// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

Shadow AI verhindern: Leitfaden für österreichische Unternehmen

Shadow AI im KMU kontrollieren: DSGVO, EU AI Act, 5-Phasen-Plan und Kostenrahmen — speziell für österreichische Unternehmen.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
20. Mai 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/shadow-ai-verhindern-oesterreich-unternehmen/

Eine Mitarbeiterin im Controlling lädt das Monatsreporting als PDF in ChatGPT — um schneller eine Zusammenfassung zu erstellen. Aus ihrer Perspektive ist das eine sinnvolle Arbeitshilfe. Aus DSGVO-Perspektive ist es möglicherweise eine meldepflichtige Datenpanne: Kundenumsätze, Gehaltsdaten oder Margenkennzahlen haben das Unternehmen verlassen, ohne dass ein Auftragsverarbeitungsvertrag existiert oder die Verarbeitungszwecke geprüft wurden.

Dieses Szenario ist kein Einzelfall. Analysen zu Shadow IT zeigen, dass in mittleren Unternehmen regelmäßig 30 bis 50 Prozent der genutzten Softwaretools außerhalb der IT-Kontrolle liegen — und der Anteil von KI-Tools wächst seit 2023 besonders schnell. Mitarbeitende handeln dabei selten böswillig. Sie wollen effizienter arbeiten, kennen aber die rechtlichen und technischen Konsequenzen nicht.

Dieser Artikel liefert keinen Appell zum Verbot. Er liefert einen Governance-Rahmen, der funktioniert: mit österreichischer Rechtslage, konkreten Erkennungsmethoden, einer 5-Phasen-Implementierung und einer realistischen Kosteneinschätzung — verständlich für Geschäftsführung und HR, nicht nur für die IT-Abteilung.

Was ist Shadow AI – und warum ist es mehr als ein IT-Problem?

Shadow AI ist eine Teilmenge von Shadow IT: KI-gestützte Tools, die Mitarbeitende ohne Wissen oder Genehmigung der Unternehmens-IT für Arbeitsaufgaben einsetzen. Der entscheidende Unterschied zur klassischen Shadow IT liegt in der Art der Datenverarbeitung: Beim Einsatz von ChatGPT oder Gemini verlassen Eingabedaten das Unternehmen und werden von einem externen Anbieter verarbeitet — mit eigenen Nutzungsbedingungen, Trainingsdaten-Policies und Serverstandorten.

Der häufigste Irrtum in der Praxis: Mitarbeitende unterscheiden nicht zwischen einem privaten Browser-Einsatz und einem geschäftlichen Verwendungszweck. Wer abends zuhause ChatGPT für eine Geburtstagsrede nutzt, entwickelt intuitiv dasselbe Verhalten für den Arbeitsalltag — ohne zu wissen, dass die Kontexte rechtlich völlig unterschiedlich sind.

Drei Ebenen des Problems:

- **Datenschutz:** Personenbezogene oder vertrauliche Unternehmensdaten verlassen die eigene Infrastruktur ohne rechtliche Absicherung.
- **Compliance:** Das Unternehmen verliert die Kontrolle über Verarbeitungszwecke und kann bei einer DSB-Prüfung keine Rechenschaft ablegen.
- **Operative Risiken:** KI-generierte Outputs fließen ohne Qualitätsprüfung in Entscheidungen — ein Angebot basiert auf einer halluzinierten Markteinschätzung, ein Vertrag enthält KI-formulierte Klauseln, die niemand geprüft hat.

Typische Shadow-AI-Tools in österreichischen KMU: ChatGPT Free/Plus, Google Gemini, Microsoft Copilot (über private Accounts), Grammarly, DeepL Write, Perplexity, Midjourney, Canva AI, Notion AI. Viele davon sind als Browser-Tools oder Extensions zugänglich — ohne Installation, ohne IT-Ticket, ohne Spur im System.

Österreichische Rechtslage: Was Unternehmen jetzt wissen müssen

DSGVO: Die drei entscheidenden Artikel

Art. 28 DSGVO (Auftragsverarbeitung): Sobald ein externer Dienstleister personenbezogene Daten im Auftrag eines Unternehmens verarbeitet, ist ein Auftragsverarbeitungsvertrag (AV-Vertrag) Pflicht. Lädt eine Mitarbeiterin Kundendaten in ein KI-Tool ohne abgeschlossenen AV-Vertrag, fehlt die rechtliche Grundlage — unabhängig davon, ob der Anbieter einen solchen Vertrag anbieten würde.

