PROVECTUS

5 GRÜNDE,

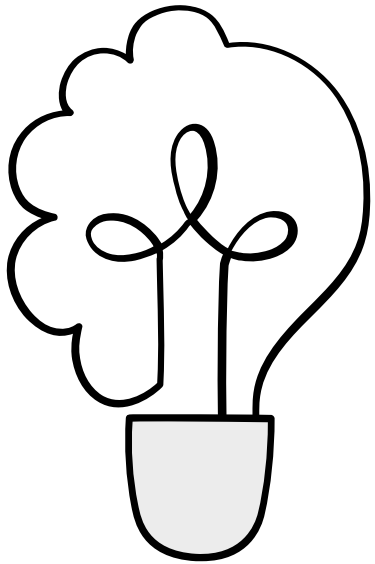
WARUM DIE EFFIZIENTE KI NUTZUNG IN UNTERNEHMEN SCHEITERT

Künstliche Intelligenz: Die disruptive Kraft, die Unternehmen neu definiert

KÜNSTLICHE INTELLIGENZ

EINE ZEITENWENDE FÜR WIRTSCHAFT UND TECHNOLOGIE

Künstliche Intelligenz (KI) ist keine Zukunftsvision mehr – sie ist Gegenwart und entwickelt sich mit exponentieller Geschwindigkeit. Unternehmen auf der ganzen Welt setzen KI heute bereits in Bereichen wie Automatisierung, Kundenservice, Datenanalyse, Cybersecurity oder Produktentwicklung ein. Doch das ist erst der Anfang: KI steht kurz davor, ganze Geschäftsmodelle zu transformieren, Märkte zu verschieben und Branchenführer zu entmachten, wenn diese nicht rechtzeitig handeln.



KI ist keine bloße „technologische Unterstützung" – sie ist eine disruptive Innovation, vergleichbar mit der Industrialisierung, dem Internet oder der Elektrifizierung. Unternehmen, die KI strategisch einsetzen, gewinnen nicht nur einen Effizienzvorsprung – sie schaffen neue Wertschöpfung, transformieren ihr Geschäftsmodell und sichern ihre Zukunftsfähigkeit.

DER KI-BOOM IST REAL

Laut PwC wird der wirtschaftliche Einfluss von KI bis **2030 weltweit**

15,7

Billionen US-Dollar betragen – mehr als das Bruttoinlandsprodukt von China heute.

Die McKinsey Global Survey (2023) zeigt, dass bereits

40%

der Unternehmen KI in mindestens einem Geschäftsbereich produktiv nutzen – Tendenz stark steigend.

Unternehmen, die KI frühzeitig integrieren, erzielen laut Deloitte

20–30%

höhere Margen in Bereichen wie Kundenanalyse, Automatisierung und Produktivität.

In einer Umfrage von Gartner gaben

70%

der CIOs an, dass Unternehmen ohne KI in den nächsten fünf Jahren nicht wettbewerbsfähig bleiben werden.

WARUM KI SO DISRUPTIV IST – SECHS TRANSFORMATIONSHEBEL

1.

AUTOMATISIERUNG VON WISSENSARBEIT

KI ersetzt nicht nur repetitive Tätigkeiten, sondern auch kognitive Aufgaben wie Textgenerierung, Übersetzung, Auswertung großer Datenmengen oder sogar Softwareentwicklung. Damit verändert sie ganze Berufsbilder und macht klassische Skalierungsmuster obsolet.

2.

MASSIVE PRODUKTIVITÄTSGEWINNE

Mit generativer KI, Automatisierung und Entscheidungsunterstützungssystemen können Prozesse radikal beschleunigt werden. Wer heute in der Lage ist, z. B. 10x schneller Produktideen zu testen oder Inhalte zu generieren, wird den Markt dominieren.

3.

DATENGESTÜTZTE ENTSCHEIDUNGEN IN ECHTZEIT

KI ermöglicht erstmals die intelligente, kontextuelle Auswertung riesiger Datenmengen in Echtzeit. Das bedeutet: präzisere Prognosen, bessere Customer Insights, schnellere Raktionen – und eine agile, lernende Organisation.

4.

PERSONALISIERUNG IM MASSENMASSSTAB

KI ermöglicht hyperpersonalisierte Kundenerlebnisse – etwa durch intelligente Produktempfehlungen, dynamische Preisgestaltung oder automatisierten, empathischen Kundenservice. Wer das nicht bietet, verliert gegen Plattformen, die es tun.

5.

NEUE GESCHÄFTSMODELLE & ÖKOSYSTEME

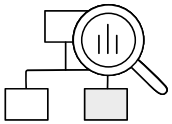
KI schafft völlig neue Wertschöpfungsketten – etwa durch KI-as-a-Service, digitale Assistenten, synthetische Medien oder autonome Systeme.

6.

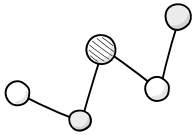
INTELLIGENTE, SCHNELLE UND ADAPTIVE PROZESSE DANK SPEZIALISIERTER KI-AGENTEN

Künstliche Intelligenz fungiert längst nicht mehr als isoliertes Werkzeug, sondern entwickelt sich vielmehr zum kooperativen System aus spezialisierten Agenten. Statt einer „All-in-One"-KI übernehmen künftig mehrere aufgabenorientierte Agenten unterschiedliche Rollen – vom Datenanalyse-Bot über Textgeneratoren bis hin zu Entscheidungsassistenten oder Automatisierungs-Engines.

Diese Multi-Agenten-Architekturen ermöglichen es Unternehmen, komplexe Prozesse modular, skalierbar und dynamisch abzubilden. Der wahre Transformationshebel liegt dabei in der Fähigkeit dieser Agenten, koordiniert zusammenzuarbeiten:



Sie teilen **Informationen kontextabhängig**.



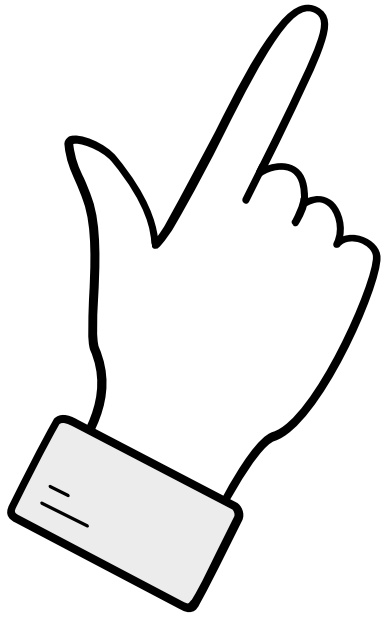
Sie übernehmen **Aufgaben entlang eines Workflows** autonom.

Und treffen **abgestimmte Entscheidungen** – in Echtzeit und auf Basis von unternehmens-spezifischen Regeln.

Das Ergebnis: Prozesse werden intelligenter, schneller und adaptiver, und die Organisation entwickelt sich zu einem lernenden System, in dem Mensch und Maschine gemeinsam wirken.

WER JETZT ZÖGERT, VERLIERT

Die Geschichte der Digitalisierung zeigt: **Technologien erzeugen Gewinner und Verlierer**. Wer zu spät reagiert, muss mühsam aufholen oder wird vom Markt verdrängt – siehe Kodak, Nokia oder Blockbuster.



