

KI-FLASH

KI-Governance im Verwaltungsrat

Was ein CEO und Verwaltungsrat über den AI Act, Data Act und die Schweizer KI-Aufsichtspraxis ungefähr wissen sollten

2026 · KI-FLASH · CA. 8 MIN. LESEZEIT · DR. IUR. DIRK SPACEK

1. Ausgangslage

KI-Regulierung ist längst nicht mehr nur ein EU-Thema für IT- und Compliance-Abteilungen. Sie ist zu einem Führungs- und Governance-Thema geworden, das auch Schweizer Unternehmen und insbesondere Finanzinstitute unmittelbar betrifft – sei es, weil sie im EU-Markt tätig sind, sei es, weil die FINMA ihre eigenen Erwartungen an KI-Governance systematisch schärft. Dieser Beitrag ordnet die regulatorischen Compliance-Rahmenbedingungen kurz zusammengefasst ein und zeigt, was ein CEO und Verwaltungsrat konkret in diesen Belangen vornehmen sollten.

2. Der europäische Regulierungsblock

Die EU regelt den Umgang mit KI nicht in einem einzigen Gesetz. Es sind mehrere Erlasse, die aufeinander aufbauen wie Bauteile eines Stapels – daher der oft gehörte Begriff «Regulierungsstack». Für Unternehmen sind aktuell vor allem zwei Erlasse zentral: Der EU AI Act (er regelt den Umgang mit KI-Systemen selbst) und der EU Data Act (er regelt den Zugang zu Daten, mit denen diese Systeme arbeiten). Beide ergänzen sich – und beide werden in der Praxis oft unterschätzt, weil man primär immer nur vom EU AI Act spricht.

AI Act	Data Act
<div>Verordnung (EU) 2024/1689, in Kraft seit 1. August 2024</div> <ul style="list-style-type: none">Regelt KI-Systeme selbst: je höher das Risiko für Menschen, desto strenger die Pflichten in diesem Gesetz.Risikobasierter Ansatz: Drei Risikostufen: 1. Inakzeptabel (z.B. Social Scoring) d.h. verboten, 2. hoch (z.B. biometrische Identifizierung), d.h. Pflichten zu begleitenden Massnahmen wie Konformitätsbewertungen, Risikomanagementsystem, Dokumentation und Transparenz), 3. mini-mal oder ohne Risiko.Pflichten aus dem AI-Act gelten gestaffelt und treten schrittweise bis 2028 vollständig in Kraft.	<div>Verordnung (EU) 2023/2854, anwendbar seit 12. September 2025</div> <ul style="list-style-type: none">Regelt nicht KI, sondern den Zugang zu Daten – v. a. aus vernetzten Geräten (IoT) und digitalen Diensten.Nutzer erhalten Anspruch auf «ihre» Maschinendaten und dürfen sie an Dritte weitergeben.Verbietet einseitige, unfaire Datenklauseln in B2B-Verträgen und erleichtert den Anbieterwechsel.

Der AI Act tritt in Etappen in Kraft

Für die Praxis wichtig: Der AI Act gilt nicht auf einen Schlag, sondern **schrittweise**. Der jüngste «**Digital Omnibus**» der EU – ein umfassendes Gesetzgebungspaket, das europäische Digitalrecht zu vereinfachen und gebündelt zu harmonisieren (AI Act, Data Act und DSGVO) um Hürden und Überschneidungen abzubauen hat die strengsten Pflichten aus dem AI Act zeitlich nach hinten verschoben – inhaltlich aber nicht abgeschwächt.

- Februar 2025 – Verbotene KI-Praktiken und Pflicht zur KI-Kompetenz der Mitarbeitenden (Art. 4) treten in Kraft.
- August 2025 – Governance-Regeln und Pflichten für General-Purpose-KI-Modelle (z. B. grosse Sprachmodelle) treten in Kraft.
- August 2026 – Transparenzpflichten (Art. 50) treten in Kraft: Chatbots, Deepfakes und KI-generierte Inhalte müssen gekennzeichnet werden.
- Dezember 2027 / August 2028 – Volle Pflichten für Hochrisiko-KI treten in Kraft (Risikomanagement, Dokumentation, menschliche Aufsicht) – diese wurden neu terminiert durch den Digital Omnibus.

Wie spielen AI Act und Data Act zusammen?

