CERHA HEMPEL

Compliance beim KI-Einsatz im Unternehmen

Dr. Roman Heidinger, M.A.

Obmann-Stv. Forschungsverein Infolaw &

Rechtsanwalt

Wien, 25. April 2024

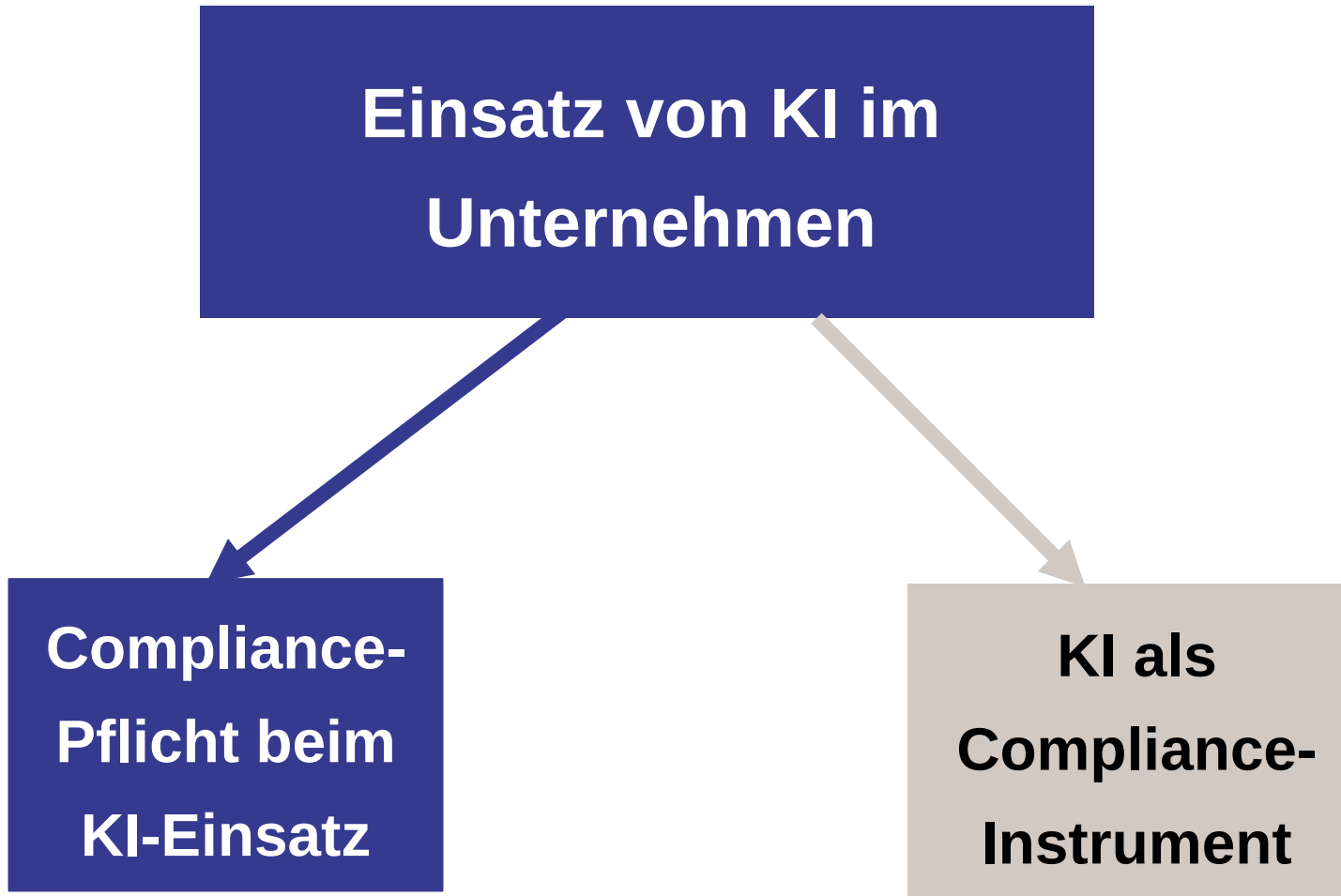
Einleitung

- KI-Systeme funktionieren nach Wahrscheinlichkeiten und mathematischen Methoden und haben kein näheres Verständnis für die analysierten/bearbeiteten Daten.
- Durch die eigenständige Fortentwicklung von Algorithmen sind die Schritte der KI nicht mehr vorhersehbar und oftmals auch nicht nachvollziehbar.
  - Prüfung der ursprünglichen Regeln iS einer Verfahrensprüfung nicht sinnvoll.
- Es stellt sich daher die Frage, nach welchen generellen Kriterien sich die Zulässigkeit des Einsatzes von KI in Unternehmen bemisst.
- Im Kern geht es um die Verantwortlichkeit der Geschäftsleitung für Schäden, die durch den (fehlerhaften) Einsatz von KI verursacht werden.

Beispiel: Geschäftsgeheimnisse Verlust

- Anfang 2023: Leak bei Samsung
  - Vertrauliche Daten (Quellcodes) wurden in ChatGPT eingegeben
  - Da OpenAI (Betreiber von ChatGPT) eingegebene Inhalte für die weitere Entwicklung speichert und verwendet, liegen diese wertvollen Informationen nun bei OpenAI
  - Eingabe bei ChatGPT = Offenlegung des Geschäftsgeheimnisses → uU kein Geschäftsgeheimnisschutz
- Verantwortlichkeit der Geschäftsleitung?
  - Bei Schaden: Wurden ausreichende Compliance-Maßnahmen gegen solche Verstöße gesetzt?

KI und Compliance



Gesellschaftsrechtlicher Rahmen

- Leitungsorgane von Kapitalgesellschaften sind gesetzlich verpflichtet, bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.
  - § 25 Abs 1 GmbHG bzw § 84 Abs 1 AktG
  - Business Judgment Rule
- Klassische Leitungsaufgaben können nicht an KI delegiert werden