ÄHNLICH VERHÄLT ES SICH MIT KI:

- **First Mover profitieren von Netzwerkeffekten,** Reifevorsprung und Datenzugang.
- **Nachzügler kämpfen mit kulturellem Wandel, veralteter Infrastruktur und internen Widerständen.**
- Das „Window of Opportunity" schließt sich schnell: KI-Modelle, Datenstrukturen und strategisches Know-how sind **nicht kurzfristig aufzuholen.**

Die Konsequenz: Wer **KI ignoriert, gefährdet** sein Geschäftsmodell

Künstliche Intelligenz ist nicht optional – sie wird Grundlage für Wertschöpfung, Innovation und Wettbewerbsfähigkeit. Wer KI ignoriert oder zu spät integriert, riskiert nicht nur den Anschluss – sondern die Relevanz seines Geschäftsmodells. Der Handlungsdruck ist hoch, die Chancen gewaltig. Unternehmen, die jetzt mutig, strategisch und verantwortungsvoll handeln, gehören zu den Gewinnern der nächsten Dekade.

PROVECTUS

REIFEGRAND

KI-REIFEGRAD IN DEUTSCHLAND

Deutschland kämpft im internationalen Vergleich noch immer mit einem massiven Rückstand im Bereich der Digitalisierung.

Während große Industrieunternehmen beim Einsatz digitaler Technologien wie Cloud, KI und Automatisierung Fortschritte machen, zeigen sich in kleinen und mittleren Unternehmen weiterhin enorme strukturelle Herausforderungen – etwa bei der Integration digitaler Prozesse, Cybersicherheit oder der Nutzung von Datenanalysen. Der Digital Economy and Society Index (DESI) der EU weist Deutschland regelmäßig auf hintere Plätze in Bereichen wie digitaler öffentlicher Dienste und digitalen Kompetenzen aus.

Als IT-Dienstleister können wir diese Ergebnisse bestätigen. Gerade öffentliche Sektoren und der Mittelstand hinken in puncto Digitalisierung nach und kämpfen wie oben erwähnt mit veralteten Infrastrukturen, mit kulturellem Wandel und blockieren sich selbst durch Widerstände und diffuse Ängste.

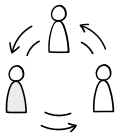
Die Hausaufgaben sind groß, wenn man nicht riskieren möchte, komplett abgehängt zu werden. Versäumnisse der letzten Jahre werden mit der zunehmenden Innovationsgeschwindigkeit schmerzvoller. Umso wichtiger ist es, dass besser gestern als heute damit begonnen wird, die Hürden zu beseitigen.

FÜNF GROßE HÜRDEN

HÜRDEN 1:

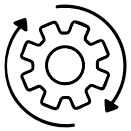
FEHLENDE DATENSTRATEGIE UND DATENQUALITÄT

Viele Unternehmen verfügen nicht über die nötige Datenbasis, um KI-Modelle zu trainieren – weder in Bezug auf Umfang noch Qualität. Im Kern umfasst es 5 Punkte, die man im Bezug auf Daten betrachten muss.



ROLLEN UND RECHTE

- **Wie viele Menschen haben Zugriff auf welche Daten?**
- Berechtigungen optimieren, entfernen, sperren
- RBAC (Role based access control) Konzept

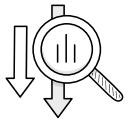


DATENLEBENS-ZYKLUS

- **Welche Steuerelemente für den Datenlebens-zyklus haben wir?**
- Aufbewahrungsrichtlinien und automatisches Löschen
- Records Management für geschäftliche, rechtliche oder behördliche Anforderungen an die Aufbewahrung

DATEN KLASSIFIZIERUNG

- **Welche Klassifizierungen gibt es und passen diese zum Lifecycle?**
- Auswahl und Definition von Typen vertraulicher Informationen
- Sicherstellung der Verschlüsselung & Retentions je nach Klassifizierung
- Integration in Data Loss Prevention Konzept



DATEN SPEICHERORTE

- **Wo sind welche Daten und wie kann darauf zugegriffen werden?**
- Erstellung eines Inventars aller Datenrepositorien
- Erstellung einer Datenlandkarte
- Datenverfügbarkeit sicherstellen

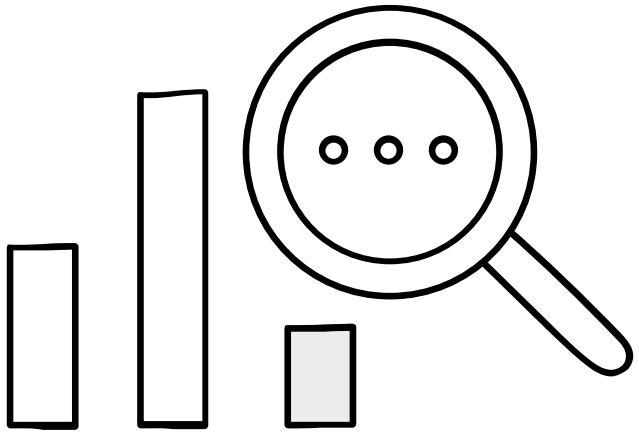
DATEN HYGIENE

- **Welche Vorschriften im Umgang mit Daten haben wir?**
- Vereinheitlichung der Ablage von Daten anstreben
- Nutzung von Meta-Daten (Tags, Kategorie, Title, etc.)
- Redundante und obsolete Daten identifizieren und loswerden

Framework Quelle: Stephanus Schulte

FEHLENDE DATENHYGIENE – EIN OFT UNTERSCHÄTZTES, ABER KRITISCHES PROBLEM

In einer zunehmend datengesteuerten Unternehmenswelt wird **Datenhygiene** – also die Qualität, Struktur, Aktualität und Pflege von Daten – zum **entscheidenden Erfolgsfaktor** für digitale Transformation und KI-Nutzung. Und doch herrscht in vielen Organisationen ein Zustand, der mit einem unaufgeräumten Lager vergleichbar ist: Daten sind vorhanden, aber sie sind verstreut, veraltet, doppelt, widersprüchlich oder schlicht unbrauchbar.



Schlechte Datenqualität führt zu fehlerhaften Analysen & falschen Entscheidungen.

Unvollständige, veraltete oder falsch formatierte Daten führen zu verzerrten Auswertungen – und damit zu Fehlentscheidungen auf operativer wie strategischer Ebene. Dieses Problem wird noch gravierender, wenn diese Daten von KI ausgelesen werden, denn KI-Modelle sind nur so gut wie die Daten, mit denen sie trainiert werden. „Garbage in – garbage out" gilt nach wie vor: Schlechte Datenqualität verhindert präzise Prognosen, automatisierte Entscheidungen oder sinnvolle Personalisierung.

DATENHYGIENE BEGINNT BEI RETENTION & ZUGRIFFSKLARHEIT

Ein oft übersehener, aber essenzieller Baustein funktionierender Datenstrategien ist die systematische Pflege und Entlastung von Dateibeständen.
Ein erster, pragmatischer Schritt hin zu besserer Datenhygiene ist die Einführung von Retention Policies bzw. Retention Labels. Damit lassen sich **automatisierte Prozesse** definieren, die z. B. dafür sorgen, dass **veraltete Dateien** (z. B. seit 5 Jahren nicht verändert), **nicht mehr relevante Inhalte oder überlagerte Versionen** entweder **gelöscht** oder in eine **Preservation Hold Library** verschoben werden – je nach rechtlichem Bedarf oder Unternehmensrichtlinie.
Das reduziert nicht nur Datenschatten und Speicherlast, sondern schützt aktiv vor Compliance-Risiken, etwa im Fall von DSGVO-konformem Datenlöschungsanspruch („Right to be forgotten").

