STRATEGIEPAPIER 04

Schatten-KI als Chance: *Ihre besten KI-Experten kennt die IT nicht.*

Wenn Mitarbeitende KI-Tools nutzen, ohne dass die IT es freigegeben hat, ist das fast nie böswillig – aber oft ein Verstoß gegen interne Regeln, den man intelligent heilen muss. Und immer ein Signal. Wer es richtig liest, findet die echten Anwendungsfälle, die besten internen Experten und den schnellsten Weg zu einer KI-Strategie, die wirklich getragen wird.

Christian Teutrine · keinwenn
KI-Manager / KI-Anwendungsberater (IHK, 2026)
keinwenn.de · info@keinwenn.de

Was Schatten-KI wirklich ist – und was die Zahlen sagen

Schatten-KI bezeichnet die Nutzung von KI-Werkzeugen im beruflichen Kontext ohne Wissen oder Genehmigung der IT- oder Datenschutzabteilung. ChatGPT für die Angebotserstellung, ein KI-Tool zur Bildbearbeitung, ein Übersetzungsdienst mit KI-Unterstützung – all das passiert täglich in fast jedem Unternehmen. Oft ohne böse Absicht. Oft ohne das Bewusstsein, dass es überhaupt ein Problem sein könnte.

Das Standardnarrativ lautet: Schatten-KI ist gefährlich. Datenschutzverstöße, unkontrollierter Datenabfluss, Haftungsrisiken. All das stimmt – und wird weiter unten klar benannt. Aber wer nur das sieht, verpasst die andere Seite.

Die Zahlen sprechen eine klare Sprache

Schatten-KI ist kein Randphänomen. Laut einer Studie von Software AG (1.500 Fachkräfte in sieben Ländern) nutzen bereits 50 Prozent der Mitarbeitenden nicht genehmigte KI-Tools – und 46 Prozent würden damit weitermachen, selbst wenn es explizit verboten wäre.[1] Der Microsoft/LinkedIn Work Trend Index 2024 (31.000 Befragte weltweit) zeigt: 75 Prozent der Wissensarbeiter nutzen KI, 78 Prozent davon mit eigenen, privaten Accounts – sogenanntes BYOAI (Bring Your Own AI).[2] Und eine IBM-Studie belegt, dass zwar 80 Prozent KI nutzen – aber nur 22 Prozent ausschließlich mit vom Unternehmen bereitgestellten Tools.[3]

Analysten von Gartner schätzen, dass bis 2027 bereits 75 Prozent aller Mitarbeitenden Schatten-KI nutzen werden – gegenüber 41 Prozent im Jahr 2022.[4] Das Thema wird nicht kleiner. Es wird größer.

> *„Schatten-KI entsteht selten aus Böswilligkeit. Sie entsteht, weil ein echter Bedarf noch keine offizielle Antwort gefunden hat."*

Was das Signal bedeutet

Wenn Mitarbeitende eigenständig KI-Tools suchen und nutzen, sagen sie damit etwas Klares: Es gibt einen Bedarf, den das Unternehmen offiziell nicht bedient. Dieser Bedarf ist real, dringlich genug zum Handeln – und jemand hat bereits eine Lösung gefunden, die funktioniert.

- Wo Schatten-KI auftaucht, gibt es echten Leidensdruck.
- Die Nutzenden haben bereits Erfahrung – sie sind interne Experten.
- Es existiert schon Evidenz, was funktioniert und was nicht.
- Die Bereitschaft zur Veränderung ist vorhanden – sie muss nur kanalisiert werden.

[1] Software AG (2024). Shadow AI Report. 1.500 Fachkräfte in sieben Ländern. 50 % nutzen nicht genehmigte KI-Tools; 46 % würden dies auch bei Verbot fortsetzen.

[2] Microsoft / LinkedIn (2024). Work Trend Index. 31.000 Befragte weltweit. 75 % der Wissensarbeiter nutzen KI; 78 % mit eigenen Accounts (BYOAI).

[3] IBM (2024). Rising AI Adoption – Shadow AI Risks. 80 % nutzen KI; nur 22 % ausschließlich mit Unternehmens-Tools.
[4] Gartner (2025). 75 % der Mitarbeitenden werden bis 2027 Schatten-KI nutzen (2022: 41 %).

Von Schatten-KI zu gelebter KI-Strategie: drei Phasen

Der Weg von unkontrollierter zu gesteuerter KI-Nutzung folgt einer klaren Logik. Wer die Phasen überspringt, scheitert – entweder weil er zu früh reguliert oder weil er zu lange wartet.

