plenum

CIO Advisory

KI-Compliance

Regulatorische Risiken erkennen
und effektiv steuern

KI in regulierten Unternehmen – Chancen und Risiken

KI bietet zahlreiche Möglichkeiten, Prozesse neu zu gestalten

Viele Unternehmen setzen KI in ihren Geschäftsbereichen, an der Kundenschnittstelle sowie internen Abteilungen ein. Die **Anwendungsfelder** sind dabei breit aufgefächert: Kunden- und Mitarbeitersupport, Vertrieb und Marketing, Prozessautomatisierung und Dokumentenverarbeitung sowie Datenanalyse und Entscheidungsunterstützung sind mittlerweile stark durch KI unterstützt oder davon geprägt.

Abb. 1: KI-Use Cases - Beispiele

Risiken beim Einsatz von KI müssen gesteuert werden

KI verspricht und liefert **Verbesserungen in Zielgrößen wie Effizienz, Kosten, Service und Qualität**. Um den Nutzen über die Umsetzung der Use Cases zu generieren, sind die damit verbundenen Risiken auf ein angemessenes Maß zu reduzieren.

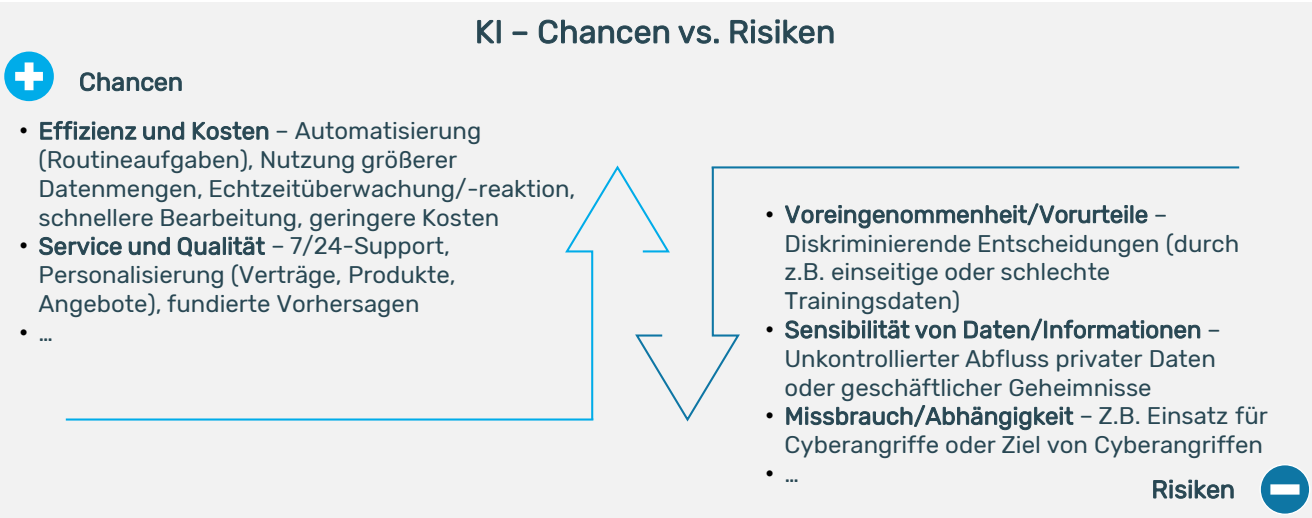

Abb. 2: Chancen- und Risikoaspekte - Exemplarisch

Die Auswirkungen der KI-Risiken sind bei möglichem Eintritt oft nur schwer bezifferbar oder treffen Akteure außerhalb der Unternehmen. Insbesondere die **Identifikation und Behandlung dieser externen Risikowirkungen** ist in der Roadmap der digitalen KI-Transformation oft **unterrepräsentiert**.

Compliance-Risiken durch komplexe Regulierung

Der EU-Gesetzgeber hat auf die Risiken durch den Einsatz von KI reagiert. Die erlassenen Verordnungen zielen auf den **Schutzbedarf sowohl der Unternehmen als auch der externen Akteure: Wirtschaft, Gesellschaft und natürlichen Personen**. Gleichzeitig soll die Innovationsfähigkeit der Unternehmen nicht beschränkt werden.

