SHADOW AI

Eine Führungsaufgabe im KI-Zeitalter

Jeger, Dennis

SYMPLASSON Informationstechnik GmbH

Shadow AI: Eine Führungsaufgabe im KI-Zeitalter

Dieses Whitepaper beschreibt den Umgang mit Shadow AI in Unternehmen. Es analysiert die Risiken, die durch unkontrollierte KI-Nutzung entstehen, und erläutert, warum Shadow AI keine technische, sondern eine organisatorische und Führungsfrage ist. Ziel ist es, Entscheidungsträgern einen Rahmen zu bieten, mit dem sich KI verantwortbar integrieren, steuern und als strategische Fähigkeit entwickeln lässt.

Inhalt

Einführung — Was Shadow AI ist und warum es eine Führungsaufgabe darstellt

Unternehmen stehen heute vor einer Realität, die weniger von einzelnen Technologien geprägt wird, als von der Geschwindigkeit, mit der Mitarbeitende produktive Lücken selbst schließen. Wo Prozesse zu langsam, Werkzeuge unzureichend oder Ressourcen knapp sind, suchen sie eigenständig nach Lösungen. Künstliche Intelligenz wird dabei zunehmend zum naheliegenden Werkzeug.

Shadow AI ist Ausdruck dieser Entwicklung: Mitarbeitende nutzen KI-Werkzeuge, die nicht autorisiert, nicht kontrolliert und nicht dokumentiert sind, um Arbeit zu beschleunigen, Engpässe zu umgehen oder fehlende interne Lösungen zu kompensieren. Es handelt sich dabei weder um böswilliges Verhalten noch um Zufall – aber um eine Form der Technologienutzung, die die Governance-Grundlagen eines Unternehmens unterläuft.

Damit unterscheidet sich Shadow AI deutlich von klassischer Shadow IT. Während Shadow IT vor allem unautorisierte Systeme und Infrastrukturen umfasst, beruht Shadow AI auf unautorisierten Datenflüssen, intransparenten Modellnutzungen, nicht bewerteten Risiken und fehlender Nachvollziehbarkeit. Die Risiken entstehen weniger durch das jeweilige Tool, sondern durch das Fehlen struktureller Kontrolle: Wo Daten verarbeitet werden, welche Modelle im Einsatz sind, wie Ergebnisse zustande kommen und wie sie geschäftlich genutzt werden, bleibt unklar.

> Ökonomisch betrachtet ist Shadow AI daher kein primäres Technologieproblem, sondern ein Steuerungsproblem.

Führungsmodelle beruhen auf Sichtbarkeit, Konsistenz und Kontrolle. Shadow AI erzeugt das Gegenteil: Intransparenz, Heterogenität und eine unkontrollierte Verlagerung von Risiken. Unternehmen können ihre Daten, Entscheidungen und Abläufe nur steuern, wenn sie wissen, wo Informationen verarbeitet werden, welche Systeme beteiligt sind und wie sich Risiken quantifizieren lassen – genau diese Grundlage fehlt im Schatten.

Die Treiber von Shadow AI

Wichtig ist dabei: Shadow AI entsteht nicht, weil Mitarbeitende leichtsinnig handeln oder bewusst Regeln umgehen. Sie entsteht, weil Organisationsstrukturen sie faktisch dazu ermutigen, sich ihre Werkzeuge selbst zu suchen. Typische Treiber sind:

Interne Tools

Zu langsam oder unflexibel

Freigabeprozesse

Wirken zu schwerfällig

Operativer Druck

Steigender Leistungsdruck

KI-Werkzeuge

Versprechen sofortige Entlastung

Im operativen Kontext handeln Mitarbeitende damit rational: Sie sichern Leistungsfähigkeit und Termintreue. Im Governance-Kontext erzeugt das Unternehmen jedoch unbeabsichtigt zusätzliche Risiken.

Für Führungsetagen ist dies der entscheidende Perspektivwechsel: Shadow AI ist ein Risiko, weil sie unkontrolliert bleibt – nicht, weil KI per se gefährlich wäre. Der Unterschied zwischen verantwortungsbewusster KI-Nutzung und Shadow AI liegt nicht in der Technologie, sondern im Führungsrahmen. Unternehmen, die KI gezielt steuern, erhöhen Effizienz, Qualität und Geschwindigkeit. Unternehmen, die KI-Nutzung dem Zufall überlassen, verlieren Kontrolle, Nachweisbarkeit und Risikotransparenz.

Shadow AI als strategische Führungsaufgabe

Shadow AI ist damit kein isoliertes IT-Phänomen. Sie ist ein Thema für Geschäftsführung, Vorstand und Risikomanagement, weil zentrale Grundlagen der Unternehmensführung betroffen sind:

- Steuerbarkeit von Risiken
- Schutz von Geschäftsgeheimnissen und Know-how
- Integrität und Nachvollziehbarkeit von Entscheidungen
- Erfüllung regulatorischer und vertraglicher Pflichten
- Sicherstellung der operativen Verlässlichkeit

Kurz gesagt: Shadow AI ist „unmasked Risk"

Sie entsteht an der Schnittstelle zwischen realem Bedarf und fehlender Governance. Genau deshalb ist sie kein Randthema der IT, sondern eine Kernaufgabe der Unternehmensführung – und ein Feld, in dem Führung aktiv gestalten kann.

