KI, Datenschutz und IT-Sicherheit. Geht das zusammen?

eDay Salzburg 2026

Martin Höck | Solutionbox GmbH

KI sicher und verantwortungsvoll einsetzen

17.03.2026

WKS
Unternehmensberatung · Buchhaltung · IT

Martin Höck
Unternehmer, IT-Experte, Gerichtssachverständiger

Solutionbox Informationstechnologie GmbH
und Solutionbox Consulting GmbH,

Salzburg. Linz, Zeltweg

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für IT.

Schwerpunkte: IT-Sicherheit, Datenschutz, KI-Einsatz und Digitalisierung für KMUs.

solutionbox
Informationstechnologie GmbH
Wir haben die Lösung!

17.03.2026

WKS
Unternehmensberatung · Buchhaltung · IT

Noch ein Thema,
das ich nicht bestellt habe ...

17.03.2026

WKS
Unternehmensberatung · Buchhaltung · IT

KI im KMU-Alltag
Wo KI bereits passiert

- Bewusst: ChatGPT, Claude, Copilot, KI-Chatbots
- Halb bewusst: Outlook-Vorschläge, Buchhaltungshilfen
- Unsichtbar: Spamfilter, Suchmaschinen, Sicherheit

Die Frage ist nicht ob. Sondern wie.

17.03.2026

WKS
Unternehmensberatung · Buchhaltung · IT

Drei Spannungsfelder

Spannungsfeld 1: DSGVO
Was passiert mit Daten in KI-Tools?

Ihre Assistentin kopiert 20 Kundendatensätze in ChatGPT, um Anschreiben zu erstellen.

Personenbezogene Daten landen auf einem US-Server. Ohne Rechtsgrundlage.

Die DSGVO verbietet KI nicht. Aber sie verbietet Sorglosigkeit.

Es gibt DSGVO-konforme Lösungen: ChatGPT Enterprise, Copilot im Firmenkonto.

Die DSGVO verbietet KI nicht. Aber sie verbietet Sorglosigkeit.

17.03.2026

WKS
Unternehmensberatung · Buchhaltung · IT

Spannungsfeld 2: AI Act
Was KMUs wissen müssen

- Seit 2024 in Kraft. Betrifft primär KI-Hersteller.
- Hochrisiko: Bewerberauswahl, Kreditentscheidungen
- GF-Haftung: Unwissenheit schützt nicht vor Strafe

Risikostufen

VERBOTEN

Inakzeptables Risiko

Social Scoring
Manipulation
Emotionserkennung am Arbeitsplatz

Seit Feb. 2025 illegal!