  - In der Literatur viel diskutiert, mA praktisch nicht so relevant
- Die Leitungsorgane trifft die Beweislast, dass sie die obliegende Sorgfalt angewendet haben.
- Darüber hinaus ist ein internes Kontrollsystem zu führen, das *„den Anforderungen des Unternehmens“* entspricht.
  - Vgl § 22 Abs 1 GmbHG, § 82 AktG

Business Judgement Rule
(§ 84 Abs 1a AktG, § 25 Abs 1a GmbHG)

- Ein Vorstandsmitglied/Geschäftsführer handelt jedenfalls im Einklang mit der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters, wenn er sich bei einer unternehmerischen Entscheidung
  - nicht von sachfremden Interessen leiten lässt und
  - **auf der Grundlage angemessener Information annehmen darf,**
  - zum Wohle der Gesellschaft zu handeln.
- Ex-ante Betrachtung (neue Technologien mA für Rückschaufehler besonders anfällig)
- Aufgrund des vielfach vorherrschenden Blackbox-Chakter bedarf es umfassende Information und einer Risikoanalyse beim KI Einsatz

Kontrollsystem

- Keine allgemein gültige Definition des Kontrollsystems bzw Compliance-Systems
  - Umfasst nicht nur Finanzgebarung (zB auch IT-Compliance)
  - Weiter Spielraum der Unternehmensleitung hinsichtlich der Risikoabschätzung
- Die Leitungsorgane trifft die Pflicht, durch Kontrollsysteme dafür Sorge zu tragen, dass Dritte (insb Mitarbeiter) ihrer Legalitätspflicht bei ihrer Tätigkeit für die Gesellschaft umfassend nachkommen.
  - Auch die Effektivität des Kontrollsystems muss persönlich überprüft werden.
- Grundlegend ist das *„Siemens/Neubürger“*-Urteil, in welchem das Gericht aussprach, dass die Leitungsorgane ihre Pflicht nur dann erfüllen, wenn sie bei entsprechender Gefährdungslage eine auf Schadensprävention und **Risikokontrolle** angelegte Compliance-Organisation einrichten.