AUFRÄUMEN MIT SYSTEM: MIT SHAREPOINT ADVANCED MANAGEMENT DIE KONTROLLE ÜBER DATENFREIGABEN ZURÜCKGEWINNEN

Mit der Einführung von Microsoft Copilot bekommen viele Organisationen automatisch Zugriff auf SharePoint Advanced Management – ein Feature, das früher separat lizenziert werden musste. Dieses Toolset ist ein echter Gamechanger für alle, die Datenzugriffe kontrollieren, strukturieren und analysieren wollen. Wer noch nicht in Copilot Lizenzen investieren möchte, kann das SharePoint Advanced Management aber auch als seperates Add-On lizenzieren.
Ein beispielsweise besonders wertvolles Feature sind die **Oversharing Reports:** Sie analysieren die Freigabestruktur innerhalb von SharePoint und identifizieren typische Problemzonen wie:

- Übermäßig viele individuelle Freigaben
- Freigaben an „alle mit dem Link" – ohne Kontrolle, wer diesen teilt
- Berechtigungs-Wildwuchs durch unstrukturierte SharePoint-Nutzung

Gerade bei einem unstrukturierten Rollout – etwa wenn Nutzer*innen einfach "loslegen dürfen" – entstehen oft inoffizielle Zugriffsrechte, die später niemand mehr nachvollziehen kann. Für Compliance und vor allem den sicheren und gezielten Einsatz von Copilot ist das ein echtes Problem: Copilot greift nur auf das zu, was technisch und berechtigungsseitig freigegeben ist – und damit im Zweifel auf zu viel.

WARUM DAS ALLES ENTSCHEIDEND IST – GERADE JETZT

- **Datenhygiene ist keine einmalige Aktion,** sondern ein kontinuierlicher Prozess – und ein zentrales Fundament für jede Art von datengetriebener Innovation.
- Wer Copilot, KI-Assistenten oder andere intelligente Systeme einführen will, braucht **saubere, strukturierte, aktuelle und korrekt berechtigte Daten.**
- Themen wie **Retention, Zugriffsanalyse und Oversharing-Reports** sind dabei keine technischen Randthemen – sie sind die Voraussetzung für Vertrauen, Compliance und effiziente KI-Nutzung.

AUFRÄUMEN IST DER ERSTE SCHRITT ZUR KI-REIFE

Wer heute beginnt, Retention-Regeln zu definieren, Zugriffsrechte zu bereinigen und Freigaben zu analysieren, schafft nicht nur Ordnung im Datenbestand, sondern legt die **Grundlage für eine sichere, skalierbare und verantwortungsvolle KI-Nutzung.**

Provectus unterstützt Sie gerne bei der Einführung praxisnaher Datenhygiene-Maßnahmen – von der technischen Umsetzung über Governance-Strukturen bis hin zur Nutzerbefähigung. Denn nur wer Ordnung schafft, kann auch intelligent automatisieren.

VOM AUFRÄUMEN ZUM EINORDNEN: WARUM DATEN-KLASSIFIZIERUNG DER NÄCHSTE LOGISCHE SCHRITT IST

Nachdem veraltete, unstrukturierte oder unberechtigte Daten identifiziert und bereinigt wurden, stellt sich die nächste zentrale Frage: **Welche Informationen sind wie schützenswert – und wer darf was womit tun?**
Hier kommt die Datenklassifizierung ins Spiel – als Schlüssel zu gelebter Datensouveränität, automatisiertem Schutz und klarer Compliance.

Die Datenklassifizierung ist ein zentraler Baustein der Informationssicherheit, Compliance und effizienten Datenverwaltung. Sie dient dazu, Informationen anhand ihres Schutzbedarfs in definierte Kategorien einzuordnen. Ihre Relevanz erstreckt sich über verschiedene Dimensionen:

1.

SCHUTZ SENSIBLER INFORMATIONEN

Nicht alle Daten sind gleich kritisch. Durch eine korrekte Klassifizierung können besonders schützenswerte Daten – etwa personenbezogene Daten, Geschäftsgeheimnisse oder vertrauliche Kommunikation – gezielt geschützt werden, z. B. durch Verschlüsselung, Zugriffsbeschränkungen oder Monitoring.

2.

EINHALTUNG GESETZLICHER UND REGULATORISCHER VORGABEN

Zahlreiche Vorgaben wie die DSGVO, ISO 27001, NIS2, DORA oder branchenspezifische Regularien verlangen eine strukturierte Kontrolle und Dokumentation sensibler Informationen. Datenklassifizierung ist oft eine Voraussetzung, um Compliance-Prüfungen zu bestehen.

3. RISIKOMINIMIERUNG

Unklassifizierte oder falsch klassifizierte Daten bergen Risiken: Datenpannen, unbefugte Zugriffe oder unzureichende Löschung können zu finanziellen Schäden oder Reputationsverlust führen. Klassifizierung hilft, Risiken gezielt zu identifizieren und zu adressieren.

4. EFFIZIENTES DATENMANAGEMENT

In der Praxis unterstützt die Klassifizierung auch organisatorische Ziele: Daten können effizienter gespeichert, archiviert oder gelöscht werden. Gerade bei wachsendem Datenvolumen ist das ein wesentlicher Vorteil für IT- und Datenschutzteams.

5. GRUNDLAGE FÜR AUTOMATISIERTE SCHUTZMASSNAHMEN

Viele Sicherheitslösungen – etwa Data Loss Prevention (DLP), Zugriffskontrollsysteme oder Verschlüsselungsmechanismen – greifen auf Klassifizierungen zurück, um automatisierte Entscheidungen zu treffen. Ohne saubere Klassifikation bleibt dieser Schutz wirkungslos.

6. KLASSIFIZIERTE DATEN SIND DIE GRUNDLAGE FÜR EFFIZIENTE KI-NUTZUNG

Daten sind der Treibstoff jeder KI – aber nicht alle Daten sind gleichwertig, und nicht alle dürfen gleich genutzt werden. Unklare Datenlagen führen zu Fehlern im Modelltraining, Datenschutzverstößen und blockieren produktive KI-Anwendungen, insbesondere in regulierten Branchen wie Finanzwesen oder Gesundheitswirtschaft.

RICHTIGE EINFÜHRUNG VON DATENKLASSIFIZIERUNG VS. GUT GEMEINTE EINFÜHRUNG VON DATENKLASSIFIZIERUNG

In vielen Organisationen treffen wir auf erste Ansätze zur Informationsklassifizierung – etwa in Form grober Datenanalysen oder vorhandener Rollenbeschreibungen. Doch häufig fehlt der entscheidende Schritt: die konsequente Umsetzung in einem technischen System und die Verankerung im operativen Alltag, die für alle Mitarbeitenden sinnvoll umsetzbar ist.
Ein typisches Beispiel ist Microsoft Purview: Die Plattform bietet mit Vertraulichkeitsbezeichnern (Sensitivity Labels) die Möglichkeit, Klassifizierungen direkt in Office-Anwendungen wie Word, Excel, PowerPoint oder Outlook sichtbar und nutzbar zu machen. Doch dafür muss die grundlegende Klassifikationslogik im Unternehmen erst sauber definiert und zugewiesen sein.

HERAUSFORDERUNG: VERANTWORTUNG UND ZUSTÄNDIGKEIT

Ein zentrales Problem ist dabei oft die fehlende Zuordnung von Verantwortung: Wer darf überhaupt festlegen, welchen Schutzbedarf eine Information hat? Diese Entscheidung kann und soll nicht bei Sachbearbeitern liegen. Sie erfordert ein übergeordnetes Verständnis für Prozesse, Risiken und regulatorische Anforderungen – und liegt daher idealerweise bei Fachbereichsverantwortlichen oder Prozesseignern.
Ein Beispiel: In der Buchhaltung müssen eingehende Rechnungen einen bestimmten Schutzbedarf erhalten – wie hoch dieser ist, sollte ein Verantwortlicher aus dem Bereich verbindlich definieren. Wichtig ist dabei, dass diese Entscheidungen **einheitlich und unternehmensweit koordiniert** getroffen werden.

LÖSUNGSANSATZ: STRUKTURIERTE BEGLEITUNG UND METHODIK

Wir begleiten Organisationen in diesem Prozess gezielt.