HOHES RISIKO

Streng reguliert

Bewerberauswahl
Kreditentscheidung
Mitarbeiterbewertung
Medizinprodukte

Ab Aug. 2026/2027

BEGRENZTES RISIKO

Transparenzpflicht

Chatbots
KI-generierte Texte
Deepfakes

Nutzer informieren!
Ab Aug. 2026

MINIMALES RISIKO

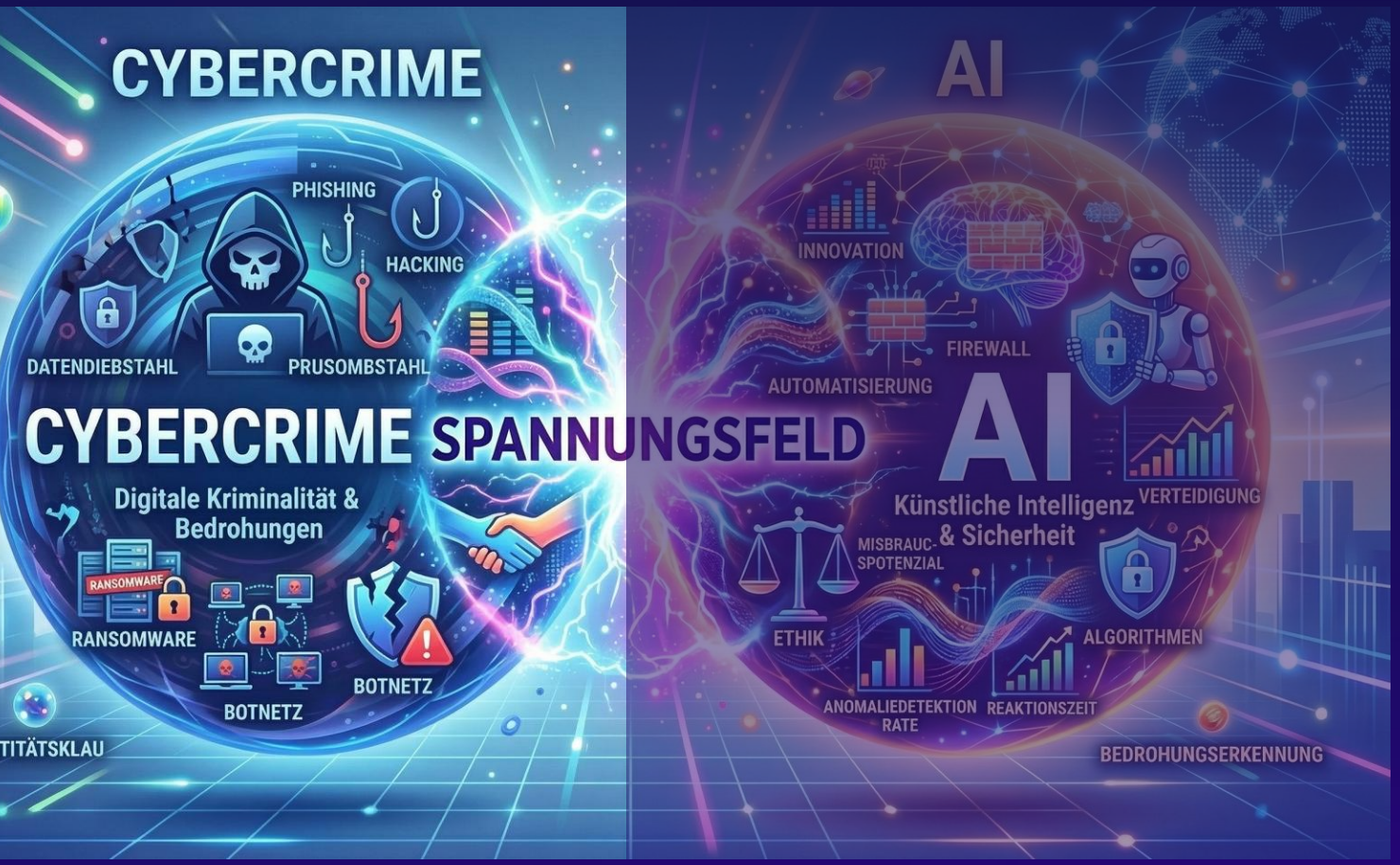
Keine Auflagen

ChatGPT / Copilot
Spamfilter
Übersetzungstools
Buchhaltungshilfen

DSGVO gilt weiterhin!

Kein Bürokratiemonster. Aber Unwissenheit schützt NICHT vor Strafe.

Spannungsfeld 3: IT-Sicherheit
KI als Waffe und als Schutzschild



KI-Phishing: Perfektes Deutsch, persönlicher Tonfall, Bezug auf reale Projekte.

CEO-Fraud 2.0: Deepfake-Stimmen aus 3 Minuten Audiomaterial.

KMUs sind attraktive Ziele: weniger Schutz, aber wertvolle Daten.

Shadow AI: Mitarbeiter nutzen KI-Tools ohne Freigabe oder Wissen der IT.

IT-Sicherheit und KI
Einfallstor und Schutzschild zugleich

- KI erkennt Anomalien in Echtzeit, 24/7
- Klare Freigabelisten statt Verbote
- Sicherheitslücke sitzt am Schreibtisch

WKS
Unternehmensberatung · Buchhaltung · IT

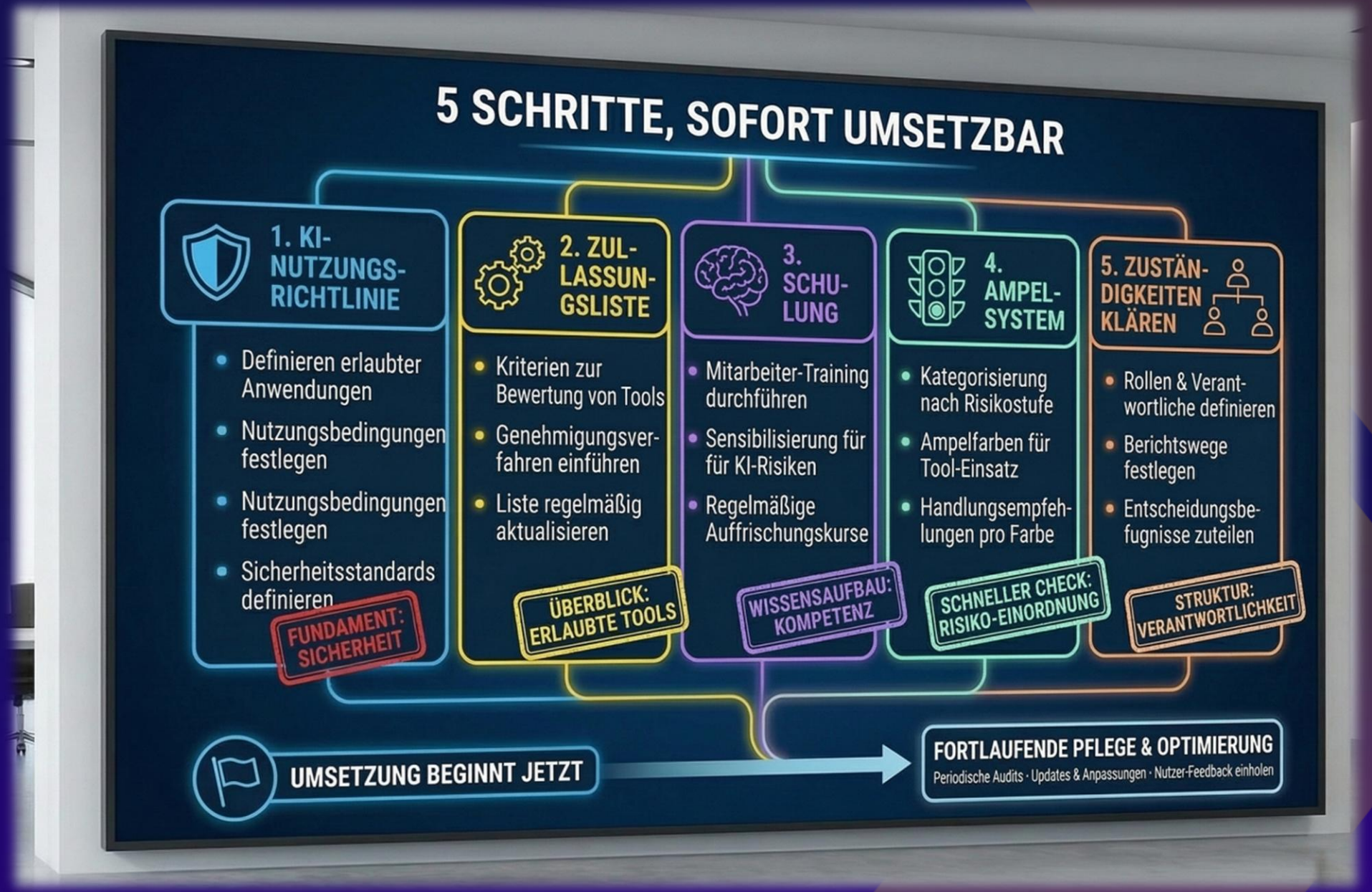
Die größte Sicherheitslücke sitzt nicht im Server. Sie sitzt am Schreibtisch.