Phase 1: Verstehen, bevor man handelt

Bevor irgendjemand etwas verbietet oder einführt: hinschauen. Wer nutzt welche Tools, wie oft, wofür? Nicht als Kontrolle, sondern als ehrliche Bestandsaufnahme. Informelle Gespräche, kurze Interviews in den Abteilungen, manchmal reicht eine offene Frage in der nächsten Teamrunde. Gartner empfiehlt, bestehende Werkzeuge wie Web-Proxys und Log-Systeme zu nutzen, um herauszufinden, was Mitarbeitende bereits tun.[5]

Phase 2: Legalisieren statt verbieten

Die wirksamste Strategie – und die, die am häufigsten vergessen wird. Wer als erste Reaktion auf Schatten-KI ein Verbot ausspricht, treibt die Nutzung weiter in den Untergrund. Sie verschwindet nicht – sie wird unsichtbar.

1. Amnestie ausrufen

Explizit kommunizieren, dass bisherige Nutzung nicht bestraft wird. Wer Angst vor Konsequenzen hat, taucht ab. Wer sich sicher fühlt, kommt ans Licht – mit seinem Wissen.

2. Pilotnutzer einbinden

Die Mitarbeitenden, die KI schon erfolgreich nutzen, kennen den Alltag. Wer sie frühzeitig einbindet – etwa in einem kurzen internen Austauschformat – nutzt vorhandenes Wissen und erhöht die Chance, dass neue Spielregeln akzeptiert werden.

3. Einfache offizielle Alternativen bereitstellen

Schatten-KI entsteht oft, weil der offizielle Weg zu langsam oder zu kompliziert ist. Wenn ein genehmigtes Tool genauso einfach zu nutzen ist wie die inoffizielle Alternative, verschwindet der Schatten von selbst.[6]

Phase 3: Strukturen aufbauen, die Nutzung ermöglichen

Einmal legalisiert, braucht die Nutzung einen Rahmen, der Orientierung gibt ohne zu lähmen. Dazu gehören: ein prägnanter interner Leitfaden, datenschutzkonforme Umgebungen, ein Feedbackkanal für neue Anwendungsfälle und gezielte Kompetenzentwicklung.

[5] Gartner Security and Risk Management Summit (2025). Empfehlung: Analyse bestehender Shadow-AI-Nutzung als Grundlage der KI-Steuerung.

[6] IBM (2024): 60 % der Mitarbeitenden: praxisorientiertes Training würde ihren KI-Einsatz verbessern.

Ermöglichen und Begrenzen – beides gehört zusammen

Wer Schatten-KI legalisieren und kanalisieren will, muss gleichzeitig klare Grenzen ziehen. Ermöglichen ohne Grenzen ist keine Strategie – es ist Naivität. Die Frage ist nur: Wie kommuniziert man Grenzen so, dass sie wirken und nicht lähmen?

Prinzipien statt Paragraphen

Verbotslisten werden nie vollständig sein. Technologie entwickelt sich schneller als Richtlinien. Wirksamer sind drei einfache Leitfragen, die jeder selbst anwenden kann:

- Würde ich das meinem Kunden erzählen? Wenn nicht, gehören diese Daten nicht in ein externes KI-System.
- Wem gehören diese Informationen? Eigene Gedanken, öffentliche Informationen – meist unbedenklich. Daten über Kunden, Mitarbeitende oder Partner – nicht ohne geprüfte, datenschutzkonforme Umgebung.
- Kann ich für das Ergebnis einstehen? KI-Ausgaben sind Entwürfe, keine Wahrheit. Wer ein KI-Ergebnis weitergibt, trägt die Verantwortung dafür.

ROTE LINIEN – IMMER VERBOTEN

- Personenbezogene Daten in externe, nicht geprüfte KI-Systeme eingeben.
- Kundendaten, Vertragsdetails oder Informationen zu Fusionen und Übernahmen (M&A) verwenden.
- Zugangsdaten, Passwörter oder sicherheitsrelevante Informationen eingeben.
- KI-Ausgaben als eigene Arbeit ausgeben ohne inhaltliche Prüfung.
- Nicht freigegebene Systeme für geschäftskritische Entscheidungen nutzen.
- KI-generierte Inhalte (Texte, Code, Bilder) verwenden ohne Prüfung der Urheberrechtslage.
- KI-Ausgaben ungekennzeichnet als Tatsache weitergeben – KI erfindet plausibel klingende Fakten (sogenannte Halluzinationen).

