Weisung eingeführt werden. Entscheidend ist weniger die formale Existenz eines Dokuments als dessen tatsächliche Anwendung im Alltag. Regelmässige Überprüfungen, Anpassungen an neue Anwendungsfälle sowie die enge Zusammenarbeit zwischen den Fachbereichen, IT, Risk, Compliance und Datenschutz sind zentrale Erfolgsfaktoren. Selbstverständlich ist allein mit dem Erlass einer Weisung noch kein Mehrwert geschaffen. Die Mitarbeitenden müssen angemessen darüber informiert, instruiert und regelmässig geschult werden, und die wichtigsten Elemente der Weisung müssen im Rahmen des IKS kontrolliert und überwacht werden.

Fazit

Auch ohne spezifisches KI-Gesetz stehen Schweizer Finanzinstitute heute in der Verantwortung, ihren Einsatz von KI angemessen zu steuern. Eine interne KI-Weisung sollte dabei kein Selbstzweck sein, sondern ein vom Management bewusst ausgerolltes Instrument zur strukturierten Risikoüberwachung. Ob und wann eine separate Weisung erforderlich ist, hängt von der Grösse des Instituts, der Komplexität des Geschäftsmodells, vom konkreten Einsatz der KI und vom damit verbundenen Risikoprofil ab. Institute, die ihre KI-Nutzung frühzeitig analysieren und pragmatisch regeln, schaffen nicht regulatorische Sicherheit, sondern stärken auch das Vertrauen von Geschäftspartnern, Prüfern, Aufsichtsbehörden, Kunden und Mitarbeitenden.

fabian.schmid@ch.gt.com
www.grantthornton.ch