Wir sollten eigenes Interesse haben,
unsere Daten zu schützen.

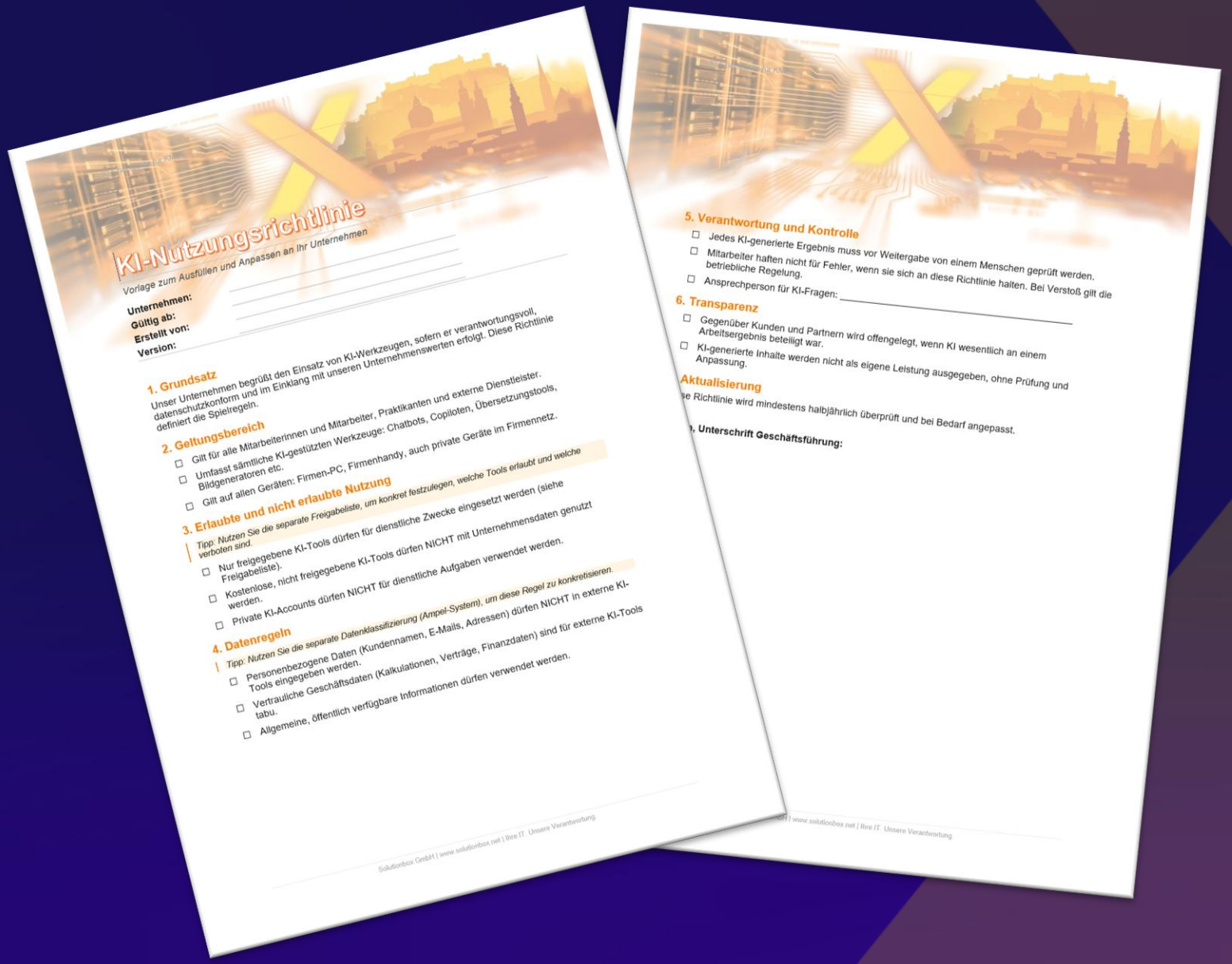
Nicht
weil es ein Gesetz verlangt.