Shadow AI vs. Shadow IT

Shadow AI wird häufig intuitiv mit Shadow IT gleichgesetzt, doch diese Analogie führt in die Irre. Während Shadow IT unautorisierte Systeme umfasst, liegt der Kern von Shadow AI in unautorisierten Informationsprozessen: Datenflüsse, Kontextbildung, Modellinteraktionen und Entscheidungen, die ohne Sichtbarkeit stattfinden. Shadow IT beeinflusst Infrastruktur. Shadow AI beeinflusst Wissensarbeit, Entscheidungsfindung und Führungsverantwortung.

Diese Verschiebung ist entscheidend. Shadow IT entsteht dort, wo die IT-Abteilung Kontrolle verliert. Shadow AI entsteht dort, wo die Organisation die Verantwortung für Informationsverarbeitung nicht definiert hat. In beiden Fällen handelt es sich um Schattenstrukturen — doch der Schatten fällt auf unterschiedliche Ebenen. Shadow AI sitzt ungleich näher am Kerngeschäft: Produktentwicklung, Analyse, Kommunikation, Kundeninteraktion und strategische Planung.

> Hinzu kommt eine kulturelle Besonderheit. Shadow IT wurde häufig aus Ungeduld oder Bequemlichkeit geboren. Shadow AI entsteht aus Leistungsanspruch.

Mitarbeitende nutzen KI, weil sie Qualität sichern, Geschwindigkeit erhöhen oder Wissensarbeit professionalisieren wollen. Das erzeugt eine paradoxe Situation: Shadow AI ist ein Risiko, das aus Leistungsbereitschaft entsteht, nicht aus Regelvermeidung.

Damit verändert sich auch der Verantwortungsbereich. Shadow IT war eine Domäne der IT-Abteilungen. Shadow AI ist eine Domäne von Führung, Governance und Organisationsdesign. Sie betrifft die Fähigkeit eines Unternehmens, Informationen zu schützen, Entscheidungen zu erklären und Risiken steuerbar zu halten.

Im Kern zeigt die Abgrenzung: Shadow AI ist kein IT-Problem, das man durch Systemkontrolle lösen kann. Es ist ein Führungsproblem, das Sichtbarkeit, Verantwortlichkeiten und Rechenschaft verlangt.

Die Risikoarchitektur von Shadow AI

Shadow AI erzeugt keine einzelnen Risiken, sondern eine mehrdimensionale Risikostruktur. Unternehmen geraten selten durch einen isolierten Fehler in Schwierigkeiten, sondern durch das gleichzeitige Versagen mehrerer Kontrollmechanismen. Die Folge ist eine Situation, in der operative und strategische Prozesse zwar funktionieren, ihre Steuerbarkeit jedoch eingeschränkt wird.

Für Führungskräfte ist dabei weniger die Technologie selbst relevant als die Frage, welche Kontrollfunktionen fehlen, wenn KI außerhalb eines strukturierten Rahmens genutzt wird. Die folgenden Dimensionen sind dabei betriebswirtschaftlich maßgeblich:

1. Geschäftsgeheimnisse und Know how – Verlust von intellektuellen Assets

Geschäftsgeheimnisse sind nur geschützt, wenn „angemessene Schutzmaßnahmen" nachweisbar bestehen. Shadow AI unterläuft diesen Nachweis, weil unklar bleibt, welche Inhalte ein Modell verarbeitet, speichert oder temporär repliziert. Wenn vertrauliche Inhalte – etwa Quellcode, Strategiepapiere, Vertragsstrukturen oder interne Prozessbeschreibungen – in unkontrollierte KI-Systeme eingegeben werden, verliert das Unternehmen die Fähigkeit, nach außen zu belegen, dass ein Schutz existierte.

Aus Sicht der Geschäftsführung betrifft dies die wirtschaftlichen Güter des Unternehmens. Fällt der Geheimnisschutz, verliert das Unternehmen ein Asset – mit potenziellen Folgen für Wettbewerb, Vertragsfähigkeit, Bewertung und Markenwert.

2. Datenschutz- und Compliance

Verlust der Rechenschaftsfähigkeit

Shadow AI widerspricht dem Grundprinzip der Rechenschaftspflicht: Unternehmen müssen belegen können, wo Daten verarbeitet werden, zu welchem Zweck und unter welchen Bedingungen. Bei der Nutzung nicht autorisierter KI-Tools fehlen diese Antworten.

Das Risiko entsteht durch den Verlust auditfähiger Kontrolle über Verarbeitung, Speicherorte, Modellinteraktionen und Zulieferketten. Für Führungskräfte entscheidend ist die Verteidigungsfähigkeit gegenüber Aufsichtsbehörden, Kunden und Partnern.

