KI-GOVERNANCE

Tatjana Furrer
Rechtsanwältin, Managing Consultant

ABLAUF

1. Aktueller Stand der KI – Warum jetzt handeln?
2. Bedeutung der KI-Governance
3. Gesetzliche Anforderungen (EU AI Act und Schweizer Rechtslage)
4. Datenschutzrechtliche Pflichten
5. KI Freigabeprozess, KI Inventar, KI Benutzerweisung, KI-Governance Weisung
6. Fazit

AKTUELLER STAND DER KI

AKTUELLE ENTWICKLUNG VON KI AUF DEN PUNKT GEBRACHT

Klassische KI

- Beruht auf fest definierten Regeln und Expertensystemen, die spezifische Aufgaben in engen Bereichen erledigen.

Generative KI

- Grosse Modelle/Generatoren für Sprache und Bilder, die aus riesigen Datenmengen eigenständig neue Texte, Bilder oder Codes erzeugen können, aber eher passiv auf Anfragen reagieren.

Reasoning-Modelle

- Ergänzen die grossen Modelle mit strukturiertem Schlussfolgern und Planen, Probleme werden in Einzelschritte zerlegt, Zwischenergebnisse werden reflektiert.

KI-Agenten

- Führen konkrete Handlungen über Schnittstellen aus (API's, Datenbanken, Bedienungsroboter) bspw. E-Mails versenden oder Transaktionen auslösen.

Agentic AI

- Zusammenführung von Autonomie, persistenter Erinnerung und adaptivem Lernen
  - Plant eigenständig,
  - Wählt Werkzeuge aus,
  - Erinnert sich, «lernt», passt sich dynamisch an
  - Koordiniert sich mit anderen Agenten

Paradigmenwechsel: von regelbasierten Abläufen hin zu digitalen Akteuren mit eigener Handlungsfähigkeit und direkter Wirkung in der Realität

WARUM JETZT HANDELN?

- **Agentic KI: verschiebt die Risiken von „falsche Antwort im Chat“ zu „falsche Handlung in der realen oder digitalen Welt“.**
- **Geschwindigkeit & Skalierung:** Fehlhandlungen in Sekunden, hohes Schadenspotential, sehr hohe Reputationsrisiken
- **Reifegrad**
  - Überhitzter Hype
  - Sehr heterogene Qualität
  - Hohe Vendor-Risiken
  - Wilder Westen, Entwicklungen ausser Rand und Band

- *Haftung?*
- *Transparenz?*
- *Nachvollziehbarkeit?*
- *Datenminimierung und Zweckbindung?*
- *Zugriff auf andere Applikationen!*

BEDEUTUNG DER KI-GOVERNANCE
GESETZLICHE ANFORDERUNGEN

WARUM IST KI-GOVERNANCE WICHTIG?

Mit **KI-Governance** ist der organisierte und kontrollierte Rahmen für den verantwortungsvollen, sicheren und rechtskonformen Einsatz von KI-Systemen in einer Organisation gemeint. Ein solches Rahmenwerk ist aus mehreren Gründen wichtig:

Datenschutz und Ethik
KI verarbeitet grosse Mengen an Personendaten, oft auch besonders schützenswerte Daten. Datenschutzrechtliche Vorgaben gelten uneingeschränkt.

Sicherheits- und Qualitätsrisiken
Schwachstellen können missbraucht werden, schlechte Trainingsdaten führen zu verzerrten Ergebnissen. Governance sorgt für Datenqualität und Notfallpläne.

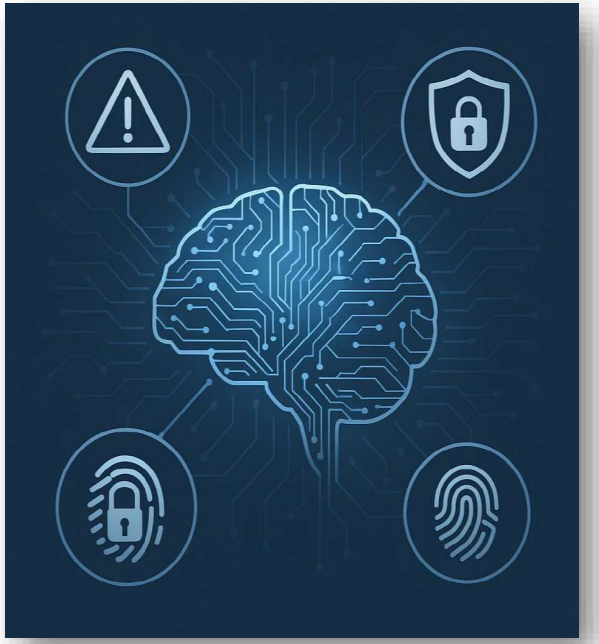
Regulatorische Anforderungen
Verschiedene Branchen (Finanz, Gesundheit, Energie) unterliegen Vorschriften. KI-Systeme und deren Einführung müssen branchenspezifischen Normen entsprechen.