Die drei wesentlichen EU-Vorgaben zu KI

Insbesondere der vergleichsweise junge **AI Act** setzt für alle Unternehmen Leitplanken und gibt konkrete, abgestufte Vorgaben zum Einsatz von KI. Aber auch in der bestehenden Regulatorik, wie z.B. der **DSGVO** bestehen Zusammenhänge mit datenverarbeitender KI. Darüber hinaus wirkt die branchenspezifische Verordnung **DORA** auf KI als Informations- und Kommunikationstechnologie (IKT).

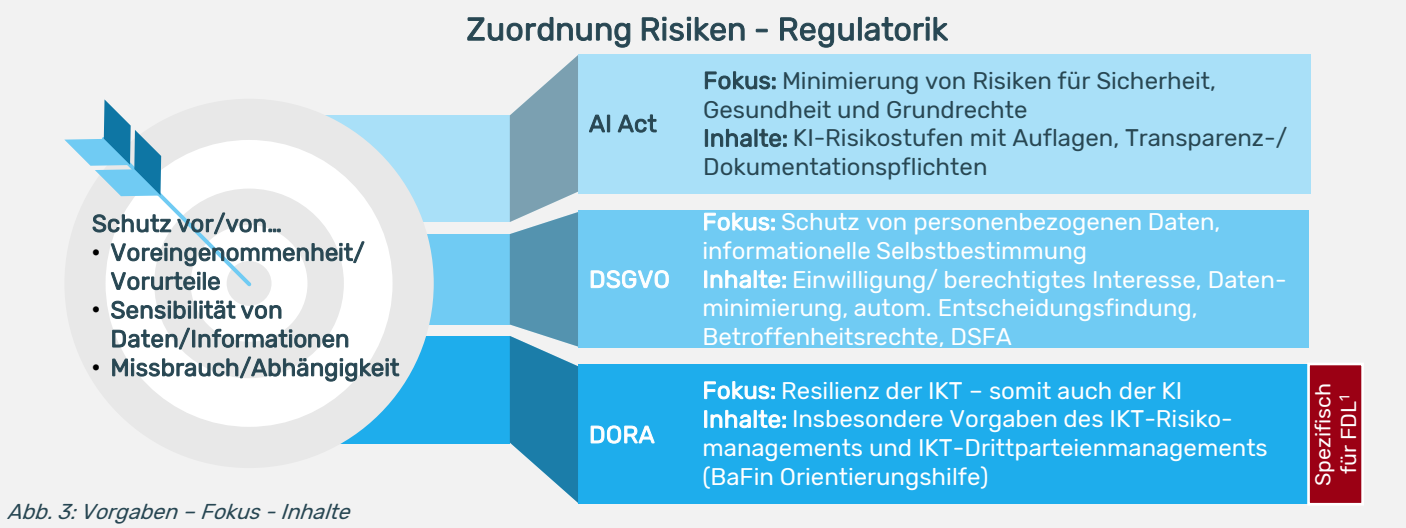

Abb. 3: Vorgaben – Fokus - Inhalte

Non-Compliance - Mögliche wirtschaftliche Auswirkungen

Die Überwachung und Überprüfung der Compliance wird durch verschiedene Behörden wahrgenommen. Für den AI Act ist dies grundsätzlich die **Bundesnetzagentur**. Die Einhaltung der DSGVO wird von der **BfDI und den Landesdatenschutzbehörden** sichergestellt. DORA wird durch die **BaFin/EZB** überwacht und seit Ende August 2026 obliegen auch die Inhalte des AI Act für Finanzdienstleister der Überwachung der Finanzaufsicht.