3. Revisionsfähigkeit

Fehlende Nachvollziehbarkeit von Entscheidungen

Unternehmen müssen in der Lage sein, Entscheidungen, Datenwege und Prozesse nachvollziehen zu können. Shadow AI verhindert dies vollständig. Es gibt keine Logs, keine Protokolle, keine systematisch dokumentierten Prompt-Inhalte. Damit verliert das Unternehmen die Fähigkeit, Vorfälle zu untersuchen, Verantwortlichkeiten zu klären oder Fehlerquellen zu identifizieren.

Für die Unternehmensführung ist das ein strukturelles Risiko: Was man nicht nachvollziehen kann, kann man weder steuern noch verteidigen.

4. Modell-Leakage & IP-Exposure

Verlust von Kontrolle über Wissensbestände

Viele KI-Systeme speichern Eingaben zumindest temporär zur Modelloptimierung. Andere replizieren Informationen intern, ohne dass der Nutzer dies erkennen kann. Shadow AI kann daher dazu führen, dass interne Inhalte in Systemen landen, die nicht unter der Kontrolle des Unternehmens stehen. In einem regulierten oder wissensintensiven Umfeld – Technologie, Finance, Beratung, Produktion – stellt dies ein massives strategisches Risiko dar.

Für Führungskräfte heißt das: Die Organisation verliert Kontrolle darüber, welches Wissen außerhalb des Unternehmens präsent ist und in welcher Form.

5. Haftungsrisiken

Fehlerhafte KI-Ausgaben als geschäftliche Entscheidungsvorlage

Wenn Mitarbeitende KI-Ergebnisse ohne Kontrolle in Kundenkommunikation, Angebote, Analysen oder technische Bewertungen übernehmen, entsteht eine unmittelbare Haftungsdimension. Shadow AI führt dazu, dass Entscheidungen auf Outputs basieren, deren Herkunft, Berechnungsgrundlagen und Zuverlässigkeit unbekannt sind. Im Streitfall trägt das Unternehmen die Verantwortung – nicht das Tool und nicht der Mitarbeiter.

Führungskräfte stehen damit im Zentrum des Risikos, weil fehlerhafte Entscheidungen, die auf intransparenten KI-Prozessen beruhen, nicht entlastbar sind.

6. Sicherheitslage und Angriffsfläche

Inoffizielle Software und unbekannte Datenwege

Shadow AI umfasst häufig Tools und Skripte, die außerhalb jeder Sicherheitsprüfung genutzt werden: Browser-Erweiterungen, lokale Modelle, inoffizielle APIs oder cloudbasierte KI-Services ohne Sicherheitszertifikate. Diese Tools können Daten auslesen, Token abgreifen, Dateien verändern oder Verbindungen aufbauen, die das Unternehmen nicht überwacht.

Für die Führung bedeutet das: Es geht nicht um „Cyberangriffe", sondern um operative Unkalkulierbarkeit. Ein Unternehmen, das nicht weiß, welche KI-Systeme im Hintergrund laufen, kann seine Sicherheitslage nicht bewerten – geschweige denn steuern.

Praxisfälle: Wie Shadow AI Unternehmen real trifft

Shadow AI entfaltet seine Wirkung in Situationen, in denen operative Anforderungen schneller wachsen als die bestehenden Governance-Strukturen. Beschäftigte suchen Lösungen, Abläufe beschleunigen sich, und Informationen gelangen in Systeme, die außerhalb der eigenen Steuerung liegen. Sichtbar wird das erst, wenn Organisationen im Rückblick feststellen, dass Kontrolle, Nachweisbarkeit oder Verantwortlichkeit fehlten.

Drei Falltypen verdeutlichen die Mechanismen:

Falltyp 1 – Wissen in externen Modellen (Beispiel Samsung)