Haftung
Fehlleistungen der KI führen zu Haftungsfragen – das Unternehmen haftet, nicht die KI.

Reputation
Voreingenommene oder falsche KI-Ergebnisse können Imageschäden verursachen. Governance stärkt Vertrauen durch Freigabeprozesse, Monitoring und Audits.

KI-Governance: Präventiver Rahmen zur Beherrschung der vielfältigen KI-Risiken.
Ziel: KI ist kein unkontrolliertes Experiment, sondern eine verlässliche gesetzeskonforme Technologie, die auch die ethischen Werte und die Interessen von Betroffenen berücksichtigt.

AKTUELLE GESETZLICHE ANFORDERUNGEN FÜR KI-SYSTEME



EU-KI-Verordnung (EU AI Act, 2024)

- Erste umfassende europäische Regelung für KI mit *risikobasiertem Ansatz* (verboten / hoch / begrenzt / minimal).
- In Kraft seit **August 2024** – Verbot bestimmter Praktiken (z. B. Social Scoring, Predictive Policing) seit 2025; Pflichten für Hochrisiko-KI ab **August 2026**.
- **Extraterritoriale Wirkung:** Schweizer Anbieter, die KI-Systeme in der EU in Verkehr bringen oder in Betrieb nehmen bzw. Schweizer Anbieter und Betreiber von KI-Systemen, wenn das vom KI-System hervorgebrachte Ergebnis in der EU verwendet wird.

Schweiz (Stand Mai 2026)

- Kein spezifisches KI-Gesetz.
- Bundesrat → technologieneutraler Ansatz, punktuelle Ergänzungen bestehender Gesetze.
- **EJPD-Mandat bis Ende 2026:** Entwurf zur Umsetzung der *Europarats-KI-Konvention* (Transparenz, Datenschutz, Nichtdiskriminierung, Aufsicht).
- Ziel: Internationale Kompatibilität und Zugang zum EU-Markt.

Branchenvorgaben

- **FINMA-Mitteilung (12/2024):** KI-Nutzung muss in Governance-, Risiko- und Kontrollsysteme integriert sein.
- **Automatisiertes Fahren (03/2025):** Zulassung von Autobahnpilot-Systemen und fahrerlosen Fahrzeugen unter Bedingungen.
- **Bundesverwaltung / EDÖB:** Leitlinien und Empfehlungen zum datenschutzkonformen KI-Einsatz.

ANWENDBARE SCHWEIZERISCHE RECHTSGRUNDLAGEN

Grundrechte
- Bundesverfassung garantiert Menschenwürde, Persönlichkeitsschutz und Diskriminierungsverbot.
- Grenzen für den KI-Einsatz, besonders bei staatlichen Stellen (z. B. keine Massenüberwachung).
- Auch im privaten Bereich gilt z. B. Art. 28 ZGB (Persönlichkeitsschutz).

Datenschutzgesetz (DSG)
- Zentrales Gesetz beim Einsatz von KI mit Personendaten.
- Verlangt Transparenz und Information bei automatisierter Entscheidungsfindung.
- Betroffene haben Anspruch auf menschliche Überprüfung oder Begründung.
- Grundprinzipien: Zweckbindung, Datenminimierung, Sicherheit.

Urheberrecht
- Geschützte Inhalte dürfen nicht beliebig für KI-Training genutzt werden.
- Nur menschlich geschaffene Werke sind urheberrechtlich geschützt.

Haftung
- Allgemeine Haftungsgrundsätze gelten auch für KI (u.a. Produktehaftpflicht, OR Art. 41, 97, 754).
- Unternehmen haften bei Fehlentscheidungen, Reputationsverlusten oder Schäden.
- Strafrechtlich sind immer Menschen verantwortlich, nicht die KI selbst.

Auch ohne spezielles KI-Gesetz ist der rechtliche Rahmen in der Schweiz klar.
Sorgfalt, Transparenz und Rechtskonformität sind die zentralen Pfeiler für den verantwortungsvollen KI-Einsatz.

DATENSCHUTZRECHTLICHE PFLICHTEN

ZIELE UND GRUNDPRINZIPIEN DES DATENSCHUTZES BEI KI-SYSTEMEN

Ziel des Datenschutzes

- Schutz der Persönlichkeit und der Privatsphäre der natürlichen Person
- Datenbearbeitung muss u.a. verhältnismässig, transparent und zweckgebunden sein
- Ziel: Missbrauch und unberechtigten Zugriff verhindern

Selbstbestimmung und Kontrolle

- Betroffene müssen wissen, wie, von wem und wozu ihre Daten bearbeitet werden
- Sie haben Kontrollrechte:
  → Auskunft
  → Widerspruch
  → Löschung

Bedeutung für KI-Systeme

- Automatisierte Entscheidungen überprüfbar, erklärbar und nachvollziehbar
- „Black Box“ Verantwortung bleibt beim Menschen

