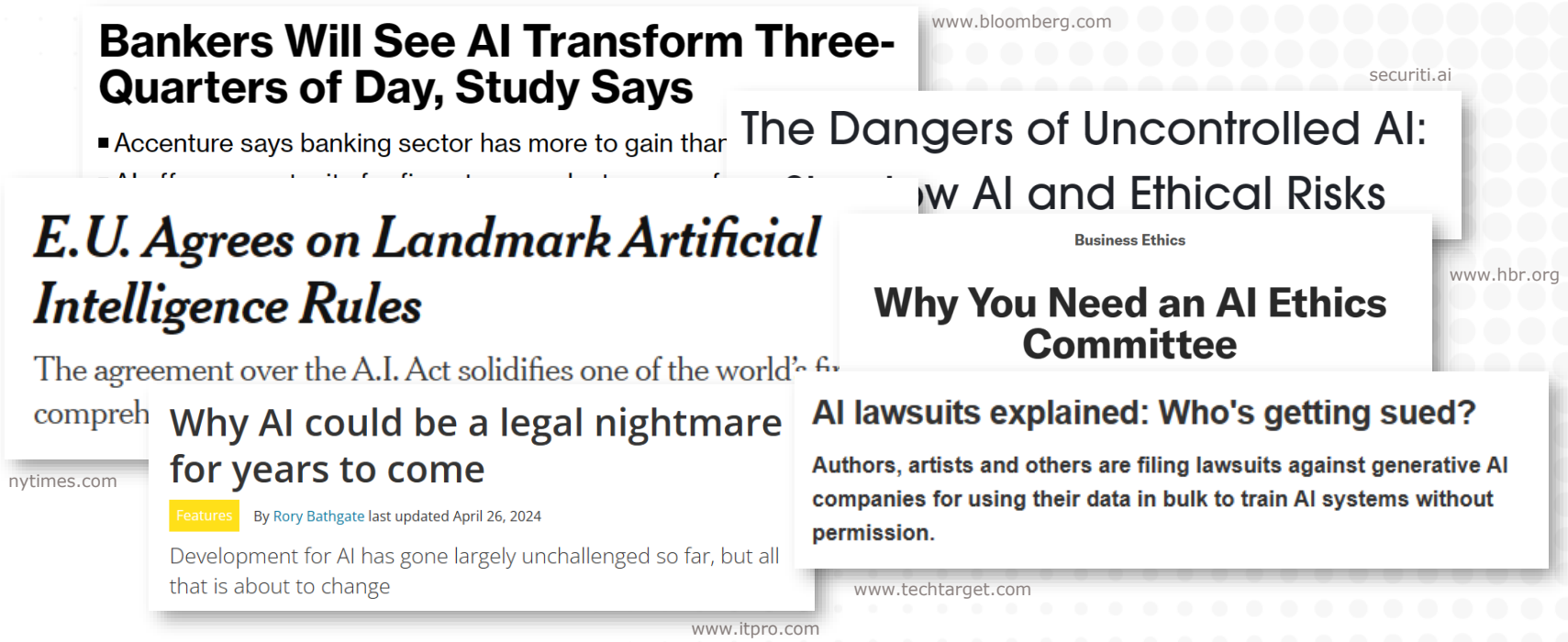
VISCHER

KI in Finanzinstituten.
Was wann wie regeln?

David Rosenthal, Partner, VISCHER AG
20. Juni 2024

Einsatz von KI wird weiter zunehmen



Die wichtigsten Compliance-Fragen

Checkliste: 18 KI-Compliance-Schlüsselfragen.