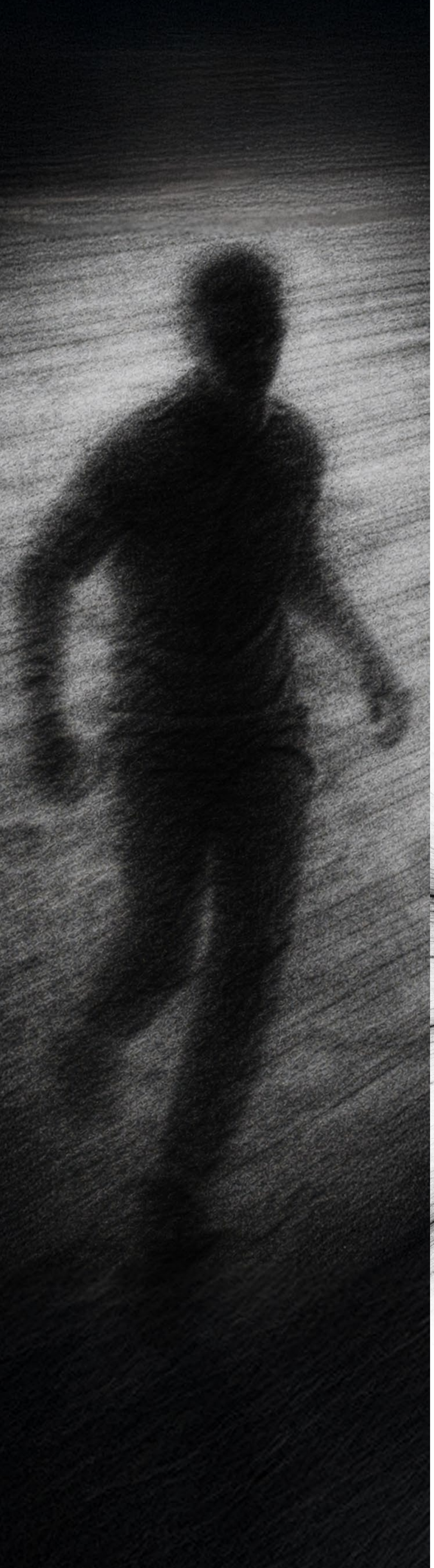
Ein prominentes Beispiel dafür ist der Fall Samsung aus dem Jahr 2023. Mehrere Entwickler nutzten öffentlich zugängliche KI-Dienste, um Quellcode analysieren zu lassen und Probleme im Entwicklungsprozess schneller zu lösen. Was aus ihrer Sicht ein pragmatischer Effizienzgewinn war, bedeutete aus Unternehmenssicht etwas völlig anderes: proprietärer Code und interne Inhalte liefen über ein externes System, das nicht unter der Kontrolle von Samsung stand. Niemand konnte im Nachhinein zuverlässig sagen, in welchem Umfang Unternehmenswissen in die Modelle eingeflossen war oder ob dieses Wissen später in anderer Form wieder auftauchen könnte. Der Vorfall war kein Hackerangriff, keine Malware, kein klassischer Sicherheitsbruch – es war schlicht improvisierte KI-Nutzung ohne Governance. Genau das macht Shadow AI so gefährlich: Ein einzelner, gut gemeinter Arbeitsschritt kann aus Sicht der Geschäftsführung zu einem strukturellen IP-Risiko werden.

Falltyp 2 – Regulierte Daten und Rechenschaftspflichten (Beispiel Gesundheitswesen)

Ein zweiter Typus zeigt sich in regulierten Branchen, etwa im Gesundheitswesen. In Großbritannien wurde dokumentiert, wie Mitarbeitende des National Health Service KI-Tools nutzten, um medizinische Informationen zu strukturieren und Formulierungen für Patientenkommunikation zu verbessern. In der Praxis bedeutete das: Gesundheitsdaten flossen in Systeme, zu denen weder die Datenschutzbeauftragten noch die IT eine klare Sicht hatten. Die Organisation konnte gegenüber Aufsichtsbehörden nicht mehr plausibel nachweisen, wo welche Daten in welcher Form verarbeitet wurden. Auch hier war das zentrale Problem nicht „böse KI", sondern der Verlust der Rechenschaftsfähigkeit. Die Verantwortlichen hatten keine vollständige Kontrolle mehr über ihre eigenen Datenflüsse – und genau das ist in einem regulierten Umfeld ein unmittelbares Geschäfts- und Haftungsrisiko.

Falltyp 3 – Entscheidungsauswirkungen im Kontakt mit Kunden (Beispiel Air Canada)

Eine weitere Facette wurde in einem Fall rund um Air Canada sichtbar. Formal kein Schattenfall, aber dasselbe Governance-Signal Dort wurde eine KI im Kundenservice eingesetzt, um Anfragen zu beantworten. Die KI formulierte selbstsicher eine Kulanzregel, die es so nie gegeben hatte – inklusive vermeintlicher Bedingungen für Erstattungen. Mitarbeitende übernahmen diese Information, der Kunde berief sich darauf und der Fall landete vor Gericht. Das Gericht entschied klar: Das Unternehmen haftet für die Auskunft, auch wenn sie von einer KI erzeugt wurde. Aus Managementsicht ist das ein Wendepunkt: Sobald KI-Ausgaben ungeprüft in die operative Kommunikation einfließen, wird jede Falschaussage zu einem potenziellen Haftungsfall. Shadow AI verstärkt dieses Risiko, weil unkontrollierte, inoffizielle KI-Tools oft genau dort genutzt werden, wo es „mal schnell gehen muss", ohne dass Qualitätssicherung oder Rechtsprüfung greifen.



Technische Träger - Browser-Erweiterungen und inoffizielle Integrationen

Technisch besonders heikel sind Fälle, in denen Shadow AI über Browser-Erweiterungen oder inoffizielle Integrationen ins Unternehmen getragen wird. Mehrere Security-Analysen haben gezeigt, dass populäre ChatGPT-Plugins und ähnliche Erweiterungen Zugriffe auf Browser-Tabs, Zwischenablage, Cookies oder Session-Daten hatten – also genau auf die Bereiche, in denen sich Zugangsdaten, interne Links, vertrauliche Kommunikation oder Webportale der Unternehmen befinden. Beschäftigte installierten diese Erweiterungen, um „KI überall nutzen zu können", tatsächlich holten sie damit aber eine nicht geprüfte Softwareebene in kritische Arbeitskontexte. Aus Sicht der Unternehmensleitung ist das eine stille Erweiterung der Angriffsfläche: Es existieren Kommunikations- und Datenschnittstellen, die weder inventarisiert, noch getestet, noch überwacht sind. Klassische Sicherheitsmechanismen greifen dort nur begrenzt, weil die Interaktion über scheinbar harmlose Texteingaben läuft.