Kurz gesagt: Der AI Act verlangt von Unternehmen, die Qualität und Herkunft ihrer KI-Trainings- und Betriebsdaten sicherzustellen und nachzuweisen. Der Data Act liefert dafür die Grundlage, indem er regelt, wer überhaupt Zugriff auf Daten kriegt und wie sie fair weitergegeben werden dürfen. Wer nur den AI Act im Blick hat, übersieht deshalb oft die Datenzugangs- und Vertragspflichten, die im Hintergrund ebenfalls erfüllt sein müssen. Ergänzt wird dieser «Stack» durch noch weitere EU-Erlasse zur Datenwirtschaft (u. a. der EU Data Governance Act, der Digital Markets/Services Act) sowie durch die DSGVO, die bei personenbezogenen Daten weiterhin Vorrang hat.

3. Weshalb betrifft das die Schweiz?

Extraterritoriale Wirkung

Weder der EU AI Act noch der EU Data Act sind in der Schweiz anwendbar – die Schweiz ist nicht in der EU. Sie hat auch kein eigenes „KI-Gesetz“. Beide Erlasse wirken jedoch **faktisch extraterritorial**: Der AI Act erfasst Schweizer Unternehmen, sobald sie KI-Systeme auf dem EU-Markt in Verkehr bringen, in der EU bereitstellen oder wenn der **Output** eines von der Schweiz aus betriebenen KI-Systems in der EU verwendet wird. Der Data Act erfasst analog Schweizer Hersteller vernetzter Produkte oder digitaler Dienste, die für den EU-Markt bestimmt sind oder EU-Nutzer betreffen. Für grenzüberschreitend tätige Schweizer Unternehmen – gerade auch Finanzinstitute mit EU-Kundschaft, EU-Niederlassungen oder EU-Cloud-Infrastruktur – ist der EU-«Stack» daher durchaus praxisrelevant.

Der Schweizer Weg: sektoriell statt horizontal

Der Bundesrat hat sich am 12. Februar 2025 gegen einen vergleichbaren AI-Act und für einen **sektoriellen Regulierungsansatz** ausgesprochen (d.h. man prüft, ob sektorspezifische

Erlasse/Gesetzesanpassungen nötig sein könnten). Die Schweiz soll die **KI-Konvention des Europarats** (im März 2025 unterzeichnet) ratifizieren und punktuell in bestehendes Recht überführen, ergänzt durch nicht verbindliche Massnahmen (Selbstregulierung, Branchenleitfäden, Ethikkodizes). Vorsicht: Der Europarat ist eine eigene internationale Organisation, nicht die EU. Auch Nicht-EU-Länder sind Mitglied. Das federführende EJPD erarbeitet derzeit zusammen mit UVEK und EDA bis Ende 2026 eine Vernehmlassungsvorlage zu den Themen Transparenz, Datenschutz, Nichtdiskriminierung und Aufsicht bei KI. Ein **horizontales KI-Gesetz nach EU-Vorbild ist aber auf absehbare Zeit nicht zu erwarten** – wohl aber punktuelle Anpassungen in einzelnen Rechtsgebieten und Sektoren.

FINMA und andere Aufsichtsbehörden werden konkreter

Im Finanzsektor hat die FINMA mit der **Aufsichtsmitteilung 08/2024** (Dezember 2024) ihre Erwartungen an Governance und Risikomanagement beim Einsatz von KI formuliert – technologieneutral, nach dem Grundsatz „same business, same risks, same rules“. Verlangt werden insbesondere eine zentrale Inventarisierung der KI-Anwendungen, klar definierte Zuständigkeiten, Dokumentation, Tests, laufendes Monitoring und Schulungen; als Hauptrisiken nennt die FINMA operationelle Risiken (Modellrisiken wie Bias oder mangelnde Erklärbarkeit), Datenrisiken, IT-/Cyberrisiken sowie eine wachsende Drittparteiabhängigkeit. Eine FINMA-Umfrage von Anfang 2025 zeigt, dass rund die Hälfte der beaufsichtigten Institute KI bereits einsetzt und ein weiteres Viertel dies in den kommenden drei Jahren plant. In der Folge hat die FINMA das Thema in weiteren Aufsichtsmitteilungen vertieft – etwa zu digitalen Betrugsrisiken und Deepfakes (Mitteilung 02/2026) sowie zu den durch Quantencomputing beschleunigten Cyberrisiken (Mitteilung 05/2026) – ein klares Signal, dass KI-Governance aus Sicht der Aufsicht Chefsache ist und bleiben soll.