Durch Interviews mit den Fachbereichen, moderierte Workshops und methodische Unterstützung helfen wir dabei, Klarheit zu schaffen:

- **Welche Informationen existieren?**
- **Wer ist deren Eigentümer?**
- **Wie schützenswert sind sie?**
- **Welche Schutzbedarfsklassen gelten unternehmensweit?**

Dabei etablieren wir sogenannte Informationscluster – strukturierte Gruppierungen von Informationen, die sich idealerweise mit konkreten Vertraulichkeitsbezeichnern abbilden lassen. Das erleichtert die technische Umsetzung in Purview erheblich und sorgt für Konsistenz und Skalierbarkeit.

KLASSIFIKATION ALS ORIENTIERUNGSHILFE – NICHT ALS HÜRDE

Im Kern funktioniert eine Klassifikation wie eine Art Schablone: Jede Information – das „Puzzlestück" – hat eine bestimmte Form, z. B. „dreieckig", und wird durch einen passenden „Schlitz" eingeordnet – etwa die Klassifikationsstufe 2. Dieser Zuordnungsprozess wurde im Vorfeld bereits durch die zuständigen Fachverantwortlichen definiert und in Microsoft Purview technisch abgebildet.
Das bedeutet: **Mitarbeitende müssen die Schutzbedarfe nicht selbst bewerten oder festlegen.**
Sie wenden lediglich die vorhandenen Klassifizierungslabel an – etwa in Word, Outlook oder Excel. Trotzdem entstehen in der Praxis Unsicherheiten oder Sonderfälle, bei denen Unterstützung erforderlich ist.

INFORMATIONSKLASSIFIZIERUNG VERSTÄNDLICH MACHEN – MIT CARE TAKERS ALS BRÜCKENBAUER IM UNTERNEHMEN

Ein erfolgreiches Informationsklassifizierungsmodell lebt nicht nur von gut definierten Richtlinien, sondern vor allem von der Praxisnähe und Umsetzbarkeit im Arbeitsalltag. Um dies zu gewährleisten, setzen wir auf eine klare Rollentrennung und gezielte Unterstützung der Mitarbeitenden durch sogenannte Information Classification Care Taker.

DIE ROLLE DER INFORMATION CLASSIFICATION CARE TAKER

Um diese Lücke zu schließen, empfehlen wir die Etablierung einer dedizierten Rolle. Der Information Classification Care Taker fungiert als eine Art „Brückenbauer“ zwischen den strategischen Entscheidungen der Fachbereichsleitung und den praktischen Anforderungen im Arbeitsalltag.

Diese Personen agieren als Ansprechpartner für Kollegen bei Fragen zur Klassifizierung, sorgen für Orientierung und Unterstützung bei Unsicherheiten im Umgang mit Labels fördern die Akzeptanz der Klassifizierung durch informelle Schulung und Vorbildfunktion, und helfen bei der Verankerung der Prozesse in den Teams.

Idealerweise handelt es sich um engagierte, kommunikative Mitarbeitende aus den Fachbereichen – häufig bereits in vergleichbaren Rollen wie Multiplikatoren, Power User oder Key User tätig. Falls solche Strukturen nicht vorhanden sind, können Care Taker gezielt aufgebaut und geschult werden.

AUFBAU UND EINFÜHRUNG: STRUKTURIERT & PRAXISNAH

Bevor Klassifizierungsfunktionen wie Sensitivity Labels breit ausgerollt werden, erfolgt die Identifikation und Befähigung dieser Care Taker. In Schulungen und mit praxisnahen Materialien werden sie in die Lage versetzt, ihre Kollegen im Umgang mit der Informationsklassifizierung kompetent zu begleiten.

Der Fachbereichsleiter, der den Schutzbedarf initial definiert hat, bleibt dabei entlastet – er hat seine Aufgabe erfüllt. Die Care Taker stellen sicher, dass das Wissen in die Breite getragen wird, ohne jedes Mal auf zentrale Stellen zurückgreifen zu müssen.

NACHHALTIGKEIT DURCH INTEGRATION

Am Ende steht nicht nur eine theoretische Klassifizierung, sondern eine lebensnahe, im System integrierte Lösung, die Mitarbeitende aktiv unterstützt – durch sichtbare Labels, automatische Schutzmaßnahmen und klare Zuständigkeiten. So wird Informationsklassifizierung nicht zum einmaligen Projekt, sondern zu einem nachhaltigen Bestandteil der Sicherheitskultur.

HÜRDEN 2:

TECHNOLOGISCHE ALTLASTEN, UNZUREICHENDE SECURITY & FEHLENDE SICHERHEITSSTRATEGIE

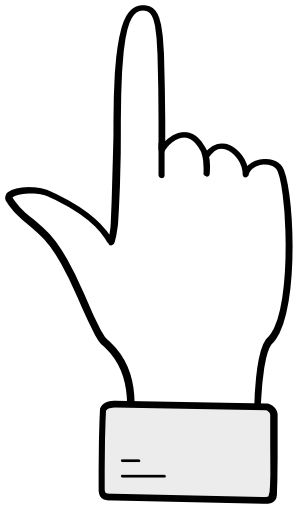
Deutschland befindet sich bei der Umsetzung von KI- und Cloud-Technologien noch immer am Anfang eines tiefgreifenden digitalen Wandels. Um diesen Weg sicher und zukunftsfähig zu gestalten, braucht es mehr als punktuelle Modernisierungen: **Security-by-Design, konsequente technologische Erneuerung und moderne Sicherheitsparadigmen wie Zero Trust sind unerlässlich.**

Unternehmen müssen jetzt den Mut aufbringen, ganzheitliche Sicherheits- und Digitalstrategien zu entwickeln, die nicht nur den regulatorischen Anforderungen (z. B. DSGVO, NIS2, AI Act) standhalten, sondern vor allem stabile, skalierbare und resiliente IT-Infrastrukturen schaffen. Ohne diese Grundlagen drohen technologisches Abgehängt sein, erhebliche Sicherheitslücken – und letztlich der Verlust von Vertrauen bei Kunden, Partnern und Aufsichtsbehörden.

DIE REALITÄT: STRUKTURELLE DEFIZITE UND STEIGENDE RISIKEN

Tatsächlich aber dominieren vielerorts noch technologische Altlasten: veraltete Betriebssysteme, unzureichend gepatchte Software, mangelhafte Netzwerksegmentierung und Insel-Lösungen ohne strategischen Kontext. Besonders Behörden sowie kleine und mittlere Unternehmen (KMU) leiden unter Ressourcenknappheit und fehlender IT-Sicherheitskompetenz.

Die rasante Einführung von Cloud-Lösungen, Remote-Work-Strukturen und das Wachstum von IoT-Landschaften haben die Angriffsflächen deutlich erweitert. Gleichzeitig wachsen durch neue Technologien wie künstliche Intelligenz die Komplexität der Systeme und die potenziellen Schwachstellen. Reaktive Sicherheitsmaßnahmen genügen längst nicht mehr – es braucht präventive, kontinuierliche und adaptive Strategien, die mit dem technologischen Wandel mitwachsen.



ZERO TRUST ALS SCHLÜSSEL: PARADIGMENWECHSEL IN DER IT-SICHERHEIT

Ein zentraler Baustein moderner Sicherheitsarchitekturen ist das **Zero Trust Modell – ein grundlegend neuer Denkansatz,** der sich vom klassischen Perimeterschutz verabschiedet.

WAS BEDEUTET ZERO TRUST?

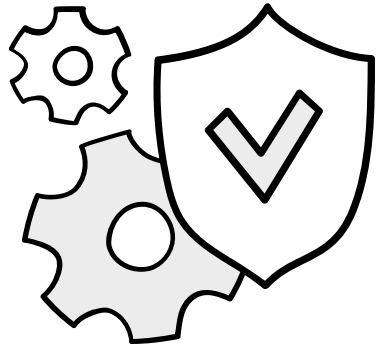
Zero Trust folgt dem Prinzip: **„Vertraue niemandem – weder innerhalb noch außerhalb des Netzwerks."** Jeder Zugriff – unabhängig vom Ort, vom Nutzer oder vom Gerät – wird standardmäßig als potenziell unsicher bewertet und muss kontinuierlich authentifiziert, autorisiert und geprüft werden.