Unter vischer.com/ki finden Sie kostenlose Ressourcen zu diesen Themen sowie zu KI-Governance und Risikomanagement (keine Registrierung erforderlich)

KI = System, das Ergebnisse auf Basis eines Trainings und nicht nur einer Programmierung erzeugt

Datenschutz

- Haben wir einen angemessenen Vertrag mit den von uns genutzten Providern (z.B. einen ADV, EU SCC, Verbot der Eigennutzung unserer Daten)?
- Haben wir die Leute über die Zwecke informiert, zu denen wir Daten von ihnen bearbeiten oder erzeugen?
- Haben wir es im Griff, wenn die KI falsche oder anderweitig unzulässige Daten über sie produziert?
- Wenn eine KI wichtige Entscheidungen über sie trifft, können sie diese von einem Menschen prüfen lassen?
- Ist unsere KI vor Missbrauch und Angriffen geschützt und auch sonst sicher, insbesondere, wo wir Dritten die Nutzung erlauben (z.B. Chatbot)?
- Können wir Auskunfts- und Berichtigungsbegehren wie erforderlich umsetzen?
- Haben wir eine Risikobeurteilung für unser Vorhaben (inklusive einer DSFA) durchgeführt?

Vertragspflichten, Geheimhaltung

- Kommen wir unseren Geheimhaltungspflichten nach (z.B. beim Einsatz von Providern, Verhinderung der unerwünschten Preisgabe von Daten)?
- Untersagen unsere Verträge die von uns ins Auge gefasste Anwendung (z.B. NDA, welches die Nutzung von Daten für unsere Zwecke einschränkt)?

Schutz von Inhalten Dritter

- Füttern wir KI-Systeme nur dann mit Inhalten Dritter, soweit unsere Lizenzen oder die gesetzlichen Schranken des Urheberrechts dies zulassen?
- Vermeiden wir die Erstellung von Inhalten, die bereits bestehenden Inhalten Dritter entsprechen?

EU AI Act (noch nicht in Kraft)

- Ist klar, dass wir entweder nicht unter den EU AI Act fallen oder unser Vorhaben keine verbotene Praktik ist und möglichst auch kein "Hoch-Risiko"-KI-System (und gehen wir ansonsten richtig damit um)?
- Wenn eine KI "Deep Fakes" erstellt oder mit Menschen interagiert oder sie beobachtet, werden sie dann darauf hingewiesen gemacht?

Andere (auch ethische) Aspekte

- Vermeiden wir Diskriminierung beim Einsatz von KI?
- Behält der Mensch (wirklich) die Kontrolle über die KI?
- Können wir unsere KI-Ergebnisse rechtfertigen/erklären?
- Sagen wir es den Leuten, wie wir KI einsetzen, wenn es für sie unerwartet sein könnte, und erlauben wir ihnen gar, sich für oder gegen deren Einsatz zu entscheiden?
- Haben wir ein angemessenes KI-Testing, angemessene Überwachung und ein angemessenes Risk-Management?

VISCHER

Blog-Beitrag und weitere Infos:

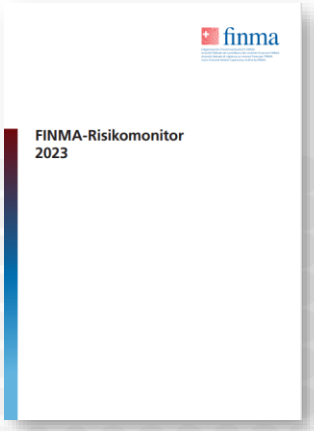
https://bit.ly/3WNgxeO
https://vischer.com/ki

Hier wirken auch die Aufsichtsbehörden

vischerlnk.com/ki-compliance-kurz

Erwartungen der FINMA

1. Es müssen klare Rollen und Verantwortlichkeiten sowie Risikomanagementprozesse definiert und implementiert werden. Die Verantwortung für Entscheidungen kann nicht an KI oder Drittparteien delegiert werden. Alle Beteiligten müssen über genügend Know-how im Bereich KI verfügen.
2. Bei der Entwicklung, der Anpassung und in der Anwendung von KI ist sicherzustellen, dass die Ergebnisse hinreichend genau, robust und zuverlässig sind. Dabei sind sowohl die Daten als auch die Modelle und die Resultate kritisch zu hinterfragen.
3. Die Erklärbarkeit der Resultate einer Anwendung sowie die Transparenz über deren Einsatz sind je nach Empfänger, Relevanz und Prozessintegration sicherzustellen.
4. Nicht begründbare Ungleichbehandlung ist zu vermeiden.