4. Was sollte ein CEO und Verwaltungsrat jetzt konkret tun und umsetzen?

Unabhängig davon, ob der EU AI Act formal anwendbar ist: Er setzt im Europäischen Raum faktisch den Marktstandard für «gute» KI-Governance, an dem sich auch FINMA-Erwartungen orientieren. Für Verwaltungsrat und Geschäftsleitung – besonders bei Finanzinstituten – empfiehlt sich allgemein folgendes Vorgehen:

Governance & Verantwortlichkeiten

- **KI-Inventar** führen: alle eingesetzten, eingekauften und in Entwicklung befindlichen Systeme erfassen, inkl. Rolle (Anbieter/Betreiber), Zweck und verarbeiteter Daten.
- **Klare Zuständigkeiten** festlegen (VR-Verantwortlicher für KI-Governance, KI-Verantwortliche/r bzw. KI-Ausschuss auf Geschäftsleitungsebene) mit regelmässigem Reporting an den Verwaltungsrat.
- **Risikoklassifizierung pro Anwendungsfall** – orientiert an der AI-Act-Logik – als Grundlage für den Umfang der nötigen internen Kontrollen.

Schatten-KI («Shadow AI») erkennen und eindämmen

Ein Punkt, der in vielen Governance-Konzepten fehlt: KI-Einführung beginnt selten mit einer formellen Strategie, sondern damit, dass ein Team ein neues Tool ausprobiert, eine Mitarbeiterin einen KI-Assistenten nutzt oder ein Anbieter KI-Funktionen in eine bestehende Plattform einbaut. Das ist per se nicht problematisch – es ist oft genau das, was Unternehmen wollen: Innovation und Effizienz. Kritisch wird es aber, wenn die KI-Nutzung schneller wächst, als die Organisation nachvollziehen kann – wenn die Geschäftsleitung zwar weiss, welche Tools offiziell freigegeben sind, aber nicht, welche Tools Mitarbeitende wirklich nutzen, welche Daten dabei eingegeben werden und wer für KI-gestützte Entscheide letztlich verantwortlich bleibt. Genau deshalb ist Schatten-KI nicht nur ein IT-Thema, sondern ein Warnsignal für die Governance in einem Unternehmen: Man kann nicht steuern, was man nicht sieht.

- **Sichtbarkeit (Dokumentation) vor Bürokratie:** ein verlässliches Bild verschaffen, welche KI-Tools wofür genutzt werden, welche Daten sie verarbeiten, wer den Anwendungsfall verantwortet und welche Fälle eine Freigabe oder zusätzliche Kontrollen brauchen.
- **Governance-Prozess:** Kernbausteine dafür sind eine KI-Richtlinie, ein Onboarding-Prozess für neue Tools, ein KI-Inventar, klare Zuständigkeiten, Freigabewege und die Dokumentation wesentlicher Entscheide. Aber Vorsicht: Ein zu langsamer oder komplizierter Prozess treibt die Nutzung nur weiter in den Schatten.
- **Governance nach Risiko differenzieren:** Ein KI-Tool für unkritische interne Textentwürfe braucht andere Kontrollen als eines, das mit Kunden-, Personal- oder Gesundheitsdaten arbeitet oder Entscheide massgeblich beeinflusst.
- **Einbindung von Entwicklern:** Nicht verbieten, sondern einbinden: Mitarbeitende werden KI weiter ausprobieren – die wirksamere Strategie ist, die tatsächliche Nutzung in einen Rahmen mit Sichtbarkeit, Verantwortlichkeit und verhältnismässigen Kontrollen zu gestatten, statt die Vorteile der Technologie zu verhindern.

Daten & Dritte

- **Data Governance** nach dem Vorbild von Art. 10 AI Act: Datenqualität, -herkunft und Bias-Prüfungen von KI-Systemen dokumentieren.
- **Sofern Personendaten betroffen sind:** Zulässigkeit/Berechtigung beim Einsatz von solchen Daten in KI-Systeme nachweisen und Sicherungsmassnahmen für eine datenschutzkonforme Bearbeitung (sowohl unter der DSGVO als auch unter dem Schweizer Datenschutzgesetz).
- **Verträge mit KI- und Cloud-Anbietern auf Data-Act-Konformität prüfen** (keine missbräuchlichen Klauseln, ausreichend Exit-/Wechselmöglichkeiten, Schnittstellenoperabilität). Ziel dieser Prüfung ist, sicherzustellen dass das Unternehmen

ausreichen Exitmöglichkeiten hat (kein vendor lock in) und ob der Zugriff auf seine eigenen (Maschinen-)Daten vertraglich sichergestellt ist.