Was tun?

Fünf Schritte - Sofort umsetzbar



KI-Nutzungsrichtlinie



KI-Nutzungsrichtlinie

Vorlage zum Ausfüllen und Anpassen an Ihr Unternehmen

Unternehmen:
Gültig ab:
Erstellt von:
Version:

1. Grundsatz

Unser Unternehmen begrüßt den Einsatz von KI-Werkzeugen, sofern er verantwortungsvoll, datenschutzkonform und im Einklang mit unseren Unternehmenswerten erfolgt. Diese Richtlinie definiert die Spielregeln.

2. Geltungsbereich

- ☐ Gilt für alle Mitarbeiterinnen und Mitarbeiter, Praktikanten und externe Dienstleister.
- ☐ Umfasst sämtliche KI-gestützten Werkzeuge: Chatbots, Copiloten, Übersetzungstools, Bildgeneratoren etc.
- ☐ Gilt auf allen Geräten: Firmen-PC, Firmenhandy, auch private Geräte im Firmennetz.

3. Erlaubte und nicht erlaubte Nutzung

Tipp: Nutzen Sie die separate Freigabeliste, um konkret festzulegen, welche Tools erlaubt und welche verboten sind.

- ☐ Nur freigegebene KI-Tools dürfen für dienstliche Zwecke eingesetzt werden (siehe Freigabeliste).
- ☐ Kostenlose, nicht freigegebene KI-Tools dürfen NICHT mit Unternehmensdaten genutzt werden.
- ☐ Private KI-Accounts dürfen NICHT für dienstliche Aufgaben verwendet werden.

4. Datenregeln

Tipp: Nutzen Sie die separate Datenklassifizierung (Ampel-System), um diese Regel zu konkretisieren.

- ☐ Personenbezogene Daten (Kundennamen, E-Mails, Adressen) dürfen NICHT in externe KI-Tools eingegeben werden.
- ☐ Vertrauliche Geschäftsdaten (Kalkulationen, Verträge, Finanzdaten) sind für externe KI-Tools tabu.
- ☐ Allgemeine, öffentlich verfügbare Informationen dürfen verwendet werden.

Solutionbox GmbH | www.solutionbox.net | Ihre IT. Unsere Verantwortung.

5. Verantwortung und Kontrolle

- ☐ Jedes KI-generierte Ergebnis muss vor Weitergabe von einem Menschen geprüft werden.
- ☐ Mitarbeiter haften nicht für Fehler, wenn sie sich an diese Richtlinie halten. Bei Verstoß gilt die betriebliche Regelung.
- ☐ Ansprechperson für KI-Fragen: _____

6. Transparenz

- ☐ Gegenüber Kunden und Partnern wird offengelegt, wenn KI wesentlich an einem Arbeitsergebnis beteiligt war.
- ☐ KI-generierte Inhalte werden nicht als eigene Leistung ausgegeben, ohne Prüfung und Anpassung.

Aktualisierung

…se Richtlinie wird mindestens halbjährlich überprüft und bei Bedarf angepasst.

…, Unterschrift Geschäftsführung:

…ox GmbH | www.solutionbox.net | Ihre IT. Unsere Verantwortung.

17.03.2026

WKS Unternehmensberatung · Buchhaltung · IT

KI-Freigabeliste

KI-Tool Freigabeliste

Welche Tools dürfen genutzt werden, welche nicht?

Unternehmen:
Stand:

Diese Liste regelt verbindlich, welche KI-Tools im Unternehmen eingesetzt werden dürfen. Tools, die nicht auf dieser Liste stehen, gelten als NICHT freigegeben und dürfen nicht genutzt werden.

Freigegebene und gesperrte Tools

KI-Tool / Anwendung	Status	Firmenkonto?	Anmerkung
ChatGPT Enterprise / Team	ERLAUBT	Ja, Pflicht	Daten werden nicht zum Training genutzt
Microsoft Copilot (M365)	ERLAUBT	Ja, Pflicht	Innerhalb unserer M365-Umgebung
ChatGPT Free (Browser)	VERBOTEN	Nein	Daten können zum Training verwendet werden
Google Gemini Free	VERBOTEN	Nein	Keine Unternehmensdaten eingeben
DeepL Pro	ERLAUBT	Ja, Pflicht	Nur mit Firmenlizenz, keine Kundendaten
DeepL Free	VERBOTEN	Nein	Keine vertraulichen Texte
Grammarly Business	PRÜFEN	Offen	Evaluierung läuft
[ ]			
[ ]			

Legende

ERLAUBT: Tool darf mit Firmenkonto genutzt werden.
VERBOTEN: Tool darf nicht mit Unternehmensdaten genutzt werden.
PRÜFEN: Tool wird aktuell evaluiert. Nutzung nur nach Rücksprache.