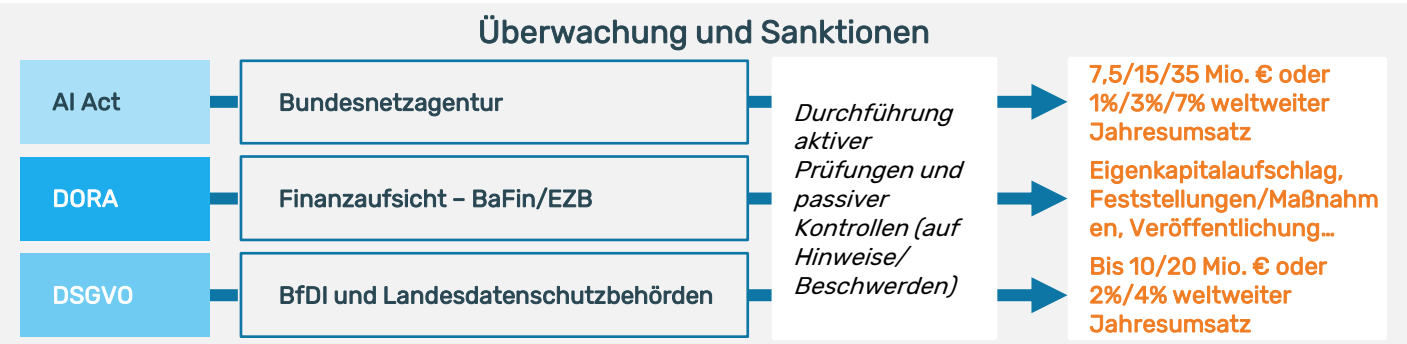

Abb. 4 Überwachung und Strafen/Maßnahmen

Nicht-Einhaltungen und Verstöße können zu **empfindlichen Strafen und Maßnahmen** führen. Unterlassungsanordnungen können zudem das Geschäft nachhaltig schädigen. Damit wird KI-Compliance auch zu einem **wirtschaftlichen Faktor** für die Unternehmen.

Fazit – Zeit für eine Standortbestimmung zur KI-Compliance

Jedes Unternehmen sollte sich mit dem spezifischen Blickwinkel KI die folgenden Fragen stellen:

- Welche Rolle(n) nehme ich im Rahmen des AI Act ein und wie ist mein Stand der Vorgabenerfüllung dazu?
- Wie wirken sich die DSGVO-Vorgaben auf KI-Use Cases/-Systeme aus und wie ist der Stand dazu?
- Für Finanzdienstleister: Welche DORA-Vorgaben gelten auch für KI und werden sie schon für KI befolgt?

[1] FDL – Finanzdienstleister

plenum Leistungsportfolio zur KI-Compliance

Use Cases compliant realisieren - KI-Compliance Check

Mittels eines **strukturierten KI-Compliance Check** identifizieren wir mit Ihnen die Gaps zu den Anforderungen des AI Act, den KI-spezifischen Anforderungen der DSGVO und, für Finanzunternehmen, den KI-spezifischen Anforderungen der DORA. Auf Basis der Analyse werden in Folge die bestehenden Gaps bewertet, und Maßnahmen abgeleitet, so dass Ihr Unternehmen deren Schließung priorisiert und wirksam angehen kann.

