Tech Industry Leadership
KI, Automatisierung und Führung



KI sicher nutzen:

Vom Schatten zur Strategie

In vielen Betrieben nutzen Mitarbeitende KI längst, nur eben nicht offiziell – und genau das öffnet Sicherheitslücken. Wie du aus dieser Schatten-Nutzung mit einem 90-Tage-Fahrplan eine sichere Strategie machst, erfährst du in diesem Newsletter.

In vielen Betrieben in Deutschland ist KI längst Realität, allerdings nicht offiziell. Mitarbeitende „fragen mal eben ChatGPT“, lassen sich E-Mails verbessern, ihren Code prüfen oder sich bei Recherche und Lieferantensuche helfen. Währenddessen diskutiert das Management noch über Risiken und lässt sich mit dem besten Gewissen viel Zeit. Schließlich setzt man ja offiziell noch gar keine KI ein.

Im Ergebnis entstehen durch diese **Schatten-Nutzung** große Sicherheitslücken. Daten wandern planlos in Tools, niemand macht sich Gedanken, wo diese Tools gehostet werden, Zugriffe sind unklar und nicht dokumentiert. Spätestens durch die Nutzung von Google & Co wird inzwischen bereits KI eingesetzt. Die erste Antwort bei einer normalen Internetsuche kommt inzwischen meistens von der Browser-eigenen KI.

Die unbequeme Wahrheit ist:	„Wir setzen (noch) keine KI ein“ klingt beruhigend, ist aber in den meisten Unternehmen leider nicht mehr als die gute alte „Vogel-Strauß-Taktik“. Wir lügen uns in die Tasche und gehen damit ein unkalkuliertes Risiko ein.

Die gute Nachricht: **Sicherheit muss kein Showstopper sein, im Gegenteil, mit den richtigen Überlegungen kannst du sie in einen Wettbewerbsvorteil umwandeln.**

Was unter dem Radar so alles passiert (und wie du es stoppst)

In Kundenprojekten habe ich gerade bei „noch KI-freien Unternehmen“ abenteuerliche KI-Anwendungen mit unüberlegtem Dateneinsatz vorgefunden, die der Geschäftsleitung oft nicht bewusst war. Zum Beispiel:

- **Vertrauliche Inhalte im Prompt:** Vertrieb kopiert Kundendaten in einen öffentlichen Assistenten.
  Möglicher Fix: Datenklassifizierung + automatische Schwärzung/Maskierung sensibler Felder in der Eingabe (PII, Vertragsnummern, Preislisten).

- **Code-Leaks aus der Entwicklung:** Development-Teams lassen proprietären Code prüfen.
  Möglicher Fix: Whitelisted, unternehmensinterne Modelle/Instanzen, Repository-Filter und Policies: „Keine proprietären Snippets > n Zeilen extern einfügen“ (Festlegen der Grenzen, wie viele Zeilen Code eingefügte Snippets haben dürfen).

- **Tool-Wildwuchs (>30 inoffizielle Apps):** Teams testen begeistert alles Mögliche.
  Möglicher Fix: KI-Stack definieren (zugelassene Tools, Hosting-Standorte, Rollenrechte) und einen schlanken Genehmigungsprozess für neue Tools etablieren.

- **Kein Audit-Trail:** Wer hat was mit welchen Daten getan?
  Möglicher Fix: Protokollierung aktivieren (Prompts, Outputs, Metadaten), revisionssicher ablegen, regelmäßige Stichproben-Reviews.

Dein sicherer KI-Betriebsrahmen (Industrial Grade)

Betrachte KI wie ein Betriebssystem. Auch dort stehen als erstes die **Governance und die dafür geeignete Plattform. Dann wird die Datennutzung definiert, Prozesse implementiert und die Mitarbeiter geschult.**

Und das tun wir heute schon ganz selbstverständlich und niemand hat deswegen die Nutzung von Betriebssystemen ausgeschlossen. Kein Grund, das bei der Nutzung von KI anders zu machen. KI ist nichts anderes als eine Technologie. Eine, die wir brauchen.

Dazu brauchen Unternehmen etwas mehr als der Privatmann bei der heimischen Nutzung an seinem privaten PC. Für Unternehmen steht hier aufgrund des Sicherheitsaspektes zunächst die Wahl der richtigen KI-Plattform an, die die minimalen Sicherheitsanforderungen erfüllt und damit eine sichere und dennoch effiziente Nutzung von KI ermöglicht.