Siemens-Neubürger-Urteil
(LG München I vom 10.12.2013, 5 HK O 1387/10)

„Im Rahmen seiner Legalitätspflicht hat ein Vorstandsmitglied dafür Sorge zu tragen, dass das Unternehmen so organisiert und beaufsichtigt wird, dass keine Gesetzesverstöße wie Schmiergeldzahlungen an Amtsträger eines ausländischen Staates oder an ausländische Privatpersonen erfolgen.

Seiner Organisationspflicht genügt ein Vorstandsmitglied bei entsprechender Gefährdungslage nur dann, wenn ***er eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet.***

Entscheidend für den Umfang im Einzelnen sind dabei Art, Größe und Organisation des Unternehmens, die zu beachtenden Vorschriften, die geografische Präsenz wie auch Verdachtsfälle aus der Vergangenheit.“

Anforderungen an das Compliance-System (OGH 3.8.2021, 8 Ob A 109/20t, GesRZ 2022, 132)

- Die klagende Gesellschaft wurde Opfer eines *„fake president fraud“.*
- Mitarbeiter wurden von den Tätern unter Vortäuschung falscher Identitäten zur Überweisung von Geld bewegt.
- Entgegen der Vorgabe des Vieraugenprinzips wurden die Telebanking-Überweisungen tatsächlich alleine von der Gruppenleiterin der Finanzbuchhaltung durchgeführt, die dazu sämtliche TAN-Karten mit dem Vermerk der notwendigen PIN-Codes aufbewahrte.
- Die beklagten Geschäftsführer hatten keine Kenntnis von der Missachtung des Vieraugenprinzips.
  - Auch war kein Anlass für einen Verdacht vor dem Schadensfall gegeben.

Anforderungen an das Compliance-System (OGH 3.8.2021, 8 Ob A 109/20t, GesRZ 2022, 132)

- Kontrollsystem war ausreichend:
  - Schulungen (zB hinsichtlich Pishing-E-Mails)
  - Richtlinien
  - Zahlungsprozesse wurden vom Wirtschaftsprüfer überprüft
  - Social-Engineering-Tests durch externe Unternehmen
- Es liegt aber auf der Hand, dass ein Betrug, der die angesprochenen Mitarbeiter gerade zur Umgehung der Kontrolleinrichtungen verleiten will, damit allein nicht verhindert werden kann.
- Vgl aber OGH 26.08.2020, 9 Ob A 136/19v, wo die Nichteinhaltung des Vieraugenprinzips bei Überweisungen bewusst geduldet wurde.

KI Compliance als Teil der IT-Compliance

- Die Leitungsorgane haben auch im Hinblick auf die IT-Systeme für ein Kontrollsystem zu sorgen.
  - IT-Compliance: Summe aller Maßnahmen zur Einhaltung von sämtlichen gesetzlichen und vertraglichen Regelungen betreffend die Sicherheit der IT-Systeme eines Unternehmens
  - Keine (reine) Aufgabe der IT-Abteilung
- Angesichts der Bedeutung von IT-Systemen für das Funktionieren und den Fortbestand des Unternehmens gehört es zu den Pflichten der Leitungsorgane, das Unternehmen vor erkennbaren Gefahren im IT-Bereich zu schützen.
  - zB Hinsichtlich IT-Sicherheit, Redundanz usw.
- Diese Prinzipien gelten auch für den Einsatz von KI
  - Vermeidung von Schäden an der Gesellschaft (zB Geheimnisverlust)
  - Vermeidung von Schäden bei Dritten, welche die Gesellschaft schädigen (zB Produkthaftung)