> Allen diesen Fällen ist eines gemeinsam: Shadow AI macht Risiken unsichtbar, bis sie sich in einem Vorfall manifestieren. Es gibt keinen zentralen Verantwortlichen, keine definierte Plattform, keine klare Prozessbeschreibung – und damit auch keine echte Verteidigungsstrategie.

Umgang mit Shadow AI: Verantwortung und Governance

Genau an diesem Punkt setzt ein professioneller Umgang mit KI an: Nicht bei Verboten, sondern bei Transparenz, Steuerbarkeit und der bewussten Entscheidung, KI aus der Schattenzone in ein gestaltetes, verantwortbares Betriebsmodell zu holen. Die Frage für Führungskräfte lautet daher nicht mehr, ob KI im Unternehmen eingesetzt wird – das geschieht längst. Die Frage lautet, ob sie bereit sind, Verantwortung für diesen Einsatz zu übernehmen und die Strukturen zu schaffen, die zwischen produktivem Nutzen und strukturellem Risiko entscheiden.

Nicht der Einsatz von KI als solcher ist gefährlich, sondern der Zustand, in dem KI bereits flächig genutzt wird, während die Organisation so tut, als sei das Thema noch „in der Zukunft".

Warum Mitarbeitende Shadow AI nutzen: Der organisatorische Blindspot

In Gesprächen mit Führungskräften zeigt sich häufig ein wiederkehrendes Missverständnis: die Annahme, Mitarbeitende würden KI primär nutzen, um Abkürzungen zu nehmen oder Verantwortung zu vermeiden. In der Praxis geschieht das selten. Tatsächlich ist in der Regel das Gegenteil der Fall. Mitarbeitende nutzen KI, weil sie Leistung bringen wollen – nicht, weil sie sie umgehen wollen. Sie greifen zu Werkzeugen, die ihnen helfen, Fristen einzuhalten, Qualität zu sichern oder komplexe Aufgaben zu strukturieren.

Shadow AI entsteht damit an einer anderen Stelle als häufig angenommen: Sie entsteht im produktiven Kern des Unternehmens. Dort, wo operative Anforderungen schneller sind als die Werkzeuge und Prozesse, die sie tragen sollen.

Kultureller Faktor

Viele Mitarbeitende nutzen KI bewusst im Verborgenen, weil sie nicht riskieren wollen, als unqualifiziert oder überfordert zu wirken. In klassischen Leistungskulturen gilt es als problematisch, wenn man ein Werkzeug braucht, um „gute Arbeit" zu leisten.

Verlust der Transparenz

KI wird also verdeckt genutzt, und genau dadurch verliert das Unternehmen das Wichtigste: Transparenz. Shadow AI entsteht dann nicht aus Böswilligkeit, sondern aus der Angst vor Urteil.

Innovation braucht Offenheit

Eine Organisation, die Innovation will, darf niemals eine Kultur fördern, die Offenheit bestraft.

Technische Faktoren

Auch technische Faktoren spielen eine Rolle. Viele Unternehmen implementieren restriktive Sicherheitsmechanismen, die KI-Zugriffe blockieren oder einschränken. Diese Maßnahmen sind gut gemeint, führen aber häufig zu einem paradoxen Effekt: Je stärker der offizielle Zugang erschwert wird, desto eher nutzen Mitarbeitende private Endgeräte, inoffizielle Browser, alternative Tools oder mobile Apps, um KI trotzdem einzusetzen. Die Kontrolle geht dabei vollständig verloren. Was eigentlich Schutz erzeugen sollte, schafft ungewollt Schattenstrukturen, die deutlich riskanter sind als ein kontrollierter, sicherer KI-Einsatz.

> **Der zentrale Punkt ist: Shadow AI ist immer ein Organisationsproblem.** Menschen nutzen die Werkzeuge, die ihnen produktiv helfen. Wenn das Unternehmen keine funktionierenden KI-Prozesse anbietet, wird sich die Nutzung unweigerlich in die Schatten verschieben.

Für die Geschäftsführung bedeutet das, dass der Versuch, Shadow AI durch Verbote zu eliminieren, nicht funktionieren kann. Verbote verschieben Nutzung lediglich an verborgene Orte – und erhöhen damit Risiko, Haftung und operative Intransparenz. Das Einzige, was langfristig wirkt, ist die Gestaltung eines Rahmens, in dem Mitarbeitende KI offen, sicher und kontrolliert nutzen können.

Shadow AI ist damit ein Spiegel der Organisation. Sie zeigt, wo Prozesse zu langsam sind, wo Werkzeuge fehlen, wo Führung unklare Signale sendet und wo Verantwortlichkeit nicht klar definiert ist. Ein Unternehmen, das Shadow AI ernsthaft reduzieren will, muss nicht härter kontrollieren, sondern besser führen. In diesem Sinne ist Shadow AI eine Diagnose: Sie zeigt, wo das Unternehmen nachsteuern muss, bevor es Schaden nimmt.