> *„Prinzipien geben Orientierung im Graubereich. Rote Linien schaffen Klarheit dort, wo es keine Graubereiche geben darf.“*

Was ein Mindestrahmen konkret braucht

Wer Schatten-KI legalisieren will, bekommt sofort die Frage: Wer entscheidet das? Nach welchen Kriterien? Und was passiert, wenn etwas schiefgeht? Der folgende Rahmen ist bewusst leichtgewichtig gehalten.

Wer entscheidet über Tool-Freigaben?

Empfehlung: drei Rollen, klare Zuständigkeit.

- IT / Informationssicherheit – prüft technische Risiken: Wo werden Daten verarbeitet? Wer hat Zugriff? Gibt es eine Vertragsgrundlage (Auftragsverarbeitung nach DSGVO)?
- Datenschutzbeauftragte/r – prüft rechtliche Anforderungen: Welche Datenkategorien sind betroffen? Findet eine Datenübertragung ins Ausland statt?
- KI-Koordinator/in im Fachbereich – erster Ansprechpunkt für Mitarbeitende, sammelt neue Bedarfe, gibt Ersteinschätzung vor formaler Prüfung.

Vier Datenstufen – welches Tool ist erlaubt?

- Stufe 1 – Öffentlich: Informationen, die schon veröffentlicht sind. Freie KI-Tools erlaubt.
- Stufe 2 – Intern: Nicht vertraulich, aber nicht für externe Weitergabe. Nur freigegebene Tools mit Datenschutzvertrag (AVV).
- Stufe 3 – Vertraulich: Geschäftsgeheimnisse, Projektdetails, Personaldaten. Nur geprüfte Unternehmensumgebung, kein Training auf Daten.
- Stufe 4 – Streng vertraulich: Kundendaten, M&A, Compliance-relevante Informationen. Keine KI-Nutzung ohne explizite Einzelfreigabe.

Drei leichtgewichtige Kontrollmechanismen

- Tool-Register: Eine kurze Liste freigegebener KI-Tools mit erlaubten Nutzungsfällen und Datenstufen-Beschränkungen. Kein 40-seitiges Dokument – eine Seite genügt.
- Unternehmens-Account statt Privat-Account: Viele Tools (ChatGPT, Copilot, Claude) bieten Unternehmensversionen an, bei denen Eingaben nicht für das Training genutzt werden.
- Meldepflicht bei Unsicherheit: Wer nicht weiß, ob ein Tool für einen Anwendungsfall erlaubt ist, fragt – ohne Angst vor Konsequenzen.

Der eigentliche Kern: Kulturwandel

Schatten-KI in offizielle KI-Nutzung zu überführen ist keine technische oder rechtliche Aufgabe. Es ist eine Führungsaufgabe. Die Frage, die dahintersteht, lautet nicht: Welches Tool genehmigen wir? Sondern: Was für eine Lernkultur wollen wir sein?

Unternehmen, die Schatten-KI als Signal statt als Problem verstehen, verschaffen sich einen messbaren Vorteil: Sie wissen früher, welche Anwendungsfälle wirklich tragen, haben interne Experten bereits identifiziert und können ihre KI-Strategie auf echter Erfahrung aufbauen statt auf Annahmen.

Was Unternehmen mit gesunder KI-Kultur gemeinsam haben

- Sie bestrafen Neugier nicht – sie kanalisieren sie.
- Sie setzen auf Transparenz statt auf Kontrolle als erstes Mittel.
- Sie machen aus Pilotnutzern interne Experten, nicht aus internen Regelbrechern Sündenböcke.
- Sie aktualisieren ihre Spielregeln, wenn sich die Technologie ändert.
- Sie verstehen KI-Kompetenz als Teil der beruflichen Entwicklung.

> *„Der schnellste Weg zu einer KI-Strategie, die wirklich getragen wird, führt über die Menschen, die KI bereits nutzen – nicht an ihnen vorbei."*

Start-Playbook: Erste 30 Tage

Schatten-KI lässt sich nicht per Rundmail lösen. Sie braucht einen strukturierten Prozess, der schnell sichtbare Ergebnisse liefert und das Vertrauen der Mitarbeitenden nicht verspielt.

A – VERSTEHEN (WOCHE 1–2)

Ziel: herausfinden, was bereits passiert

- 5–10 informelle Gespräche in verschiedenen Bereichen: Welche KI-Tools werden genutzt, wofür, wie oft?
- Keine Sanktionen, keine Protokolle – ehrliche Bestandsaufnahme als Vertrauenssignal.
- Ergebnis: kurze Liste realer Anwendungsfälle und der Tools, die Mitarbeitende selbst gewählt haben.
- Optional: Web-Proxy-Logs oder SaaS-Nutzungsberichte als quantitative Ergänzung.