Art. 5 DSGVO (Zweckbindung): Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Das Trainieren von KI-Modellen durch einen Drittanbieter mit Kundendaten des Unternehmens entspricht in aller Regel nicht diesem Zweck.

Art. 32 DSGVO (Technisch-organisatorische Maßnahmen): Unternehmen sind verpflichtet, angemessene Sicherheitsmaßnahmen zu treffen. Das unkontrollierte Abfließen von Daten über nicht freigegebene KI-Tools ist ein Indikator dafür, dass diese Pflicht nicht erfüllt wird.

Welche Daten bei KI-Tools konkret gefährdet sind und wie Datenverlust verhindert wird, haben wir in unserem Artikel zu DSGVO & ChatGPT im Unternehmen detailliert aufgearbeitet.

Datenschutzbehörde Österreich (DSB)

Die österreichische DSB hat seit 2023 mehrere Verfahren im KI-Bereich geführt und zeigt eine zunehmend aktive Haltung gegenüber ungeregelter KI-Nutzung in Unternehmen. Bußgelder nach Art. 83 DSGVO können bei KMU bis zu 2 Prozent des weltweiten Jahresumsatzes betragen — für ein Unternehmen mit 5 Millionen Euro Umsatz wären das bis zu 100.000 Euro. Für unternehmensindividuelle Einschätzungen empfiehlt sich eine datenschutzrechtliche Beratung; dieser Abschnitt ersetzt diese nicht.

EU AI Act: Was Deployer ab 2025/2026 beachten müssen

Als „Deployer" — also Unternehmen, die KI-Systeme einsetzen — haben österreichische KMU nach dem EU AI Act konkrete Pflichten. Für Hochrisiko-Systeme (z. B. KI in der Personalentscheidung oder Kreditbewertung) sind Risikobewertungen, technische Dokumentation und Überwachungsprozesse vorgeschrieben. Entscheidend für Shadow AI: Die Compliance-Verantwortung bleibt beim Unternehmen — auch dann, wenn eine Mitarbeiterin ein Tool eigenständig nutzt, ohne dass die Geschäftsführung davon weiß.

Was KMU konkret unter dem EU AI Act tun müssen, erläutern wir ausführlich im Artikel EU AI Act: Was müssen KMU jetzt wirklich tun?.

Arbeitsrecht Österreich: Betriebsrat nicht vergessen

Wer Monitoring-Maßnahmen einführt, um Shadow AI zu erkennen, braucht in Betrieben mit Betriebsrat dessen Zustimmung — § 96 ArbVG gilt für Systeme zur Überwachung des Verhaltens oder der Leistung von Mitarbeitenden. Das betrifft Netzwerküberwachung genauso wie Auswertungen von Browser-Aktivitäten. Frühzeitige Einbindung ist kein bürokratisches Hindernis, sondern verhindert teure Rückschritte.

Shadow AI erkennen – so sehen Sie, was wirklich im Netzwerk passiert

Netzwerkebene: DNS- und Proxy-Logs

Der direkteste Weg zur Bestandsaufnahme: Welche Domains werden von Unternehmensgeräten aufgerufen? Bekannte KI-Anbieter-Domains sind unter anderem `api.openai.com`, `chat.openai.com`, `gemini.google.com`, `claude.ai`, `huggingface.co` und `perplexity.ai`. Wenn diese Domains in Ihren DNS-Logs auftauchen, ohne dass entsprechende Tools freigegeben wurden, haben Sie Shadow AI im Netz.

Für kleinere Netzwerke reicht oft eine einfache Auswertung des bestehenden Routers oder Firewalls. Wichtig: Die Auswertung muss mit dem Betriebsrat abgestimmt sein.

Cloud-Access-Security-Broker (CASB)

CASB-Lösungen wie Microsoft Defender for Cloud Apps oder Netskope ermöglichen granulare Sichtbarkeit darüber, welche Cloud-Dienste aus dem Unternehmensnetz genutzt werden — inklusive Klassifizierung nach Risikostufe. Der Einsatz lohnt sich in der Regel ab etwa 50 Nutzerinnen und Nutzern, da erst dann der Konfigurationsaufwand und die Lizenzkosten in einem vernünftigen Verhältnis zum Erkennungsgewinn stehen.