- **Sorgfaltsprüfung bei KI-Drittanbietern:** Konformitätsnachweise, Dokumentation und vertragliche Absicherung (Haftung, Auskunftsrechte, Auslagerungsregeln) sollten auch bei diesen Drittanbietern vorliegen.

Nachweis- und Schulungspflichten

- **KI-Kompetenz im Unternehmen sicherstellen** (Schulungskonzept, insbesondere für Mitarbeitende in sensiblen Bereichen wie HR oder Kreditvergabe).
- **Transparenzmassnahmen umsetzen** (Kennzeichnung von Chatbots, KI-generierten Inhalten, Deepfakes) – auch ohne unmittelbare Schweizer Pflicht als Reputations- und Vertrauensschutz sinnvoll.
- **Nachvollziehbare Dokumentation und Monitoring-Prozesse** etablieren, die im Prüfungsfall belastbare Nachweise liefern.

Cybersicherheit parallel zum KI-Ausbau verstärken

Ein weiterer Aspekt wird beim Aufbau von KI-Governance oft übersehen: Nicht nur Unternehmen setzen verstärkt auf KI – auch Cyberkriminelle haben sie längst für sich entdeckt. Angreifer nutzen bevorzugt, KI-gestützte Tools, um Schwachstellen automatisiert zu scannen, Angriffe zu automatisieren und Phishing-E-Mails in einem Bruchteil der bisherigen Zeit zu erstellen – mit höherer Angriffsfrequenz und -erfolgsquote. Wer in den **Aufbau eigener KI-Fähigkeiten** investiert, sollte die **Cybersicherheit zumindest im gleichen Tempo mitziehen**.

- **Cybersicherheits-Tools** einsetzen, die gezielt auf KI-gestützte Angriffsmuster (automatisierte Scans, adaptive Malware, KI-Phishing) ausgelegt sind.
- **Cybersicherheitsschulung** nicht kürzen, sondern ausbauen: Technologie allein schützt nicht – gute digitale Sicherheitsgewohnheiten (u. a. Multi-Faktor-Authentifizierung, Passworthygiene, Erkennen von KI-generiertem Phishing) bleiben zentral.
- **Cybersicherheits-Budget und KI-Investitionsbudget gemeinsam planen**, damit das Sicherheitsdispositiv nicht der KI-Einführung hinterherhinkt.

Finanzinstitut-spezifisch

- Abgleich der internen Governance mit **FINMA-Aufsichtsmitteilung 08/2024:** Inventarisierung, Zuständigkeiten, Tests, Monitoring, Schulung als Mindeststandard.
- Bei KI-Einsatz in kritischen Prozessen oder bei der Berechnung regulatorisch vorgegebener Grössen frühzeitig das Gespräch mit der FINMA suchen.
- Erklärbarkeit und unabhängige Prüfung von Modellen sicherstellen, insbesondere bei Kreditvergabe, Betrugserkennung und Transaktionsmonitoring.

- Regulatorische Entwicklungen aktiv verfolgen (EU Digital Omnibus, Schweizer Vernehmlassung Ende 2026, weitere FINMA-Mitteilungen) und Governance-Framework periodisch aktualisieren.

4. Take Away für den CEO und VR

KI-Governance ist kein IT-Projekt, sondern ein Führungsthema, das Risikomanagement, Datenrecht, Vertragsgestaltung und Aufsichtsrecht zusammenführt. Wer diesen «Stack» strukturiert angeht, reduziert nicht nur regulatorische Risiken, sondern schafft die Grundlage, KI-Chancen im Unternehmen verantwortungsvoll zu nutzen. Eine vertiefte Analyse einzelner Aspekte – etwa zu den Risikoklassifizierungen unter dem EU AI Act, zu einzelnen Vertragsklauseln unter dem EU Data Act oder zu den FINMA-Detailanforderungen – wird hier nicht vorgenommen und bleibt einer separaten Prüfung im Einzelfall vorbehalten.

Diese Kurzpublikation dient der allgemeinen Information und ersetzt keine Rechtsberatung im Einzelfall.

Dirk Spacek, Dr. iur., LL.M. ist Rechtsanwalt und Partner in Zürich. Er berät Unternehmen in allen vertrags- und wirtschaftsrechtlichen Belangen mit besonderem Fokus auf Fragen an der Schnittstelle von Technologie, Immaterialgüter- und Daten/Cyberrecht.