Wichtige Regeln

- ☐ Ein Tool, das NICHT auf dieser Liste steht, gilt automatisch als NICHT freigegeben.
- ☐ Vor Nutzung eines neuen Tools: Rücksprache mit der Ansprechperson (siehe Verantwortungsmatrix).
- ☐ Kostenlose Versionen sind grundsätzlich verboten, sofern nicht explizit freigegeben.
- ☐ Private Accounts sind für dienstliche Nutzung tabu.
- ☐

Freigabe durch:

Solutionbox GmbH | www.solutionbox.net | Ihre IT. Unsere Verantwortung.

17.03.2026

WKS Unternehmensberatung · Buchhaltung · IT

Schulung

KI-Basis-Schulung

2 Stunden reichen, um 90 % der Fehler zu vermeiden

Unternehmen:
Schulungsdatum:
Trainer/in:

Schulungsagenda (ca. 120 Minuten)

Zeit	Thema	Inhalte / Lernziel
0:00-0:15	**Was ist KI?**	Kurze Einführung: Was KI kann, was nicht. Alltagsbeispiele: Spamfilter, Sprachassistenten, ChatGPT. Mythen vs. Realität.
0:15-0:35	**KI in unserem Betrieb**	Welche KI-Tools nutzen wir bereits (bewusst und unbewusst)? Vorstellung der Freigabeliste. Erlaubt vs. verboten.
0:35-0:55	**Datenregeln**	Ampel-System erklären: Grün, Gelb, Rot. Praxisbeispiele: Was darf eingegeben werden, was nicht? Live-Demo: So sieht ein typischer Fehler aus.
0:55-1:05	**Pause**	10 Minuten Pause
1:05-1:25	**Rechtliches**	DSGVO-Grundlagen für KI. AI Act: Was uns betrifft. Haftung: Wer trägt die Verantwortung?
1:25-1:40	**IT-Sicherheit**	Phishing 2.0: KI-gestützte Angriffe erkennen. CEO-Fraud und Deepfakes. Shadow AI: Warum nicht freigegebene Tools gefährlich sind.
1:40-1:55	**Praxis-Workshop**	Teilnehmer bewerten 3-4 Szenarien: Darf ich das? Gemeinsame Diskussion der richtigen Reaktion.
1:55-2:00	**Abschluss**	KI-Nutzungsrichtlinie gemeinsam durchgehen. Ansprechperson vorstellen. Fragen klären.

Checkliste Schulungsvorbereitung

- ☐ Freigabeliste ist aktuell und ausgedruckt
- ☐ KI-Nutzungsrichtlinie ist finalisiert
- ☐ Datenklassifizierung (Ampel) ist vorbereitet
- ☐ 3-4 Praxis-Szenarien für den Workshop vorbereitet
- ☐ Beamer / Bildschirm für Live-Demo bereit
- ☐ Teilnehmerliste vorbereitet

Praxis-Szenarien (Vorschläge für den Workshop)

Szenario 1: Ihre Kollegin kopiert eine Kundenliste mit Namen, E-Mail und Bestellhistorie in ChatGPT Free, um personalisierte Anschreiben zu erstellen. Richtig oder falsch?

Antwort: Falsch. Personenbezogene Daten + kostenloses Tool = DSGVO-Verstoß.

Szenario 2: Sie nutzen Microsoft Copilot (Firmenkonto), um aus einer internen Projektbeschreibung eine Zusammenfassung zu erstellen. Richtig oder falsch?

Antwort: Richtig. Freigegebenes Tool + Firmenkonto + interne Daten (gelb) = erlaubt.

Szenario 3: Ein Mitarbeiter bekommt eine E-Mail vom Geschäftsführer mit der Bitte, sofort 15.000 Euro zu überweisen. Die Mail klingt authentisch. Was tun?

Antwort: Telefonisch beim GF rückfragen. Niemals auf Basis einer E-Mail allein überweisen. Könnte KI-generiert sein.

Szenario 4: Sie installieren eine kostenlose KI-App auf dem Firmenhandy, die Besprechungen automatisch zusammenfasst. Erlaubt?

wort: Nein. Tool steht nicht auf der Freigabeliste, zeichnet Gespräche auf = Datenschutzproblem.