Endpoint-Ebene: Browser-Extensions und Apps

Ein erheblicher Teil der Shadow-AI-Nutzung läuft über Browser-Extensions — Grammarly, Compose AI oder ähnliche Tools sind in Sekunden installiert. Mobile Device Management (MDM) und Endpoint-Management-Lösungen ermöglichen es, installierte Extensions zu inventarisieren und nicht freigegebene Tools zu blockieren. Wer bereits mit Microsoft Intune oder einem vergleichbaren System arbeitet, hat die technische Basis oft bereits.

Wer bereits mit genehmigten KI-Tools wie Copilot arbeitet, sollte auch die Berechtigungsebene im Griff haben — unser Leitfaden zu KI DSGVO-konformem Einsatz gibt dazu die nächste Tiefenstufe.

Mitarbeiter-Umfragen als unterschätztes Instrument

Eine anonyme Kurzbefragung liefert oft mehr verwertbare Informationen als technische Logs — und zwar schneller und ohne arbeitsrechtliche Komplexität. Fragen wie „Welche digitalen Tools nutzen Sie regelmäßig, die nicht offiziell vom Unternehmen bereitgestellt werden?“ schaffen Transparenz und signalisieren gleichzeitig, dass die Geschäftsführung das Thema ohne Sanktionsabsicht angehen will. Das Framing ist entscheidend: keine Kontrolle, sondern Bestandsaufnahme.

Schritt-für-Schritt – Shadow AI in 5 Phasen unter Kontrolle bringen

Phase 1 – Bestandsaufnahme (Woche 1-2)

Starten Sie mit zwei parallelen Maßnahmen: einer anonymen Mitarbeiter-Umfrage (5 bis 8 Fragen, maximal 10 Minuten Aufwand) und einer Auswertung der verfügbaren Netzwerk-Logs. Ziel ist keine lückenlose Überwachung, sondern ein erster Überblick.

Besonders betroffen sind erfahrungsgemäß Marketing (Texterstellung, Bildgenerierung), HR (Stellenausschreibungen, Bewerber-Kommunikation), Vertrieb (Angebote, E-Mails) und Finance (Reporting, Datenauswertung). Priorisieren Sie die Befragung in diesen Bereichen.

Output dieser Phase: Eine Liste der genutzten Tools, kategorisiert nach Verbreitung und Risikopotenzial. Diese Liste ist die Arbeitsgrundlage für alle weiteren Schritte.

Phase 2 – Risikobewertung (Woche 2-3)

Nicht jedes Tool stellt dasselbe Risiko dar. Entscheidend ist, welche Datenkategorien in Kombination mit welchem Tool genutzt werden. Eine einfache 2×2-Matrix hilft: Wahrscheinlichkeit der Nutzung (hoch/niedrig) auf einer Achse, Schadenspotenzial (hoch/niedrig) auf der anderen.

Prüfen Sie für jedes identifizierte Tool: Existiert bereits ein AV-Vertrag? Ist der Anbieter DSGVO-konform (Serverstandort, Datenschutzerklärung, Trainingsdaten-Policy)? Gibt es eine Business-Version mit stärkeren Datenschutzgarantien? ChatGPT Enterprise oder Microsoft Copilot mit aktiviertem Data Protection Mode sind zum Beispiel deutlich anders einzustufen als die kostenlose ChatGPT-Free-Version.

Eine ausführliche Einschätzung, wie KI-Workflows mit Unternehmensdaten abgesichert werden, finden Sie in unserem Artikel KI-Workflows mit Unternehmensdaten absichern.

Phase 3 – Richtlinie erstellen (Woche 3-4)

Eine KI-Nutzungsrichtlinie für KMU muss nicht 30 Seiten lang sein. Sie muss drei Dinge klar regeln:

1. **Genehmigter Tool-Katalog:** Welche KI-Tools sind für welche Zwecke freigegeben?
2. **Verbotene Anwendungsfälle:** Welche Datenkategorien dürfen grundsätzlich nicht in externe KI-Tools eingegeben werden (z. B. Kundendaten mit Personenbezug, Lohndaten, strategische Geschäftsdaten)?
3. **Meldeprozess:** Wie können Mitarbeitende neue Tools zur Prüfung melden, ohne Sanktionen zu befürchten?