Compliance im Zusammenhang mit KI

- Auswahl geeigneter Anwendungsbereiche
  - Entscheidende vs vorbereitende KI
  - Genuine Leitungsentscheidungen können nicht an KI übertragen werden
- Pflicht zur sorgfältigen Auswahl von KI-Systemen
  - Risikoanalyse (Senkung zB durch explainable AI)
  - Testläufe
- Qualitätssicherung des Datenmaterials
- Laufende Überprüfung der KI-Systeme (insb Plausibilisierung)
- Sicherheitsmaßnahmen
  - Notfallabschaltung der KI (?)
  - Schutz vor externer Manipulation („Cyberangriff“)
- Erstellung von Richtlinien

Sondergesetzliche Compliance-Pflichten

- Die allgemeinen gesellschaftsrechtlichen Compliance-Pflichten werden durch spezielle Normen ergänzt.
- Dazu zählen (ua):
  - KI-Verordnung
  - NIS2-Richtline
  - DSGVO
  - Normen für den Finanzmarkt (zB DORA)
- Insbesondere der risikobasierte Ansatz der KI-Verordnung lässt sich verallgemeinern.
  - Alleinige Erfüllung der KI Verordnung ist aber nicht ausreichend, um der Einrichtung eines Compliance-Systems Genüge zu tun.

Typische Risiken beim Einsatz von KI

Datenschutzver-letzungen durch unerlaubte Nutzung personenbezogener Daten	**Verbreitung von Falschinformationen**	**Verletzung von Immaterialgüter-rechten (Input/Output)**	**Beeinträchtigung der IT-Sicherheit durch Schwachstellen im KI-System**
Produkthaftung (insbesondere in Risikobereichen wie selbstfahrende Autos und Medizintechnik)	**Marktmissbrauch durch Algorithmen, unbeabsichtigter Zugriff auf wettbewerbsrelevante Informationen**	**ESG Risiken (Energieverbrauch)**	**Gefährdung von Geschäftsge-heimnissen**

Unterfall: Datencompliance

- Unklar ist, inwieweit KI Systeme „vergessen“ können. Im Extremfall darf gesamtes KI System nicht verwendet werden.
  - Herausfiltern einzelner Daten kann technisch schwierig sein.
- Das Risiko beim unerlaubten Einsatz von Trainingsdaten kann nach Rechtsgebieten variieren.
  - Urheberrecht: Unterlassungsanspruch maximal auf Verwendung der Daten, wenn das Werk nach dem Trainingsvorgang „verblasst“
  - DSGVO: Personenbezug muss entfernt werden
  - Bei Geschäftsgeheimnissen: Weites Nutzungsverbot nach § 26c UWG, aber Gutgläubigkeit kann relevant sein.
- Bei Lizenzierung: Compliance in der Lieferkette

Pflicht zum Einsatz von KI?

- Leitungsorgane haben nicht nur das Recht, sondern auch die Pflicht, den Einsatz von KI Systemen zu prüfen.
- Eine Pflicht zum Einsatz von KI besteht nur dann, wenn der Entscheidungsspielraum der Leitungsorgane durch den Nichteinsatz deutlich überschritten wird.
- Dies wird nur bei ausreichend erprobten Anwendungen der Fall sein.

Zusammenfassung

- Über die Regelungen der KI-Verordnung hinaus muss der Einsatz von KI den (gesellschafts)rechtlichen Vorgaben entsprechen.
- Leitungsorgane haben – außerhalb spezieller Normen – einen weiten Ermessenspielraum beim Einsatz von KI.
  - In der Regel gibt es keine Pflicht zum Einsatz von KI-Systemen in Unternehmen
- Im Schadensfall wird es für Leitungsorgane aber idR notwendig sein, das Vorhandensein geeigneter Maßnahmen zur Schadensprävention zu belegen.
  - Kontrollsysteme, Dokumentation von Entscheidungsprozessen
  - Rückschaufehler im Prozess als besondere Gefahr in der Praxis
- Für den Einsatz von KI-Systemen im Internet (General purpose AI system) sollten Leitlinien erarbeitet werden.
- Aufgabe des Aufsichtsrates?

CERHA HEMPEL

Vielen Dank für *Ihre Aufmerksamkeit!*