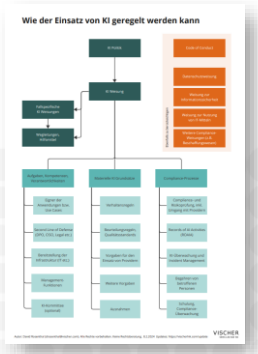
Haben Sie verstanden, worum es der FINMA geht und wie dies zu erfüllen ist?

KI-Governance: Sechs Schritte

- Voraussetzungen schaffen: Robustes **Data Management**
- Aufgaben, Kompetenzen und Verantwortlichkeiten (**AKV**) regeln
- Richtlinie mit Vorgaben zum **Umgang mit KI** um Mitarbeitende "sicher" zu machen und einen KI-Einsatz zu ermöglichen
- **Schulung** im sicheren und verantwortungsvollen Umgang mit KI und Vermittlung von KI-Kenntnissen – bis zur GL und zum VR, damit die Risiken bekannt sind und übernommen werden können
- **Map & Track** von (relevanter) KI im Unternehmen
- **Risiko-Management** für KI-Vorhaben und Tools (heisst: die wichtigsten Risiken beurteilen und Massnahmen dazu treffen)

Inhalte einer KI Weisung 1/2

vischerlnk.com/
ki-governance



- **Ableitung** aus "KI Politik", Abgrenzung zu anderen Weisungen
- **Aufgaben, Kompetenzen und Verantwortlichkeiten**
  - Eigner von KI-Anwendungen, Second Line (inkl. Koordination), Zulassung von KI-Anwendungen, KI-Kommittee (optional)
  - Bereitstellung von Infrastruktur, Abgrenzung zu Anwendungen
- **Prozesse**
  - Verzeichnis der KI-Anwendungen (analog Datenschutz)
  - Zulassung von KI-Anwendungen und Provider-Verträge (inkl. Compliance-Prüfung und Risiko-Management)
  - KI-Überwachung (und Korrekturen), Incident Management
  - Anfragen von betroffenen Personen
  - Schulung der Mitarbeitenden, Compliance-Überwachung

IKS

Inhalte einer KI Weisung 2/2

vischerlnk.com/ki-provider-check

- **Vorgaben für Mitarbeitende**
  - Welche KI-Anwendungen wofür und womit (Daten) erlaubt sind
  - Verhaltensregeln beim Einsatz von KI (z.B. Human Oversight, Prüfung der Ergebnisse, Transparenz, Meldepflichten)
- **Vorgaben für KI-Anwendungen (und Provider)**
  - Einhaltung des anwendbaren Rechts, der aufsichtsrechtlichen Erwartungen und der weitergehenden Vorgaben ("Ethik")
  - Datenquellen, Testing, Dokumentation, Überwachung, Verträge
  - Aber: Freiräume für den Experimentaleinsatz sichern
- **(KI-)Regelungen für andere Bereiche**
  - Policy betr. Secondary Use von Daten in Verträgen mit Dritten

z.B. Formulierung von Leitsätzen zur Konkretisierung der Vorgaben

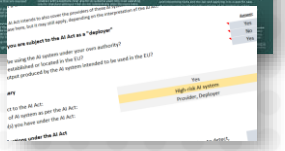
Zunahme an Cloud-Projekten (→ CCRA-FI)

Sonderfragen

- **Braucht es einen "AI Officer"?**
  - Nein, jedenfalls nicht aus Sicht der Compliance
- **Risikobasierter Ansatz?**
  - Ja, denn nur wenige Anwendungen bergen ein hohes Risiko
  - Belastung durch unterschiedliche "Prüftiefen" reduzieren
  - Risiken strukturiert beurteilen und dokumentieren (z.B. vischerlnk.com/gaira [Open Source, kostenlos])
- **Wie umgehen mit dem EU AI Act?**
  - Anwendungsfälle erheben und verzeichnen (Sind wir in-scope? Hoch-Risiko-KI-Systeme? Welche Rolle? Welche Pflichten?)
  - Revisoren/FINMA erwarten Wissen und Einhaltung

vischerlnk.com/gaira

vischerlnk.com/ki-risikocheck



vischerlnk.com/ai-act-uc

vischerlnk.com/gaira

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: david.rosenthal@vischer.com

Mehr Unterlagen:
www.vischer.com/ki
www.rosenthal.ch

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com