Wichtig: Eine Richtlinie allein verändert kein Verhalten. Ohne Schulung bleibt sie ein Dokument im Intranet. Ebenso wichtig: Mitarbeitende sollten bei der Erstellung eingebunden werden — wer an einer Regelung mitgewirkt hat, hält sich eher daran.

Phase 4 – Schulung und Kommunikation (Monat 2)

Schulungsbedarf ist nicht homogen. IT-Mitarbeitende brauchen technische Tiefe (Erkennungsmethoden, Konfiguration). Fachabteilungen brauchen praxisnahe Beispiele: Was darf ich eingeben, was nicht? Führungskräfte brauchen die rechtliche Einordnung und ihre Vorbildrolle.

Die Kernbotschaft für alle Ebenen: „Wir wollen KI ermöglichen, nicht verbieten — aber nur so, dass das Unternehmen und seine Kundendaten geschützt bleiben." Wer das Thema defensiv kommuniziert, erzeugt Misstrauen. Wer es als Enablement-Programm rahmt, gewinnt Mitarbeitende als aktive Mitgestalter.

Checkliste für Mitarbeitende vor der KI-Tool-Nutzung: - Ist das Tool im genehmigten Tool-Katalog aufgeführt? - Enthält meine Eingabe personenbezogene Daten von Kunden oder Mitarbeitenden? - Enthält meine Eingabe vertrauliche Geschäftsinformationen (Umsatzzahlen, Strategiepapiere, M&A-Informationen)? - Wenn eine dieser Fragen mit „Ja" beantwortet wird: Erst intern klären, bevor das Tool genutzt wird.

Phase 5 – Technische Absicherung und laufendes Monitoring

Der wichtigste Grundsatz: Verbote ohne Alternativen funktionieren nicht. Wenn Mitarbeitende ChatGPT für legitime Aufgaben einsetzen und Sie das unterbinden, ohne einen genehmigten Ersatz bereitzustellen, weichen sie auf andere Wege aus — oder werden frustriert.

Stellen Sie freigegebene Tools aktiv bereit. Konfigurieren Sie technische Kontrollen: DNS-Filterung für nicht freigegebene KI-Domains, App-Freigabelisten im MDM, Conditional Access Policies in Microsoft 365. Viele dieser Maßnahmen sind mit vorhandenen Bordmitteln umsetzbar — ohne zusätzliche Lizenzkosten.

Etablieren Sie einen quartalsweisen Review-Prozess. Die KI-Landschaft verändert sich zu schnell, als dass eine einmalig erstellte Richtlinie dauerhaft trägt. Neue Tools, neue Anbieter, neue Risiken — und manchmal auch neue Möglichkeiten, die freigegeben werden sollten.

Kostenrahmen – Was kostet ein Shadow-AI-Governance-Programm im KMU?

Typische Kostenpositionen sind: externe Beratung für Konzeption und Richtlinienerstellung, interne Personalzeit (IT, HR, Führung), ggf. Tool-Lizenzen für CASB oder MDM, sowie Schulungsaufwand.

Realistische Einschätzung nach Unternehmensgröße:

UNTERNEHMENSGRÖSSE	TYPISCHER AUFWAND	EINMALIGE KOSTEN (SCHÄTZUNG)
10–30 Mitarbeitende	1–2 Tage Beratung, 2–3 Tage intern	2.000–5.000 €
30–100 Mitarbeitende	3–5 Tage Beratung, 5–10 Tage intern	6.000–15.000 €
100–200 Mitarbeitende	5–10 Tage Beratung, 10–20 Tage intern	15.000–35.000 €

Diese Zahlen sind Orientierungswerte und hängen stark davon ab, wie viel intern geleistet werden kann und ob bereits Infrastruktur (MDM, CASB, Microsoft 365 E3/E5) vorhanden ist.

Gegenrechnung: Ein DSGVO-Bußgeld der DSB kann bis zu 4 Prozent des weltweiten Jahresumsatzes betragen (bei schwerwiegenden Verstößen nach Art. 83 Abs. 5 DSGVO). Dazu kommen Reputationsschäden, Kundenvertrauensverlust und der Aufwand für behördliche Verfahren — Kosten, die ein schlankes Governance-Programm in aller Regel bei weitem übersteigen.