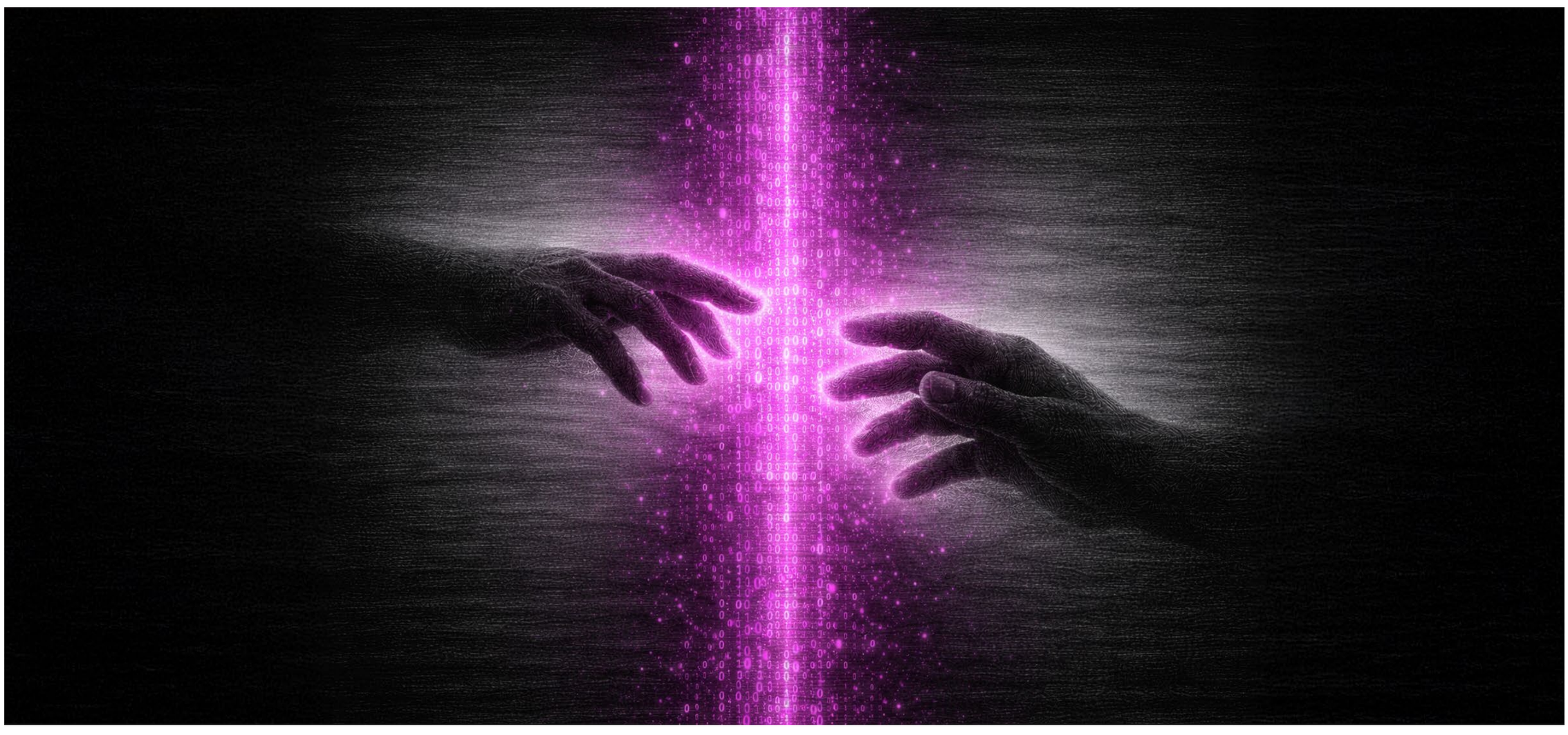
Der Forbidden-Fruit-Effekt: *Sobald Unternehmen KI verbieten, steigt die Schattennutzung signifikant.*

Wenn Führung versucht, Shadow AI mit Verboten, Warnungen oder erhobenem Zeigefinger zu lösen, passiert immer dasselbe: Mitarbeitende werden inoffiziell kreativer. Und der Schatten wird größer.

Die falsche Grenze zwischen Daten und Information

In vielen Organisationen herrscht die Annahme, Shadow-AI-Risiken ließen sich vermeiden, indem lediglich keine personenbezogenen Daten eingegeben werden. Diese Sicht ist verbreitet, aber verkürzt. KI-Modelle erzeugen Risiken nicht allein durch Speicherung von Eingaben, sondern durch Ableitungen, Rekonstruktionen und Kontextbildung.

AI verschiebt Risiken aus dem Bereich der Datenspeicherung in den Bereich der Informationsrekonstruktion. Modelle können aus harmlos wirkenden Informationen Muster ableiten, Rollen zuordnen oder implizite Zusammenhänge herstellen. Dadurch entstehen Informationen, die organisatorisch und geschäftlich relevant sind, ohne dass sensible Daten im engeren Sinne verarbeitet wurden. Die Unsicherheit entsteht in diesem Fall nicht durch einen Datenpunkt, sondern durch die Fähigkeit des Modells, Kontext zu erschließen.



Juristische Komponente

Rechenschaftspflichten betreffen nicht nur die Daten, die eingegeben werden, sondern auch die Informationen, die daraus entstehen.