Was muss diese Plattform mindestens bieten?

1) Governance: klare Leitplanken

- **KI-Policy** in „Plain German" formulieren: Was ist erlaubt? Was ist tabu? Sorge für klare Regeln und anschauliche Beispiele!
- **Rollen & Verantwortungen festlegen (RACI):** CIO/CTO (Plattform), CISO/IT-Security (Richtlinien), Fachbereiche (Use Cases), Datenschutz, Betriebsrat.
- **Genehmigungen & Ausnahmen:** dokumentierte Prozesse mit SLA (Service Level Agreement).

2) Wahl der KI-Plattform: trennend & sicher

- **Hosting-Optionen** nach Risiko wählen: EU-Cloud, Private Cloud, On-Prem – triff eine bewusste Wahl und halte die Begründung fest.
- **SSO (Single Sign-On für mehrere Systeme)** nur gezielt erlauben, **besser RBAC (Role-Based-Access Control)** Beschränke den Zugriff auf autorisierte Rollen.
- **Mandantentrennung & Logging:** Schaffe getrennte Umgebungen (Development / Test / Produktiv-System), Schalte Audit-Trail standardmäßig ein.
- **Model-Router:** Internes Routing je nach Datenkritikalität (z. B. interne Modelle für vertrauliche Inhalte, externe für offene Recherche).

3) Daten: Schutz vor, während und nach der Nutzung

- **Datenklassifizierung:** Lege fest, was öffentlich, intern, vertraulich oder streng vertraulich ist.
- **Pre-Prompt-Sanitizing:** automatische Anonymisierung/Maskierung.
- **Retrieval-Kontrolle:** Binde nur freigegebene Wissensquellen an (z. B. DMS / Confluence / SharePoint), statt dem gesamten Fileserver.
- **Retention:** Lege fest, wie lange die Outputs gespeichert werden sollen und wer darauf zugreifen darf.

4) Menschen: Enablement statt Verbote

- **Schulungen pro Rolle:** Dabei ist Vertrieb ≠ Entwicklung ≠ Einkauf.
- **Playbooks & Musterprompts:** Lasse geprüfte Vorlagen für wiederkehrende Aufgaben (E-Mail-Antworten, Entwicklungsreviews, Qualitätsdokumente) anlegen.

- **„Masterprompt für Compliance“:** Ein vordefinierter Prompt, der automatisch Policies, Tonalität, Datenschutzregeln und Quellenpflicht zieht, kann von einer guten KI-Plattform in „klar-deutsch“ hinterlegt werden.

5) Betrieb: messen, testen, verbessern

- **Qualitätsmetriken** sollten erfasst und optimiert werden können, z. B. Genauigkeit, Halluzinationsrate, Bearbeitungszeit, Nutzerzufriedenheit.
- **Red-Team-Tests:** Prompt-Injection-Checks, Datenabfluss-Simulationen.
- **Release-Rhythmus:** Regelmäßige Modell-Updates/Prompt-Library-Reviews mit Change-Log.

90-Tage-Fahrplan (pragmatisch & realistisch)

Wie gehst du jetzt konkret vor? Hier ist ein Vorschlag über einen 90-Tage-Fahrplan, mit dem du deine KI-Sicherheit herstellst und damit die effektive Nutzung dieser Technologie ermöglichst und förderst – ein eindeutiger Wettbewerbsvorteil gegenüber denen, die noch mit dem Kopf im Sand stecken!

Woche 1–2: Sicht schaffen & Risiken stoppen

- Shadow-IT-Scan: Befrage deine Teams und finde heraus, welche Tools derzeit im Unternehmen genutzt werden. Von wem? Wofür?
- Quick-Policy (1-Pager) + Kommunikation: „Was ab heute erlaubt/verboten ist“.
- Lasse Sofortmaßnahmen erarbeiten: PII-Maskierung bei Text-Prompts; Leitfaden „Keine vertraulichen Inhalte in externe Tools“.

Woche 3–6: Safe Foundations

- Minimaler **KI-Stack**: Stelle eine Liste mit Tools auf, die genutzt werden können und wofür, z. B. freigegebener Assistent, EU-Hosting, SSO, Logging aktiv.
- **Masterprompt** & 5 geprüfte Use-Case-Vorlagen (z. B. Angebotszusammenfassung, Lieferantenrecherche, Qualitätsmeldung, Meeting-Protokoll, FAQ-Antworten).
- Erste **Retrieval-Anbindung**: Erstelle eine geprüfte Wissensbasis, die nun obligatorisch genutzt werden soll (Versioniert, kuratiert).