Viele der notwendigen Maßnahmen lassen sich mit vorhandenen Microsoft-365-Bordmitteln umsetzen: Conditional Access, Microsoft Defender for Cloud Apps (in E5 enthalten), Intune für Endpoint-Management und Azure AD-Gruppen für Zugriffssteuerung. Wer diese Funktionen bereits lizenziert hat, zahlt für die Konfiguration, nicht für neue Lizenzen.

Führungsebene und HR – Ihre Rolle bei Shadow-AI-Governance

Warum Shadow AI kein reines IT-Thema ist

Technische Maßnahmen allein lösen das Problem nicht. DNS-Filter kann man umgehen. App-Verbote erzeugen Kreativlösungen. Was nachhaltig wirkt, ist eine Unternehmenskultur, in der Mitarbeitende verstehen, warum bestimmte Regeln gelten — und sich sicher fühlen, Fragen zu stellen oder neue Tools zu melden, ohne Sanktionen zu befürchten. Das ist keine IT-Aufgabe. Das ist Führungsaufgabe.

Aufgabe der Geschäftsführung

Drei konkrete Beiträge der Führungsebene sind unersetzlich: Erstens ein klares öffentliches Bekenntnis, dass KI-Governance Priorität hat und Budget bekommt. Zweitens Vorbildfunktion — wenn die Geschäftsführung selbst ungeregelte KI-Tools nutzt, ist jede Richtlinie unglaubwürdig. Drittens die Entscheidung, welche KI-Tools das Unternehmen aktiv bereitstellen will — das nimmt Mitarbeitenden den Druck, sich selbst zu behelfen.

Aufgabe HR

HR hat zwei Hebel: Prävention und Integration. Neue Mitarbeitende sollten die KI-Nutzungsrichtlinie bereits im Onboarding kennenlernen — nicht als Beiblatt zum Arbeitsvertrag, sondern als aktiv kommunizierten Teil der Unternehmenskultur. Bestehende Mitarbeitende brauchen regelmäßige Auffrischung, insbesondere wenn sich die freigegebenen Tools oder die Richtlinie ändern.

Beim Umgang mit Regelverstößen gilt österreichisches Arbeitsrecht: Disziplinarmaßnahmen setzen in der Regel eine klare, vorab kommunizierte Richtlinie voraus. Wer erst heute eine Richtlinie einführt, kann nicht rückwirkend ahnden.

Betriebsrat als Verbündeter, nicht als Hindernis

Betriebsräte, die frühzeitig eingebunden werden, werden in aller Regel zu konstruktiven Partnern — weil Shadow AI auch Arbeitnehmerinteressen berührt: ungeregelter Einsatz kann zur ungewollten Selbstüberwachung führen, KI-Outputs können zu fehlerhaften Leistungsbeurteilungen beitragen. Ein gemeinsam erarbeitetes Regelwerk hat deutlich bessere Akzeptanz als eine top-down erlassene IT-Richtlinie.

Praxistipp: Etablieren Sie eine interne KI-Taskforce aus je einer Person aus IT, HR, einer Fachabteilung und der Führungsebene. Dieses Gremium trifft sich quartalsweise, bewertet neue Tools, aktualisiert die Richtlinie und ist Anlaufstelle für Mitarbeitende. Der Aufwand ist überschaubar; der Nutzen — einheitliche Linie, klare Verantwortung — erheblich.

Praxis-Tipp: Schnell-Assessment für Ihren Startpunkt

Mit den folgenden sieben Fragen können Sie in fünf Minuten einschätzen, wie dringend Handlungsbedarf besteht. Beantworten Sie jede Frage ehrlich mit Ja oder Nein:

1. Haben Sie eine aktuelle, vollständige Liste aller KI-Tools, die in Ihrem Unternehmen genutzt werden?
2. Existiert eine schriftliche KI-Nutzungsrichtlinie, die Mitarbeitende kennen?
3. Wurden in den letzten 12 Monaten Mitarbeitende zum Thema KI und Datenschutz geschult?
4. Gibt es für alle genutzten KI-Tools mit Datenverarbeitung einen gültigen AV-Vertrag?
5. Sind technische Kontrollen vorhanden, die die Nutzung nicht freigegebener KI-Tools einschränken?
6. Ist der Betriebsrat (sofern vorhanden) in KI-Governance-Entscheidungen eingebunden?
7. Gibt es einen definierten Prozess, über den Mitarbeitende neue KI-Tools zur Prüfung melden können?