Strategische Komponente

Know-how und Absichten können sichtbar werden, ohne dass sensible Daten direkt eingegeben wurden.

Shadow AI unterläuft damit die intuitive Grenzziehung zwischen sensiblem Input und harmloser Nutzung.

Unternehmen müssen festlegen, welche Arten von Informationen KI sehen dürfen und welche nicht. Nicht jede Information ist schützenswert, aber einige sind geschäftskritisch — Geschäftsgeheimnisse, Prozesswissen, Verhandlungspositionen. Die Trennlinie verläuft nicht entlang personenbezogener Daten, sondern entlang geschäftlicher Auswirkung. Das schützt nicht nur juristisch, sondern auch strategisch.

Modellverhalten und Risikofaktoren

Ein weiterer Aspekt betrifft das Modellverhalten selbst. Viele KI-Systeme nutzen Eingaben nicht nur zur Beantwortung von Anfragen, sondern zur Optimierung oder zum Training. Dadurch können Inhalte in Modelle gelangen, in denen sie nicht mehr kontrollierbar sind. Der Risikofaktor entsteht durch die Möglichkeit, dass sich Informationen im Modell reproduzieren oder in anderer Form wieder auftauchen. Das betrifft Geschäftsgeheimnisse ebenso wie Prozesswissen, strategische Absichten oder Verhandlungspositionen.

Unternehmen müssen entscheiden, welche Modelle sie öffnen, welche Informationen sie zulassen und welche Bedingungen sie technisch oder vertraglich absichern. Steuerung ersetzt an dieser Stelle die klassische Logik aus Erlaubnis und Verbot. Führung entscheidet nicht, ob KI genutzt wird, sondern unter welchen Bedingungen sie verantwortbar genutzt werden kann.

Wie Unternehmen Shadow AI kontrollieren – ohne Innovation zu blockieren

Der Einsatz von KI entwickelt sich aktuell schneller als jede interne Governance-Struktur. Die meisten KI-Anwendungen werden nicht aktiv eingeführt, sondern „passieren einfach" – besonders dort, wo operative Prozesse eng getaktet sind.. Mitarbeitende probieren Tools aus, suchen Abkürzungen, automatisieren Abläufe. Das ist menschlich, effizient und oft sogar sinnvoll. Doch ohne Rahmen entsteht ein Paradox: Produktivitätsgewinn durch Intransparenz – und Risiko durch Komfort.

> Die Aufgabe liegt nun darin zu lernen,KI wie jede andere produktive Ressource zu integrieren:

Handlungsempfehlungen für Geschäftsführer, CIOs und IT-Leiter

01

Formulieren Sie ein klares Führungsstatement

Bevor Sie Regeln erlassen

02

Geben Sie den Mitarbeitenden Sicherheit

Nicht Verbote

03

Definieren Sie Grundprinzipien

Kein komplexes Regelwerk

04

Etablieren Sie einen Verantwortungsanker

Eine Stelle, die die Fäden hält

05

Starten Sie mit einem Pilotbereich

Mit klarer Beobachtung

06

Nutzen Sie Reflexion

Als Führungsinstrument

Detaillierte Handlungsempfehlungen

1. Formulieren Sie ein klares Führungsstatement – bevor Sie Regeln erlassen

Regeln werden nur akzeptiert, wenn klar ist, wozu sie dienen. Deshalb beginnt Governance nicht mit Prozessen, sondern mit Haltung. Ein einfaches, präzises Statement der Geschäftsleitung schafft Orientierung:

> „KI soll uns unterstützen. Wir wollen sie bewusst nutzen, nicht zufällig."

Das erzeugt drei Effekte gleichzeitig: Legitimation, Richtung und Verantwortlichkeit. Mitarbeitende wissen, dass KI nicht heimlich genutzt werden muss und dass Führung den Rahmen setzt.

2. Geben Sie den Mitarbeitenden Sicherheit, nicht Verbote

Die größte Unsicherheit der Mitarbeitenden besteht selten darin, gegen Regeln zu verstoßen, sondern darin, Fehler zu machen. Viele Transformationsvorhaben scheitern daran, dass Unternehmen KI-Nutzung einschränken, um Risiken zu reduzieren. Das Ergebnis ist jedoch das Gegenteil: Schattenräume und Improvisation. Führung muss daher Erlaubnis mit Rahmen kombinieren: KI darf genutzt werden — und zwar sichtbar, reflektiert und verantwortet. Der Effekt ist unmittelbar spürbar. Aus Versteckspiel wird Mitarbeit, aus Unsicherheit wird Verantwortlichkeit.

3. Definieren Sie ein erstes Set von Grundprinzipien – kein Regelwerk

In der Anfangsphase reicht ein Mini-Rahmen aus den wesentlichen Grundgedanken:

- KI ersetzt keine Menschen – sie unterstützt Entscheidungen.
- Ergebnisse müssen überprüfbar und plausibel sein.
- Sensible Daten werden nie direkt eingegeben.
- Entscheidungen bleiben in menschlicher Verantwortung.

Solche Prinzipien ermöglichen einen schnellen Einstieg, ohne Prozessdruck oder Overhead.