Woche 7–10: Pilot produktiv

- Zwei Fachbereiche (z. B. Vertrieb + Service) starten im **MVP-Betrieb** (= Minimum Viable Product), also mit einem ersten Prototypen, der die Mindestanforderungen abdeckt.)
- KPIs messen (Zeitgewinn, Fehlerquote, Akzeptanz).
- Red-Team-Test durchführen (Prüfen auf Sicherheitslücken), Erkenntnisse in Optimierungen umsetzen.

Woche 11–12: Rollout & Skalieren

- Nun kannst du Schulungen im Unternehmen ausrollen, die Prompt-Library erweitern und das Reporting im Management verankern.
- Schaffe nun auch einen Prozess für neue Use Cases (Aufnahme → Risiko-Check → Freigabe → Template).

Erscheint dir das aufwändig? – Durch die Wahl einer geeigneten KI-Plattform kannst du viele dieser Punkte mit einem Schlag abdecken, der Grund, warum so eine Plattform als Grundlage für Unternehmen unbedingt zu empfehlen ist.

So sieht „sicher & schnell“ im Alltag aus

- **Vertrieb:** E-Mail-Assistent innerhalb der Plattform (mit Masterprompt + Tonalität + PII-Filter). Kein Copy-Paste in öffentliche Tools.
- **Entwicklung:** Code-Review über interne Instanz; Snippet-Grenzen, Lizenz-Check, kein Upload proprietärer Module in externe Dienste.
- **Service:** Falllösungen via Retriever aus freigegebenen Handbüchern; Tickets werden automatisch dokumentiert.
- **Einkauf:** Lieferantenrecherche mit Quellenpflicht; Ergebnisse inkl. Risikonotiz und Freigabe-Workflow.
- **Qualität/Compliance:** Protokoll-Ansicht aller KI-Interaktionen, stichprobenartige Prüfung, Erkenntnisse zurück in die Playbooks einspielen.

Und nur, falls du im Unternehmen diese Antworten bekommst…

- **„Zu teuer.“** Nicht handeln ist z.B. bei einem Datenleck oder dem Verlust von firmeninternem Knowhow deutlich teurer. Nacharbeit und wildes Herumprobieren kostet Zeit und verzögert Projekte. Ein schlanker Stack an ausgewählten und gezielt genutzten KI-Tools mit klaren Regeln senkt Risiken **und** steigert die Produktivität.
- **„Zu komplex.“** Mit 1-Pager-Policy, Masterprompt und zwei Pilotbereichen auf einer industriell tauglichen KI-Plattform wirst du in wenigen Wochen produktiv.

- **„Wir warten auf perfekte Rechtssicherheit."** Du brauchst **angemessenes** Risikomanagement, nicht Stillstand. Saubere Protokolle, klare Zuständigkeiten, kuratierte Datenquellen bringen dich auf ein akzeptables Niveau, das vermutlich deutlich höher liegt, als die derzeitige Situation.

(Hinweis: Dieser Newsletter bietet keine Rechtsberatung. Prüfe rechtliche Anforderungen mit Datenschutz/Legal in deinem Unternehmen.)

Dein nächster Schritt

1

Benenne ein Kernteam (Fachbereich, IT-Sec/Datenschutz, Betriebsrat).

2

Starte mit dem 1-Pager: Was ist ab heute erlaubt? Was nicht?

3

Pilot in 2 Bereichen, mit Masterprompt, Logging und retriever-gestützter Wissensbasis.

4

Messe Nutzen & Risiken – und skaliere, was funktioniert.

Gerne gehe ich diese Schritte mit dir gemeinsam, von der Wahl der KI-Plattform bis zur Implementierung und Schulung deiner Teams. Ich bringe dazu nicht nur die Expertise als zertifizierter KI-Consultant und 30 Jahre Erfahrung in Vertriebs- und

Führungspositionen der deutschen technischen Industrie mit, sondern auch Kontakte zu Programmierern, Automatisierern und Spezialisten in der KI-Welt.

Gemeinsam werden wir schnell, gezielt und effektiv eine rechtsichere Nutzung von KI in deinem Unternehmen ermöglichen.



Über die Autorin

Anita Renc

KI-Consultant und Business Coach mit über 30 Jahren Industrie- und Führungserfahrung

info@futuresetup.de **futuresetup.de**