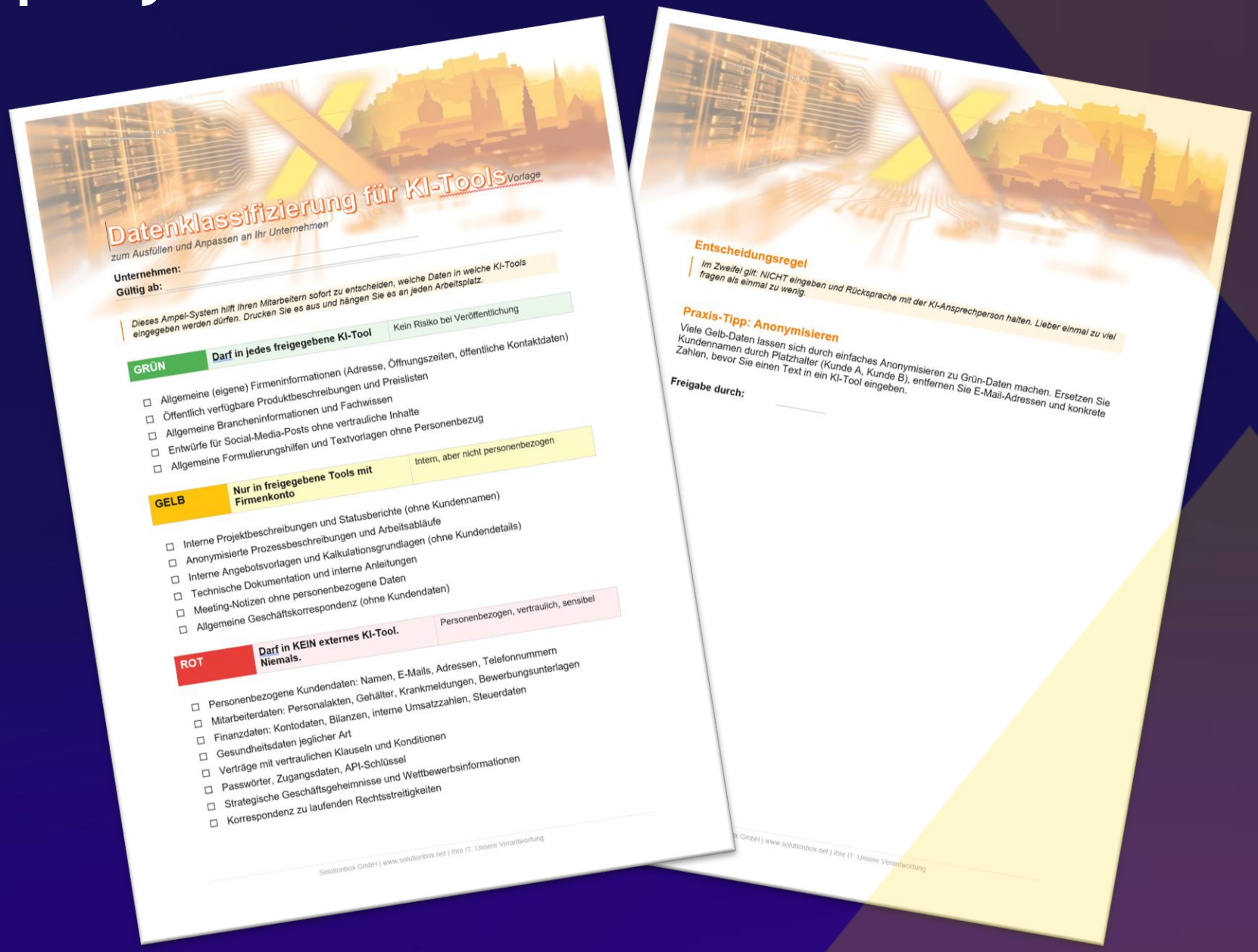
bereitung

eilnehmer haben KI-Nutzungsrichtlinie unterschrieben
hulung im Schulungsprotokoll dokumentiert
hster Schulungstermin festgelegt (Empfehlung: alle 6 Monate Auffrischung)

17.03.2026

WKS Unternehmensberatung · Buchhaltung · IT

Ampelsystem



Datenklassifizierung für KI-Tools Vorlage

zum Ausfüllen und Anpassen an Ihr Unternehmen

Unternehmen:

Gültig ab:

Dieses Ampel-System hilft Ihren Mitarbeitern sofort zu entscheiden, welche Daten in welche KI-Tools eingegeben werden dürfen. Drucken Sie es aus und hängen Sie es an jeden Arbeitsplatz.

GRÜN — **Darf in jedes freigegebene KI-Tool** — Kein Risiko bei Veröffentlichung

- ☐ Allgemeine (eigene) Firmeninformationen (Adresse, Öffnungszeiten, öffentliche Kontaktdaten)
- ☐ Öffentlich verfügbare Produktbeschreibungen und Preislisten
- ☐ Allgemeine Brancheninformationen und Fachwissen
- ☐ Entwürfe für Social-Media-Posts ohne vertrauliche Inhalte
- ☐ Allgemeine Formulierungshilfen und Textvorlagen ohne Personenbezug

GELB — **Nur in freigegebene Tools mit Firmenkonto** — Intern, aber nicht personenbezogen

- ☐ Interne Projektbeschreibungen und Statusberichte (ohne Kundennamen)
- ☐ Anonymisierte Prozessbeschreibungen und Arbeitsabläufe
- ☐ Interne Angebotsvorlagen und Kalkulationsgrundlagen (ohne Kundendetails)
- ☐ Technische Dokumentation und interne Anleitungen
- ☐ Meeting-Notizen ohne personenbezogene Daten
- ☐ Allgemeine Geschäftskorrespondenz (ohne Kundendaten)

ROT — **Darf in KEIN externes KI-Tool. Niemals.** — Personenbezogen, vertraulich, sensibel