4. Etablieren Sie einen Verantwortungsanker – eine Stelle, die die Fäden hält

KI braucht eine Stelle, in der Beobachtungen, Risiken und Erfahrungen zusammenlaufen. Ohne Verantwortungsanker entsteht Wildwuchs; mit ihm Steuerbarkeit. Ob diese Funktion im CIO-Bereich, in der IT-Sicherheit, im Digital Office oder direkt in der Geschäftsführung liegt, ist zweitrangig. Entscheidend ist, dass sie Rückhalt besitzt und nicht rein technisch verortet wird.

5. Starten Sie mit einem kleinen Pilotbereich – aber mit klarer Beobachtung

KI-Einführung funktioniert nicht unter Laborbedingungen. Sie muss dort erprobt werden, wo reale Abläufe, fachliche Entscheidungen und Kundeninteraktionen zusammenfallen. Ein Pilotbereich eignet sich dafür besser als jedes Testumfeld, weil er den operativen Druck, die tatsächlichen Fragen und die notwendigen Abwägungen sichtbar macht.

Damit ein Pilot trägt, benötigt er einen definierten Rahmen. Dazu gehören ein Modell, dessen Nutzungskontext klar ist, Regeln für die Dokumentation von Erfahrungen sowie ein Rückkanal an die Verantwortlichen. Dadurch entsteht ein Lernsystem: Die Organisation versteht besser, wie KI wirkt, wo Unsicherheiten auftauchen, wie Entscheidungsprozesse beeinflusst werden und welche Anforderungen aus der Praxis an Governance gestellt werden.

Wichtig ist: Ein Pilot dient nicht dazu, Erfolge zu demonstrieren. Er dient dazu, Erkenntnisse zu gewinnen. Die Organisation lernt, bevor sie skaliert. Und Führung lernt, bevor sie entscheidet.

6. Nutzen Sie Reflexion als Führungsinstrument

KI entfaltet ihren Wert nicht automatisch durch Nutzung, sondern durch Reflexion. Erst im Austausch darüber, wie Entscheidungen beeinflusst wurden, welche Unsicherheiten entstanden und welche Risiken sichtbar wurden, entsteht ein Verständnis dafür, wie KI in der Organisation wirkt. Diese Reflexion ist kein technisches Element, sondern ein Führungsinstrument.

Solche Gespräche sind selten operativ, aber hochwirksam. Sie stellen Fragen, die im Tagesgeschäft nicht gestellt werden:

- Was hat funktioniert?
- Was war unklar?
- Welche Entscheidungen wurden durch KI verändert?
- Welche Regeln haben gefehlt oder waren zu vage?

> Aus diesen Beobachtungen entsteht keine Kontrolle, sondern Erkenntnis.
> Diese Gespräche bauen etwas auf, das in vielen Organisationen fehlt: eine gemeinsame Denksprache über KI. Nur damit wird KI langfristig steuerbar.

Fazit – Die neue Führungsaufgabe im KI-Zeitalter

KI verändert das Fundament, auf dem Organisationen Informationen bewerten, Prioritäten setzen und Entscheidungen treffen. Damit verändert sie zwangsläufig die Aufgabe von Führung.

Früher war Führung vor allem die Kunst, Ziele zu setzen, Ressourcen zu verteilen und operative Stabilität sicherzustellen. Mit dem Aufkommen von KI verschiebt sich diese Rolle: Führung wird zur Gestalterin von Kontext, zur Hüterin von Verantwortlichkeiten und zur Architektin von Entscheidungsfähigkeit.

Die KI bringt nicht nur Potenziale – sie bringt eine neue Realität: Entscheidungen entstehen schneller, in größerem Umfang und teilweise automatisiert. Die Frage ist nicht mehr, ob eine Organisation KI nutzen wird, sondern wie sehr sie die Kontrolle über ihre Entscheidungsqualität behält.

Führungskräfte stehen deshalb vor einer historischen Wahl: Lassen wir KI als Schattenkraft agieren – unkoordiniert, unkontrolliert, voller Risiken? Oder gestalten wir KI als strategische Fähigkeit – sichtbar, verantwortbar, wertschöpfend?

KI nicht das Ende der Unternehmensführung, sondern ihre vielleicht größte Chance. Die Organisation, die diese Wahl bewusst trifft, gewinnt Stabilität. Die Organisation, die sie ignoriert, verliert sie.

Shadow AI:

Eine Führungsaufgabe im KI-Zeitalter

Whitepaper

Autor: Dennis Jeger

Kontakt: djeger@symplasson.de

Version: 1.0 – Januar 2026

Unsere Kontaktdaten

SYMPLASSON Informationstechnik GmbH

Holstenstraße 205

22765 Hamburg

Tel. +49 40 533 071-0

E-Mail: info@symplasson.de

Web: www.symplasson.de

Dieses Dokument dient ausschließlich Informationszwecken und stellt keine Rechtsberatung dar. Alle Inhalte wurden sorgfältig erstellt, ersetzen jedoch keine individuelle Prüfung im Einzelfall. Angaben nach bestem Wissen, ohne Gewähr. Änderungen vorbehalten.