MEHR ALS EIN TOOL: ZERO TRUST IST EIN SICHERHEITSPROZESS

Zero Trust ist keine einzelne Lösung oder Software, sondern ein dynamisches Sicherheitskonzept, das auf zentralen Prinzipien basiert:

- **Least Privilege Access:** Nur der notwendige Zugriff wird gewährt – und auch dieser zeitlich und kontextbezogen limitiert.
- **Microsegmentation:** IT-Systeme werden fein granular voneinander getrennt, um Angriffe lokal zu isolieren.
- **Kontinuierliches Monitoring:** Sicherheit ist kein einmaliger Zustand, sondern ein fortlaufender Prüfprozess.

Durch die konsequente Umsetzung von Zero Trust lassen sich **Angriffsflächen minimieren, laterale Bewegungen von Angreifern verhindern und Sicherheitslücken frühzeitig erkennen.**

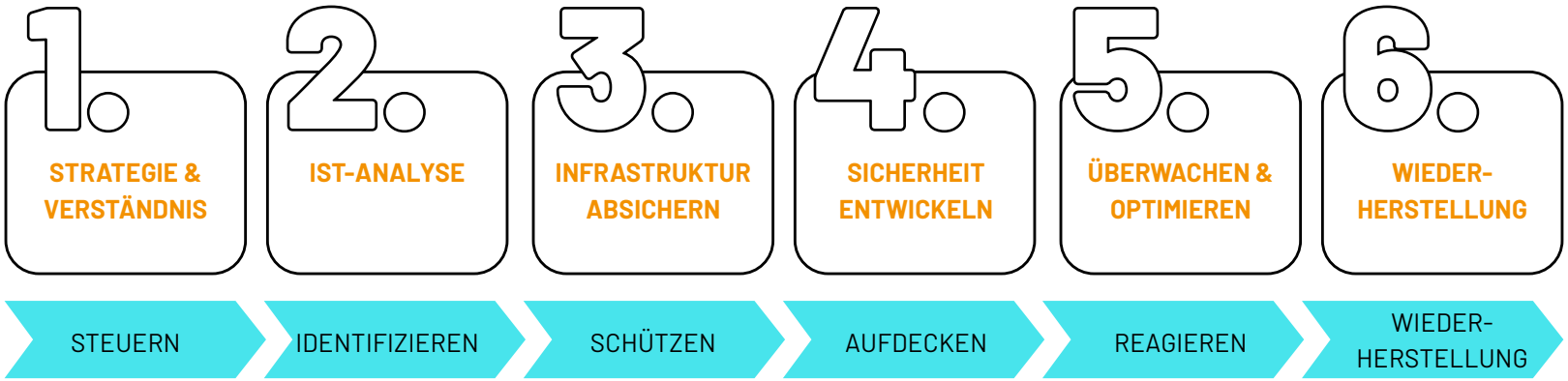


HANDLUNGSEMPFEHLUNG: JETZT MIT DEM WANDEL BEGINNEN

Unternehmen sollten nicht länger warten, sondern ihre Sicherheitsstrategie **jetzt strategisch neu aufzustellen.** Ein sinnvoller Startpunkt ist eine umfassende IST-Analyse der aktuellen IT- und Sicherheitslandschaft:

- Welche Systeme sind am stärksten gefährdet?
- Wo existieren unkontrollierte Zugänge oder nicht gepatchte Schwachstellen?
- Wie werden Zugriffsrechte aktuell vergeben und überwacht?

Im Anschluss sollten **Prioritäten identifiziert** und eine Roadmap entwickelt werden, um sukzessive auf eine Zero Trust Architektur hinzuarbeiten – abgestimmt auf die jeweiligen technischen, organisatorischen und regulatorischen Rahmenbedingungen.

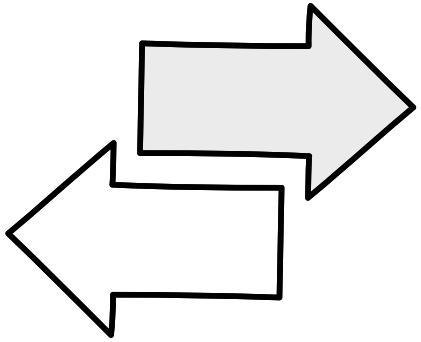


HÜRDEN 3:

UNKLARE REGULATORISCHE RAHMENBEDINGUNGEN – RECHTS-KONFORMITÄT ALS KRITISCHER ERFOLGSFAKTOR FÜR KI

Künstliche Intelligenz entfaltet ihr volles Potenzial nur dann, wenn sie nicht nur effizient, sondern auch rechtskonform betrieben wird. In Deutschland und der EU sehen sich Unternehmen mit einem zunehmend komplexen Regelwerk konfrontiert, das sowohl datenschutzrechtliche als auch ethische und branchenspezifische Anforderungen umfasst.

Insbesondere der EU AI Act, in Kombination mit der Datenschutz-Grundverordnung (DSGVO) sowie regulatorischen Branchenvorschriften z. B. im Gesundheitswesen oder der Finanzbranche, macht deutlich: **Rechtssicherheit ist kein optionaler Nebenaspekt – sie ist ein zentrales Element nachhaltiger KI-Strategien.**



WAS BEDEUTET DAS KONKRET?

Unternehmen müssen also, wie in Hürde 1 bereits beschrieben, detailliert prüfen:

- Welche Daten dürfen für KI-Anwendungen überhaupt verarbeitet werden?

>> Insbesondere bei personenbezogenen oder sensiblen Daten (Gesundheit, Verhalten, Ethnie etc.) sind strenge rechtliche Vorgaben einzuhalten.

- Wie wird die Nachvollziehbarkeit und Erklärbarkeit automatisierter Entscheidungen gewährleistet?

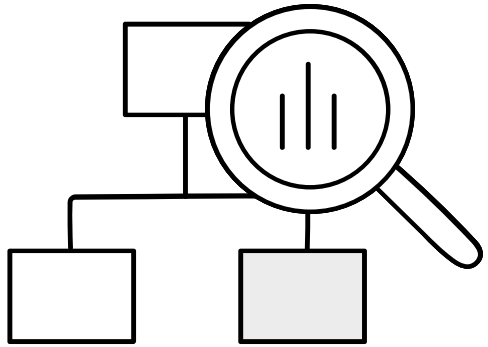
>> Blackbox-Modelle ohne dokumentierte Entscheidungslogik sind in vielen Anwendungsfällen (z. B. Kreditscoring, Personalentscheidungen) nicht zulässig.

- Welche Transparenz- und Informationspflichten bestehen gegenüber Nutzenden, Betroffenen oder Aufsichtsbehörden?

>> Der Einsatz von KI muss offengelegt und erklärbar gemacht werden – nicht nur technisch, sondern auch für juristische und nicht-technische Zielgruppen.