- ☐ Personenbezogene Kundendaten: Namen, E-Mails, Adressen, Telefonnummern
- ☐ Mitarbeiterdaten: Personalakten, Gehälter, Krankmeldungen, Bewerbungsunterlagen
- ☐ Finanzdaten: Kontodaten, Bilanzen, interne Umsatzzahlen, Steuerdaten
- ☐ Gesundheitsdaten jeglicher Art
- ☐ Verträge mit vertraulichen Klauseln und Konditionen
- ☐ Passwörter, Zugangsdaten, API-Schlüssel
- ☐ Strategische Geschäftsgeheimnisse und Wettbewerbsinformationen
- ☐ Korrespondenz zu laufenden Rechtsstreitigkeiten

Entscheidungsregel

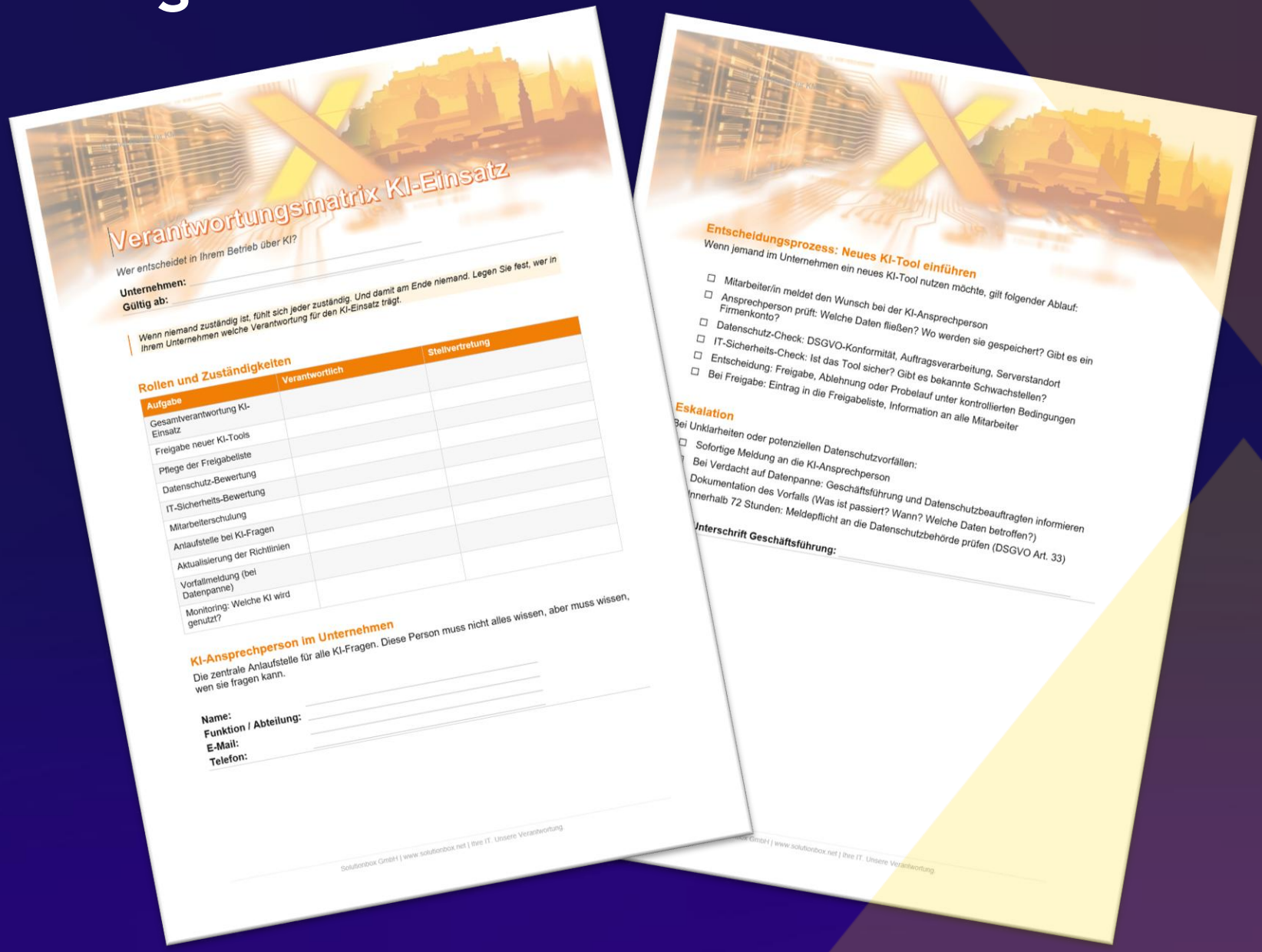
Im Zweifel gilt: NICHT eingeben und Rücksprache mit der KI-Ansprechperson halten. Lieber einmal zu viel fragen als einmal zu wenig.

Praxis-Tipp: Anonymisieren

Viele Gelb-Daten lassen sich durch einfaches Anonymisieren zu Grün-Daten machen. Ersetzen Sie Kundennamen durch Platzhalter (Kunde A, Kunde B), entfernen Sie E-Mail-Adressen und konkrete Zahlen, bevor Sie einen Text in ein KI-Tool eingeben.

Freigabe durch:

Zuständigkeiten



Verantwortungsmatrix KI-Einsatz

Wer entscheidet in Ihrem Betrieb über KI?