GRUNDSÄTZLICHE PFLICHTEN IM UMGANG MIT KI UND DATEN

- Datenschutz-Folgenabschätzung (DSFA)
- Auftrags-bearbeitung
- Datenüber-mittlung ins Ausland
- Bearbeitungs-reglement
- Einwilligung der Betroffenen
- Datensicherheit und Transparenz
- Verantwortlichkeit und Gouvernance
- Automatisierte Entscheidungen überprüfbar
- Betroffenenrechte
- Urheberrechte

KI-FREIGABEPROZESS
KI-INVENTAR
KI-BENUTZERWEISUNG
KI-GOVERNANCE WEISUNG

MINMALE UMSETZUNG AI SECURITY AND GOVERNANCE

KI-BENUTZERWEISUNG – INHALTE

Verhaltensregeln

Mitarbeitende dürfen nur die für die jeweiligen Schutzkategorien und Zwecke freigegebenen KI-Systeme nutzen; sie müssen sensible Daten schützen, Ergebnisse kritisch prüfen und Transparenz gegenüber Betroffenen gewährleisten.

Verbotene Anwendungen

Keine automatisierten Entscheidungen ohne menschliche Kontrolle, keine Datenweitergabe zu Trainingszwecken, keine KI-gestützte Mitarbeitendenüberwachung, keine diskriminierenden oder unethischen Einsätze.

Branchenspezifika

Sektorspezifische Verbote und Anforderungen können ergänzt werden (z. B. im Finanzbereich hohe Anforderungen an Trading-KI).

Schulungen

Die Weisung muss stufen- und funktionsgerecht geschult werden; neue Mitarbeitende werden im Onboarding informiert.

Meldewege

Mitarbeitende sollen Verstösse oder Unsicherheiten melden können; klare Anlaufstellen schaffen.

KI-FREIGABEPROZESS: GRUNDANFORDERUNGEN

Zweck:
Sicherstellen, dass gesetzliche Vorgaben eingehalten werden und kein KI-System unkontrolliert eingeführt wird.

1. **Antrag:** Nutzer muss für eine neue KI-Anwendung einen Antrag mit Use-Case und Nutzen einreichen.
2. **Risikokategorisierung:** Das KI-Gremium oder die Fachstelle stuft das Vorhaben in eine Risikoklasse ein (normal, mittel, hoch).
3. **Konformitätsprüfung:** Prüfung der rechtlichen Anforderungen (Rechtsgrundlage, DSFA, Auslandsübermittlungen), der technischen Sicherheit und der fachlichen Korrektheit.
4. **Entscheidung:** Das zuständige Gremium erteilt oder verweigert die Freigabe; Auflagen und Dokumentation sind erforderlich. Aufnahme im Inventar.
5. **Implementierung & Monitoring:** Technische Umsetzung und kontinuierliches Monitoring, um Abweichungen oder Vorfälle frühzeitig zu erkennen.

Für jedes KI-System gibt es einen verantwortlichen Owner.

KI GOVERNANCE-WEISUNG

Die **Governance-Weisung** ergänzt Benutzerweisung und Freigabeprozess um eine **unternehmensweite Steuerungsrichtlinie**.

Stellt sicher, dass KI-Systeme nach **einheitlichen Grundsätzen** und unter kontrollierten Bedingungen eingesetzt werden.

Legt **Zuständigkeiten und Verfahren** für den gesamten Lebenszyklus von KI-Systemen fest.

Prinzipien
Definiert die grundlegenden Prinzipien (z.B. Rechtmässigkeit, Transparenz, menschliche Kontrolle, Datenschutz, IT-Sicherheit, Fairness)

Lebenszyklus
Enthält klare Vorgaben für die Entwicklung, Beschaffung, Betrieb und Überwachung von KI. Insbesondere werden Anforderungen an die Datenqualität und die Auswahl von Trainingsdaten gestellt, Bias- und Fairness-Prüfungen verankert, regelmässige Auditierungen der KI Systeme vorgeschrieben und klare Verantwortlichkeiten für alle beteiligten Rollen festgelegt.


FAZIT

EMPFEHLUNGEN – KI-MANAGEMENT IN DER PRAXIS

☑ Verbindliche Regeln:
Definieren Sie verbindliche interne Regeln in Form einer Benutzerweisung und ggf. einer Governance-Weisung.

☑ Strikter Freigabeprozess:
Nutzen Sie einen formellen Freigabeprozess, um KI-Systeme zu prüfen und freizugeben.

☑ Zentrales Inventar:
Erfassen Sie alle KI-Systeme; prüfen Sie Vertragsgrundlagen und Risiken.

☑ Regelmässige Schulungen:
Sensibilisieren Sie Mitarbeitende zum sicheren Umgang mit KI und zu ihren Pflichten.

☑ Kontrolliertes Pilotieren:
Auch Tests und Pilotprojekte müssen die Mindestanforderungen erfüllen.

SWISS INFOSEC

IHR KONTAKT
SWISS INFOSEC AG

IHRE PROBLEMLÖSUNG

beginnt mit einem Kontakt bei uns:

+41 41 984 12 12
infosec@infosec.ch
Tatjana Furrer
Managing Consultant
tatjana.furrer@infosec.ch