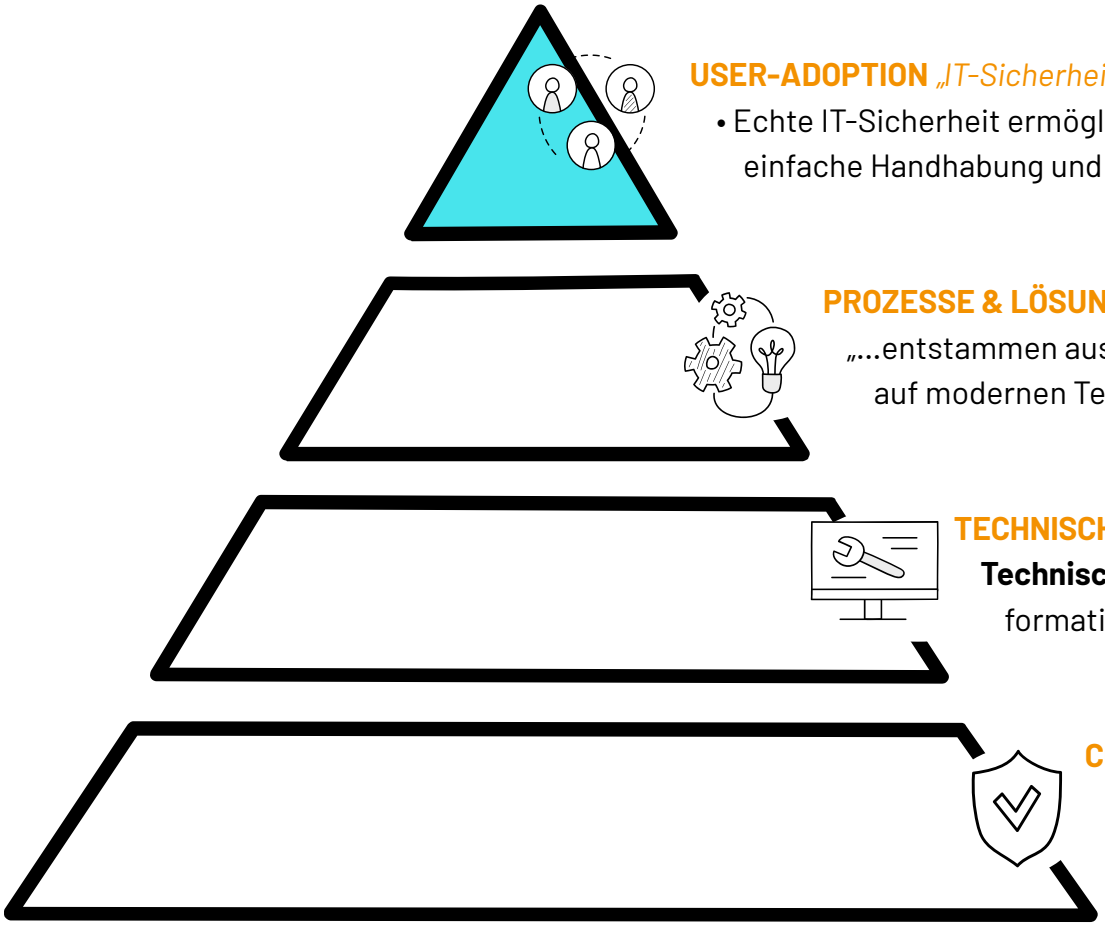
EMPFEHLUNG: RECHTLICHE SEITE IMMER FRÜHZEITIG MITDENKEN

Damit KI-Projekte tragfähig und zukunftssicher sind, sollte die **rechtliche Prüfung nicht am Ende, sondern zu Beginn** jeder Initiative stattfinden. Wir denken daher IT-Compliance & IT-Security immer gemeinsam, kombiniert mit Adoption-Maßnahmen, um die User mitzunehmen, zu sensibilisieren und ebenso KI-Ready zu machen.



ELEMENTE EINER STABILEN SICHERHEITS-PYRAMIDE

COMPLIANCE BY DEFAULT. SECURITY BY DESIGN. ADOPTION BY INTENTION.



USER-ADOPTION *„IT-Sicherheit endet nicht beim System – sie beginnt beim Nutzer."*

- Echte IT-Sicherheit ermöglichen durch verständliche Regeln, einfache Handhabung und gezielte Kommunikation.

PROZESSE & LÖSUNGEN *„Pragmatisch, nutzbar & modern."*

„....entstammen aus beiden Welten – rechtlich fundiert und basierend auf modernen Technologien."

TECHNISCHE SICHERHEITSARCHITEKTUR *„Immer mitgedacht, von Anfang an."*

Technische Sicherheitsarchitekturen (Zero Trust, H2SIS Handlungen, Informationssicherheit, DLP etc.) leisten die erforderliche Schutzwirkung.

COMPLIANCE *„Rechtskonformität als Standard. Nicht als Ausnahme."*

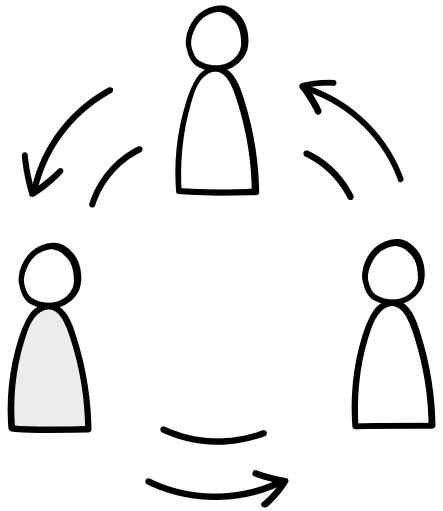
Rechtliche Anforderungen und Standards (z. B. BDSGVO, ISO 27001, NIS2, DORA) müssen stetig erfüllt werden.

HÜRDEN 4:

FEHLENDES KNOW-HOW UND MANGELNDE INTERDISZIPLINÄRE ZUSAMMENARBEIT – KOMPETENZ ALS SCHLÜSSEL ZUM KI-ERFOLG

Viele Unternehmen haben ambitionierte Vorstellungen davon, was sie mit Künstlicher Intelligenz erreichen wollen. Doch in der Umsetzung zeigt sich: **Es fehlt weniger an Visionen als an Fähigkeiten.**

Ein zentrales Hemmnis für erfolgreiche KI-Projekte ist das unzureichende domänenübergreifende Know-how. Denn KI-Initiativen erfordern weit mehr als nur Machine Learning – sie sind komplexe Transformationsprojekte, die technische, organisatorische und regulatorische Aspekte intelligent miteinander verknüpfen müssen.



WO GENAU LIEGT DAS PROBLEM?

1. FACHLICH-TECHNISCHE ISOLATION, WENN SILOS INNOVATION AUSBREMSEN

Ein zentrales Hindernis für erfolgreiche KI-Projekte liegt in der **fehlenden Verzahnung zwischen Fachlichkeit, Datenkompetenz und IT-Struktur.** In vielen Unternehmen agieren zentrale Teams nebeneinander – statt miteinander.

- **Data Scientists** entwickeln komplexe Modelle, haben jedoch oft nur begrenzten Einblick in die tatsächlichen Geschäftsprozesse oder die operativen Anforderungen.
- **Fachabteilungen** formulieren Use Cases und Erwartungen, ohne die algorithmischen Grenzen oder datenbasierten Voraussetzungen zu verstehen.
- **IT-Teams** betreiben die technische Infrastruktur, sind aber häufig nicht in strategische Datenfragen oder die Architektur der KI-Anwendungen eingebunden.

Besonders kritisch: Auch innerhalb der IT selbst fehlt es vielerorts an Abstimmung. Strategien und Herangehensweisen werden isoliert entwickelt, ohne ein gemeinsames Zielbild. So entstehen unnötige Reibungsverluste – und das Potenzial moderner Technologien bleibt ungenutzt.
Was es braucht, ist ein echter Schulterschluss zwischen allen Beteiligten – von der Fachabteilung über das Data-Team bis zur Infrastruktur. Nur wenn alle an einem Strang ziehen, kann aus Technologie tatsächlicher Nutzen entstehen.

2. UNKLARE ROLLEN UND VERANTWORTLICHKEITEN

- Welche Daten dürfen von wem benutzt werden?
- Wer besitzt ein KI-Modell – die IT, das Data-Team, das Fachgebiet?
- Wer trägt Verantwortung für Modelltraining, Wartung, Validierung oder Stilllegung?