Unternehmen:
Gültig ab:

Wenn niemand zuständig ist, fühlt sich jeder zuständig. Und damit am Ende niemand. Legen Sie fest, wer in Ihrem Unternehmen welche Verantwortung für den KI-Einsatz trägt.

Rollen und Zuständigkeiten

Aufgabe	Verantwortlich	Stellvertretung
Gesamtverantwortung KI-Einsatz		
Freigabe neuer KI-Tools		
Pflege der Freigabeliste		
Datenschutz-Bewertung		
IT-Sicherheits-Bewertung		
Mitarbeiterschulung		
Anlaufstelle bei KI-Fragen		
Aktualisierung der Richtlinien		
Vorfallmeldung (bei Datenpanne)		
Monitoring: Welche KI wird genutzt?		

KI-Ansprechperson im Unternehmen

Die zentrale Anlaufstelle für alle KI-Fragen. Diese Person muss nicht alles wissen, aber muss wissen, wen sie fragen kann.

Name:
Funktion / Abteilung:
E-Mail:
Telefon:

Entscheidungsprozess: Neues KI-Tool einführen

Wenn jemand im Unternehmen ein neues KI-Tool nutzen möchte, gilt folgender Ablauf:

- ☐ Mitarbeiter/in meldet den Wunsch bei der KI-Ansprechperson
- ☐ Ansprechperson prüft: Welche Daten fließen? Wo werden sie gespeichert? Gibt es ein Firmenkonto?
- ☐ Datenschutz-Check: DSGVO-Konformität, Auftragsverarbeitung, Serverstandort
- ☐ IT-Sicherheits-Check: Ist das Tool sicher? Gibt es bekannte Schwachstellen?
- ☐ Entscheidung: Freigabe, Ablehnung oder Probelauf unter kontrollierten Bedingungen
- ☐ Bei Freigabe: Eintrag in die Freigabeliste, Information an alle Mitarbeiter

Eskalation

Bei Unklarheiten oder potenziellen Datenschutzvorfällen:

- ☐ Sofortige Meldung an die KI-Ansprechperson
- ☐ Bei Verdacht auf Datenpanne: Geschäftsführung und Datenschutzbeauftragten informieren
- ☐ Dokumentation des Vorfalls (Was ist passiert? Wann? Welche Daten betroffen?)
- ☐ Innerhalb 72 Stunden: Meldepflicht an die Datenschutzbehörde prüfen (DSGVO Art. 33)

Unterschrift Geschäftsführung:

Was jedes KMU jetzt starten sollte

Unabhängig von der Risikostufe

1

KI-Inventar erstellen

Welche KI-Tools werden eingesetzt? Auch unbewusst!

2

Risikostufe zuordnen

Für jedes Tool prüfen: Welche der 4 Kategorien?

3

KI-Kompetenz sicherstellen

Art. 4: Mitarbeiterschulung. Gilt seit Feb. 2025!

4

DSGVO parallel beachten

AI Act ersetzt DSGVO nicht. Beide gelten!

5

Lieferanten befragen

In welche AI-Act-Kategorie fällt deren Produkt?

6

Dokumentation starten

Schriftlich festhalten: Welche KI, warum, wie.

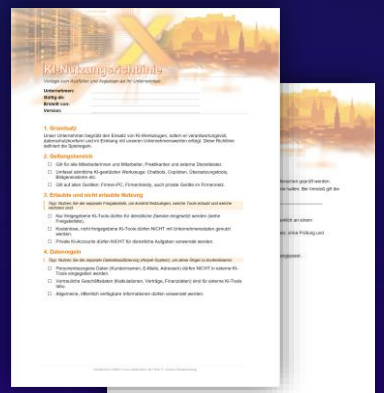
FAZIT

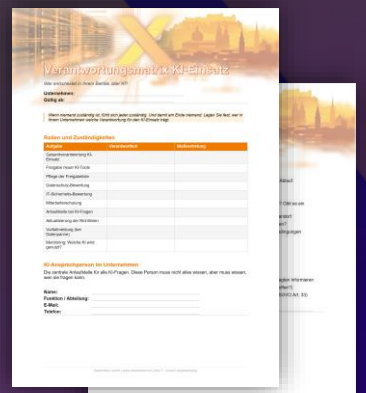
KI, Datenschutz und IT-Sicherheit gehen zusammen. Wenn der Mensch am Steuer bleibt.

17.03.2026

WKS
Unternehmensberatung · Buchhaltung · IT

Gratis Checklisten für Sie:
Kommen Sie auf mich zu!
Oder schreiben Sie mir eine E-Mail:
martin.hoeck@solutionbox.net





17.03.2026

Unternehmensberatung · Buchhaltung · IT

Fragen?

www.eday-salzburg.at/download

Danke

solutionbox Informationstechnologie GmbH
Wir haben die Lösung!

Hinweise
Grafiken wurden teils KI-Unterstützt erstellt
Dieses Dokument dient der Orientierung und stellt keine Rechtsberatung dar.
Stand: März 2026.

17.03.2026

WKS Unternehmensberatung · Buchhaltung · IT