B – LEGALISIEREN (WOCHE 2–3)

Ziel: Vertrauen schaffen und Wissen sichtbar machen

- Amnestie aussprechen: explizit kommunizieren, dass bisherige Nutzung keine Konsequenzen hat.
- 2–3 Pilotnutzer identifizieren und einbinden: kurzes internes Format, in dem sie ihre Erfahrung teilen.
- Erste einfache Spielregel kommunizieren: die drei Leitfragen (Kunde, Eigentümer, Verantwortung).
- Rote Linien klar und knapp benennen – ohne langen Richtlinientext.

C – STRUKTURIEREN (WOCHE 3–4)

Ziel: nachhaltigen Rahmen schaffen

- Einfaches Tool-Register: welche Tools sind freigegeben, für welche Nutzungsfälle, mit welchen Einschränkungen.
- Feedback-Kanal einrichten: wie melden Mitarbeitende neue Bedarfe? (E-Mail, kurzes Formular, direkte Ansprechperson)
- Erstes internes Training: nicht als Pflichtschulung, sondern als praxisnahes 60-Minuten-Format mit echten Beispielen aus dem eigenen Unternehmen.
- KI-kompetente Mitarbeitende formal als interne Ansprechpersonen benennen.

D – MESSEN UND WEITERENTWICKELN

- Anzahl gemeldeter neuer Anwendungswünsche (soll steigen – Zeichen, dass der Kanal funktioniert).
- Anteil Mitarbeitender, die genehmigte Tools nutzen (soll über Zeit steigen).
- Anteil identifizierter Schatten-Tools (soll zunächst steigen, dann sinken – erst sehen, dann heilen).
- Gemeldete Vorfälle mit KI-Bezug (Datenpannen, Fehlentscheidungen) – soll sinken.
- Durchlaufzeit für Tool-Freigaben (soll niedrig bleiben, sonst wächst der Schatten zurück).
- Review der Spielregeln alle 6 Monate – Technologie ändert sich, die Regeln müssen mithalten.

Quellen (Auswahl)

[1] Software AG (2024). Shadow AI Report. 50 % der Mitarbeitenden nutzen nicht genehmigte KI-Tools; 46 % würden dies auch bei Verbot fortsetzen.

[2] Microsoft / LinkedIn (2024). Work Trend Index: AI at Work Is Here. Now Comes the Hard Part. 31.000 Befragte weltweit. 75 % der Wissensarbeiter nutzen KI; 78 % davon mit eigenen privaten Accounts (BYOAI).

[3] IBM (2024). Rising AI Adoption – Shadow AI Risks. 80 % nutzen KI; nur 22 % ausschließlich mit Unternehmens-Tools. 97 % berichten von Produktivitätsgewinnen; fast ein Drittel spart bis zu 6 Stunden pro Woche.

[4] Gartner (2025) / Microsoft Work Trend Index (2024). Analystenschätzung: 75 % der Mitarbeitenden werden bis 2027 Schatten-KI nutzen (2022: 41 %).

[5] Gartner Security and Risk Management Summit (2025). Shadow AI can be a tool for AI innovation with the right controls. Vgl. IT Pro, 23. September 2025.

[6] IBM (2024). Rising AI Adoption. 60 % der Mitarbeitenden: Praxistraining würde ihren KI-Einsatz verbessern.

[7] CybSafe / National Cybersecurity Alliance (2024). 38 % teilen vertrauliche Daten mit KI-Plattformen ohne Genehmigung des Unternehmens.

[8] ISACA (2025). The Rise of Shadow AI: Auditing Unauthorized AI Tools. 60 % der Mitarbeitenden nutzen KI; nur 18 % kennen eine offizielle Unternehmensrichtlinie.

Über den Autor

Christian Teutrine ist Unternehmensberater mit über 25 Jahren Erfahrung in komplexen IT- und Veränderungsvorhaben, schwerpunktmäßig im Automotive- und Industrieumfeld. Er ist zertifizierter KI-Manager und KI-Anwendungsberater (IHK, 2026) und berät Unternehmen unter dem Label keinwenn in den Bereichen Unternehmensberatung, KI-Strategie und Projektmanagement.

Dieser Text wurde mit Unterstützung von KI-Werkzeugen entwickelt und vom Autor inhaltlich verantwortet.