- Wer entscheidet, ob und wann ein Modell in Produktion geht oder abgeschaltet wird?

Solche Fragen bleiben in vielen Organisationen unbeantwortet.

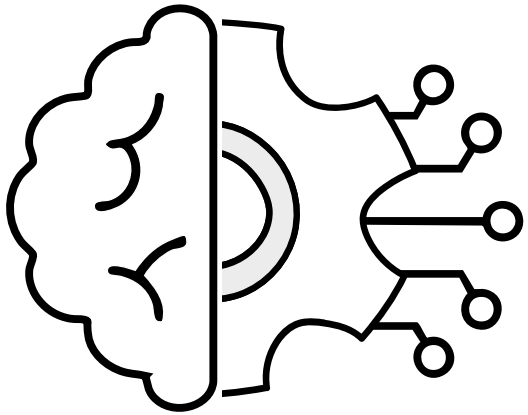
LÖSUNG: AUFBAU INTERDISZIPLINÄRER KI-KOMPETENZZENTREN

Ein zukunftsfähiger KI-Einsatz erfordert Teams, die disziplinübergreifend zusammenarbeiten, gemeinsam denken und auf Augenhöhe kommunizieren. Die Integration von Data Science, IT, Security, Recht, Ethik und Fachabteilungen ist kein "Nice to have", sondern zwingend notwendig.

WICHTIGE ROLLEN IN ERFOLGREICHEN KI-PROJEKTEN:

- **AI Product Owner:** Verantwortlich für Strategie, Business-Alignment und Priorisierung der KI-Vorhaben.
- **Data Scientist / ML Engineer:** Entwickeln und validieren KI-Modelle technisch und methodisch.
- **Data Steward:** Kümmert sich um Datenqualität, Herkunft (Lineage) und semantisches Verständnis.
- **Security & Compliance Officer:** Stellt sicher, dass Modelle sicher und regelkonform betrieben werden.
- **Change & Enablement Manager:** Unterstützt die Organisation bei Akzeptanz und Adaption neuer Technologien.

Solche Rollen müssen klar beschrieben, organisatorisch verankert und mit Entscheidungskompetenz ausgestattet werden – andernfalls versanden Projekte im Kompetenzgerangel oder laufen an realen Bedarfen vorbei.



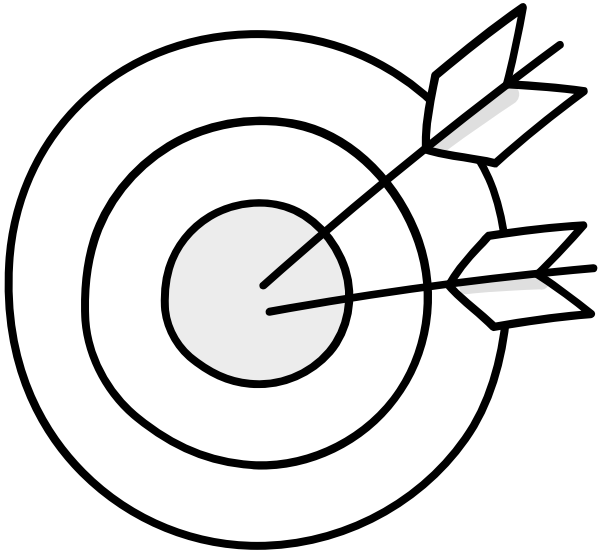
EMPFEHLUNG: QUALIFIZIERUNG, STRUKTUR UND KULTUR SCHAFFEN

- **Investieren Sie gezielt in Weiterbildung:** Nicht nur im Tech-Team, sondern auch in Fachabteilungen, Management und Support-Funktionen – etwa durch Trainings zu KI-Ethik, Prompt Engineering, Explainability oder regulatorischem Know-how.

- **Etablieren Sie interdisziplinäre KI-Teams oder "AI Competence Center":** Diese können als interne Drehscheiben für Wissen, Projektsteuerung und Governance fungieren.

- **Fördern Sie eine offene Innovationskultur:** Teams müssen lernen, in Hypothesen zu denken, datenbasiert zu arbeiten und Unsicherheiten als Teil des Lernprozesses zu akzeptieren.

- **Schaffen Sie ein stabiles Fundament aus IT-Sicherheit und Compliance:** Nur auf einer belastbaren, resilienten Basis lassen sich KI-Innovationen nachhaltig und vertrauenswürdig umsetzen. Prüfen und stärken Sie Ihre bestehenden Sicherheits- und Governance-Strukturen – sie müssen nicht nur heutigen Anforderungen genügen, sondern sich auch dynamisch an neue Technologien, Geschäftsmodelle und Regulierungen anpassen können. So wird Innovation nicht zum Risiko, sondern zur strategischen Stärke.



HÜRDEN 5:

ZÖGERLICHE INNOVATIONSKULTUR UND INTERNE BLOCKADEN – UNSICHERHEIT ALS INNOVATIONSBREMSE

In vielen Unternehmen sind die Technologie und Anwendungsszenarien längst vorhanden, doch der eigentliche Stillstand beginnt intern: KI-Initiativen scheitern nicht selten an Widerständen, die sich weniger aus tatsächlichen Risiken als aus wahrgenommenen Unsicherheiten speisen. Vor allem Datenschutzbedenken, Bedenken des Betriebsrats oder ethische Fragen führen dazu, dass vielversprechende Projekte verzögert, eingeschränkt oder ganz gestoppt werden. Diese Bedenken sind wie in den vorherig angeführten Hürden durchaus berechtigt, können aber beseitigt und bedient werden.

DIE URSACHEN SIND HÄUFIG STRUKTURELLER UND KULTURELLER NATUR:

- **Mangelnde Transparenz** über Datenflüsse und Verarbeitungslogiken
- **Unklare Verwendungszwecke** von KI-gestützten Systemen
- **Unsicherheit im Umgang mit sensiblen oder personenbezogenen Daten**
- Fehlende Kenntnisse über rechtliche und technische Schutzmechanismen
- Zu wenig Investitionen in IT-Sicherheitsmaßnahmen

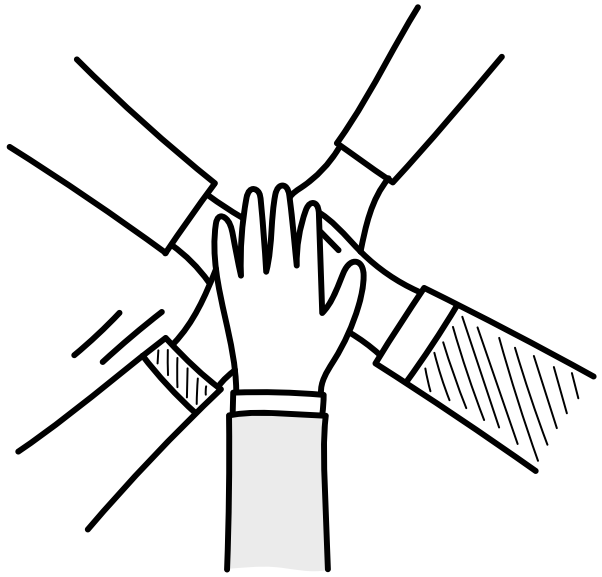
Ohne ein belastbares Datenschutz- und Kommunikationskonzept entsteht ein Klima der Vorsicht und des Misstrauens. Die Folge: interne Blockaden, verlorenes Vertrauen und ein lähmender Innovationsstillstand – selbst bei technisch ausgereiften Lösungen.