Auswertung: - **0–2 × Ja:** Dringender Handlungsbedarf. Starten Sie mit Phase 1 der oben beschriebenen Implementierung. - **3–4 × Ja:** Solide Basis vorhanden. Identifizieren Sie die offenen Punkte und schließen Sie gezielt die größten Lücken. - **5–7 × Ja:** Gut aufgestellt. Konzentrieren Sie sich auf das laufende Monitoring und die Aktualisierung bestehender Regelungen.

Die meisten österreichischen KMU landen beim ersten Durchgang bei zwei bis drei Ja-Antworten — das ist der normale Ausgangspunkt, kein Versagen. Der entscheidende Unterschied ist, ob ein Plan existiert, der diesen Zustand verändert.

FAQ

Was ist der Unterschied zwischen Shadow IT und Shadow AI?

Shadow IT bezeichnet alle selbst beschafften IT-Tools und -Dienste außerhalb der IT-Kontrolle des Unternehmens. Shadow AI ist ein Teilbereich davon, der sich speziell auf KI-gestützte Anwendungen bezieht. Der wesentliche Unterschied: KI-Tools verarbeiten Eingabedaten aktiv bei einem Drittanbieter, generieren Outputs, die in Entscheidungen einfließen, und unterliegen eigenen Nutzungsbedingungen hinsichtlich Datenspeicherung und Modelltraining. Das erzeugt spezifische DSGVO-Risiken, die bei klassischer Shadow IT so nicht auftreten.

Darf ich Mitarbeitenden die private KI-Nutzung am Arbeitsplatz einfach verbieten?

Ein vollständiges Verbot ist nach aktueller Rechtslage möglich, in der Praxis aber selten das sinnvollste Instrument. Ein kategorisches Verbot ohne Alternative erzeugt Umgehungsverhalten, belastet das Betriebsklima und verhindert legitime Effizienzgewinne. Empfehlenswerter ist ein klarer genehmigter Tool-Katalog mit definierten verbotenen Anwendungsfällen — kombiniert mit der

aktiven Bereitstellung sicherer Alternativen. In Betrieben mit Betriebsrat bedürfen umfassende Überwachungsmaßnahmen zur Durchsetzung eines solchen Verbots zudem der Mitbestimmung nach § 96 ArbVG.

Was ist, wenn ein Mitarbeiter versehentlich Kundendaten in ChatGPT eingegeben hat?

Nach aktueller Rechtslage handelt es sich dabei möglicherweise um eine meldepflichtige Datenschutzverletzung nach Art. 33 DSGVO. Die DSB ist in der Regel innerhalb von 72 Stunden zu informieren, wenn ein hohes Risiko für die betroffenen Personen besteht. Sichern Sie zunächst die Fakten (welche Daten, welches Tool, wann), ziehen Sie eine rechtliche Einschätzung hinzu und prüfen Sie, ob eine Meldung erforderlich ist. Das spricht einmal mehr dafür, präventiv klare Regelungen zu schaffen, bevor ein solcher Fall eintritt.

Nächste Schritte – So setzen Sie das heute an

Drei Maßnahmen, die Sie sofort angehen können, ohne Vorarbeit:

Erstens: Starten Sie mit der Bestandsaufnahme — eine kurze Umfrage im Team kostet zwei Stunden und liefert mehr verwertbare Information als jedes technische Audit. **Zweitens:** Lassen Sie Ihre bestehende IT-Infrastruktur auf bereits vorhandene Governance-Funktionen prüfen — Microsoft 365 E3 und E5 enthalten vieles, was KMU bereits lizenziert, aber nicht konfiguriert haben. **Drittens:** Erstellen Sie einen ersten Entwurf einer KI-Nutzungsrichtlinie — auch eine einseitige, klare Regelung ist besser als keine.

Wer das nicht intern stemmen kann oder will, muss das Rad nicht neu erfinden. Bei Strukturaflow sehen wir regelmäßig, dass der größte Aufwand nicht in der Technologie liegt, sondern in der Frage: Wo fangen wir an, und was ist für unsere Situation wirklich relevant?

In einem unverbindlichen 30-Minuten-Beratungsgespräch können wir gemeinsam einschätzen, wo Ihr Unternehmen konkret steht, welche Maßnahmen für Ihre Größe und Branche sinnvoll sind — und welche Sie sich sparen können. Kein Standardpaket, keine Verkaufsveranstaltung.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

https://wissen.strukturaflow.it.com