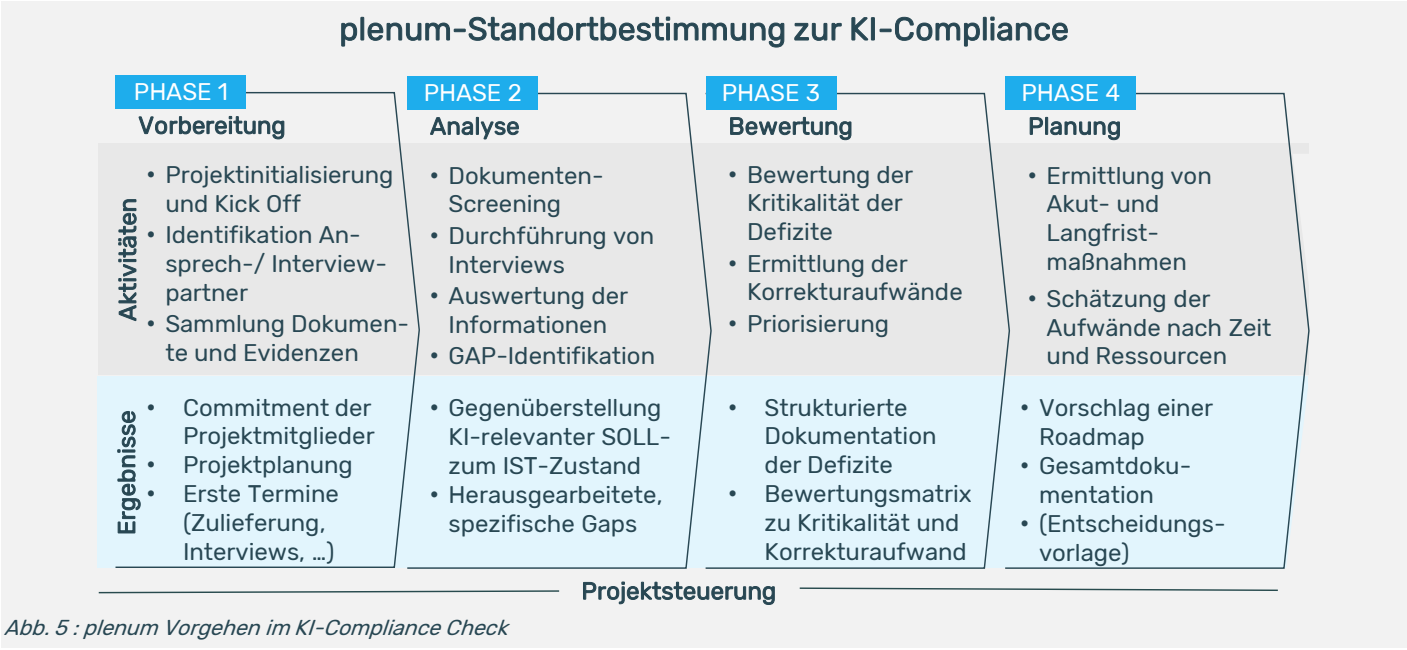

Abb. 5 : plenum Vorgehen im KI-Compliance Check

Die regulatorischen Gaps sind identifiziert – und nun?

Der Grundstein der Gap-Identifikation mit abgeleiteten Maßnahmen ist gelegt. Es steht die Umsetzung der Maßnahmen an und damit die Frage des „Wie". plenum bietet hierzu eine **operative Umsetzungsunterstützung**, welche für Ihr Unternehmen passgenau und dabei effizient und nachhaltig ausgestaltet ist. Im Handshake bewirken **weitergehende analytische und konzeptionelle Unterstützungsleistungen** in vier Schwerpunktbereichen den Aufbau und Betrieb eines Frameworks für den sicheren KI-Einsatz.

KI-Strategie

Ermittlung des Stellenwerts von KI, Bestimmung des Ambitionsniveaus und des angestrebten Reifegrads. Ableitung des KI-Beitrags zur Wertschöpfung, notwendiger organisatorischen Strukturen und Anpassungsbedarfen von Prozessen, Entscheidungen und Verantwortlichkeiten.

KI-Security

Aufbau eines Frameworks für das Management der KI-Sicherheit über den gesamten KI-Lebenszyklus. Übersetzung etablierter Standards und regulatorischer Anforderungen in konkrete technische Security Requirements zu KI. Validierung der Wirksamkeit der Schutzmaßnahmen.

KI-Governance

Readiness-Analyse zur Prüfung und Analyse der organisatorischen Voraussetzungen. Identifikation von Handlungsfeldern und Maßnahmen für die KI-Governance in den im Unternehmen bereits etablierten Strukturen.

KI-Organisation

Nachhaltige und wertschöpfende Integration von KI in vorhandene und neu zu gestaltende Organisationsstrukturen. Einsatz eines modularen und flexibel anpassbaren Transformationsmodells für den Kulturwandel.

KI-Compliance prüfen und wirksam umsetzen – mit plenum

plenum hat eine Vielzahl von Unternehmen bei der kundenspezifischen Prüfung, Strukturierung, Planung und Umsetzung regulatorischer Anforderungen unterstützt. Mit unserem praxisbewährten Vorgehen bieten wir Ihnen eine verlässliche und pragmatische Begleitung bei der Standortbestimmung zur KI-Compliance und dem wirksamen Einsatz von KI innerhalb der gesetzten Leitplanken.