EMPFEHLUNG: AUFRÜSTUNG, AUFKLÄRUNG, EINBINDUNG UND GEZIELTE KOMPETENZVERMITTLUNG

Neben der technischen Absicherung, braucht es eine proaktive, transparente und interdisziplinäre Kommunikation. Binden Sie Datenschutzbeauftragte, Betriebsräte und Fachverantwortliche frühzeitig in Ihre KI-Initiativen ein – nicht als Genehmigungsinstanz am Ende, sondern als aktive Partner im Gestaltungsprozess. Privacy-by-Design sollte kein Add-on, sondern ein integraler Bestandteil jedes KI-Projekts sein.

Zudem ist es entscheidend zu erkennen: Viele Vorbehalte entstehen aus Unwissenheit, nicht aus Ablehnung. Genau hier setzt unser Whitepaper an. Es zeigt auf, welche Stellschrauben Sie drehen müssen, um aus interner Skepsis produktive Mitgestaltung zu machen – und wie Sie durch gezielte Aufklärung und Governance-Strukturen eine tragfähige Innovationskultur schaffen können.

So wird KI nicht zum Streitpunkt, sondern zur gemeinsam getragenen Zukunftsstrategie.



GUTE NACHRICHT

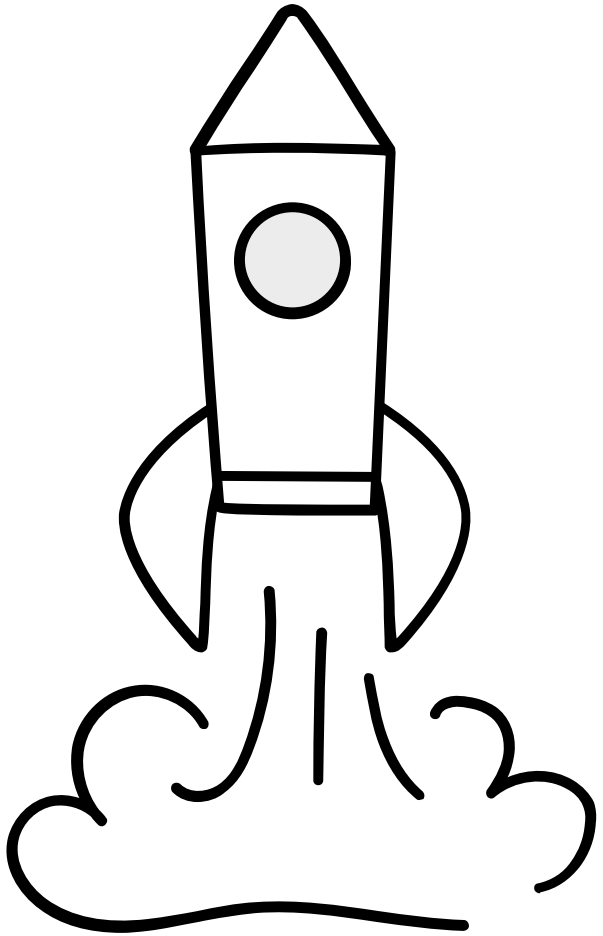
Trotz Nachholbedarf: Schon heute **sicher und datenschutzkonform** von KI profitieren

Gerade weil in vielen Unternehmen noch ein spürbarer Nachholbedarf beim Thema Künstliche Intelligenz besteht, ist jetzt der ideale Zeitpunkt, den ersten Schritt zu gehen. Viele Verantwortliche fühlen sich angesichts der Vielzahl technischer, organisatorischer und regulatorischer Anforderungen überfordert – die Folge: Stillstand aus Unsicherheit. **Doch anstatt in Schockstarre zu verfallen, lohnt es sich, den Weg zur KI-Nutzung strukturiert und schrittweise anzugehen.** Wir begleiten Sie dabei – mit Erfahrung, Klarheit und praktikablen Lösungen.

DIE GUTE NACHRICHT:
SIE KÖNNEN AUCH JETZT SCHON PROFITIEREN.

Auch wenn noch nicht alle Stellschrauben perfekt eingestellt sind, gibt es sichere und DSGVO-konforme Wege, bereits heute konkreten Mehrwert aus KI zu ziehen. Ein Beispiel dafür ist Know-Now.AI – der smarte Unternehmensassistent von Provectus.

Dieser KI-gestützte Assistent bereitet internes Wissen gezielt auf und stellt es in einer intuitiven Chat-Oberfläche bereit. So können Teams schneller, sicherer und effizienter arbeiten – ganz ohne Schatten-IT oder aufwendige Integrationsprojekte.



KNOW-NOW.AI BIETET IHNEN:

SICHERHEIT & COMPLIANCE:

Smarte KI-Lösung im eigenen Microsoft-Tenant – vollständig kontrolliert, DSGVO-konform und ohne Risiken durch Schatten-IT.

SCHNELL INTEGRIERT, SOFORT EFFIZIENT:

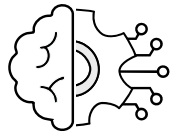
Auf Basis von Microsoft Azure und OpenAI – ganz ohne zusätzliche Copilot-Lizenzen oder komplexe Lizenzmodelle.

WISSENSSCHATZ INTERN NUTZBAR MACHEN:

Unternehmenswissen auf Abruf – ohne langes Suchen, ohne Wissensinseln, ohne Reibungsverluste.

FÜR DEN MITTELSTAND GEMACHT:

KI-Erfolg ohne Mammutprojekt – pragmatisch, skalierbar, und zugeschnitten auf die Realität mittelständischer Unternehmen.



INTERNE INTELLIGENZ STATT EXTERNER RISIKEN:

Eine KI, die nicht nach außen spricht – aber intern echten Nutzen stiftet.

FAZIT

Jetzt ist die Zeit, die Hausaufgaben zu machen – bevor es zu spät ist

Künstliche Intelligenz ist nicht länger Zukunft – sie ist längst Realität. Und doch zeigt sich eindrücklich: In vielen Unternehmen fehlt es noch an den notwendigen technischen und organisatorischen Grundlagen, um KI wirklich effizient und verantwortungsvoll zu nutzen.

Ob veraltete IT-Infrastrukturen, mangelhafte Datenstrategie, unscharfe Zuständigkeiten oder kulturelle Blockaden – die Versäumnisse der letzten Jahre lassen sich nicht länger ignorieren. Mit jedem Monat, der vergeht, ohne dass Strukturen modernisiert und Kompetenzen aufgebaut werden, wird der Rückstand größer – und der Anschluss an zukunftsfähige Märkte schwieriger.

Die gute Nachricht: Der Anfang ist möglich – und notwendig

Jetzt ist der richtige Zeitpunkt, um mit klarer Priorisierung die **notwendigen Hausaufgaben anzugehen:**

- **Technisch,** durch den Aufbau sicherer, skalierbarer und KI-fähiger Infrastrukturen, modernem Datenschutz und Governance.
- **Organisatorisch,** durch transparente Prozesse, klare Rollen und gelebte Zusammenarbeit zwischen Fachbereichen, IT, Compliance und Data Teams.
- **Kulturell,** durch ein neues Mindset: vom Zögern zum Gestalten, vom Abwarten zur Umsetzung.

Provectus unterstützt Sie auf diesem Weg – mit strategischer Klarheit, technischer Expertise, Compliance-Beratung und praxisnaher Begleitung, damit Sie Ihre KI-Hausaufgaben nicht nur machen, sondern erfolgreich meistern.

SIND SIE BEREIT, IHRE KI-HAUSAUFGABEN ZU MACHEN – BEVOR ES ZU SPÄT IST?

Wir beseitigen Hürden pragmatisch: Datenhygiene & Klassifizierung, Zero-Trust-Security, Compliance und Enablement. Mit Provectus kommen Sie von der Idee zu messbarem Nutzen – auf Wunsch mit Know-Now.AI als sicherem Start. Sprechen Sie mit Jakob.

Sprechen Sie mit uns!

IHR ANSPRECHPARTNER:
Jakob Beckmann | Sales Manager
jakob@provectus.de
+49 (0) 89 710 409 20