DSGVO & KI in Unternehmen: So nutzt du künstliche Intelligenz rechtssicher und smart

Praxisleitfaden für kleine und mittlere Unternehmen – verständlich, umsetzbar, aktuell (Stand 2025)

Ricarda Kargougou

Varika.NEXT

09.06.2025

DSGVO & Künstliche Intelligenz

Der kompakte Leitfaden für Unternehmen – Sicher, verständlich & praxisnah

Auflage 1/2025

Einleitung

Willkommen in der Zukunft der Arbeitswelt: Künstliche Intelligenz (KI) ist dabei, unsere Unternehmen, Prozesse und Kommunikationswege grundlegend zu verändern. Mit Tools wie Microsoft 365 Copilot, ChatGPT oder Azure OpenAI können wir schneller arbeiten, Inhalte automatisiert erstellen und Entscheidungen datenbasiert unterstützen lassen. Klingt fantastisch – wäre da nicht eine kleine, aber wichtige Vorschrift namens **DSGVO**.

Die Datenschutz-Grundverordnung gilt auch für KI. Und das bedeutet: Wer heute KI einsetzt, muss nicht nur innovativ, sondern auch verantwortungsbewusst handeln. Dieser Leitfaden hilft dir genau dabei. Klar, strukturiert, ohne Fachchinesisch – aber mit maximalem Praxisbezug.

Du erfährst hier:

- Welche DSGVO-Anforderungen für KI gelten
- Was Microsoft konkret zum Schutz deiner Daten umsetzt
- Wie du KI sichere Compliance in deinem Unternehmen etablierst
- Welche Tools & Checklisten dir dabei helfen

Ob IT-Admin, Geschäftsführer:in oder Datenschutzbeauftragte:r: Dieser kompakte Leitfaden ist für dich.

Los geht’s mit den Grundlagen.

Inhaltsverzeichnis

Einleitung **1**
Inhaltsverzeichnis 2
Kapitel 1: DSGVO trifft KI **3**
Kapitel 2: Microsofts Datenschutzstrategie im Überblick **4**
Was sie versprechen – und was es für dich bedeutet 4
✅ Die 7 Datenschutzversprechen im Detail: 4
Warum das für Dich wichtig ist? 6
Fazit Kapitel 2 6
Kapitel 3. Nutzungsregeln **6**
🚦 Grundregeln für den Umgang mit KI-Tools 6
🛡️ Technische Schutzmaßnahmen – konkret und notwendig 7
Kapitel 4. Rollen & Verantwortlichkeiten **7**
🔑 Zentrale Rollen und ihre Aufgaben 8
Kapitel 5: Schulung & Awareness **9**
🎯 Zentrale Bausteine einer erfolgreichen Awareness-Strategie: 9
Kapitel 6: Datenschutz-Folgenabschätzung (DSFA) – kurz erklärt und direkt umsetzbar **11**
Verantwortliche & Beteiligte: Wer ist in den Prozess eingebunden? 11
Kapitel 7: Rechtsgrundlagen für den Einsatz von KI nach DSGVO **12**
Diese vier Rechtsgrundlagen brauchst du im Alltag 12
Wie funktioniert die Interessenabwägung? 13
Kapitel 8: Best Practice – So gelingt die Umsetzung im Alltag **14**
Fazit: DSGVO-konforme KI ist machbar **15**
✅ Dein nächster Schritt: Klarheit schaffen! **16**
Quellen **16**

Kapitel 1: DSGVO trifft KI

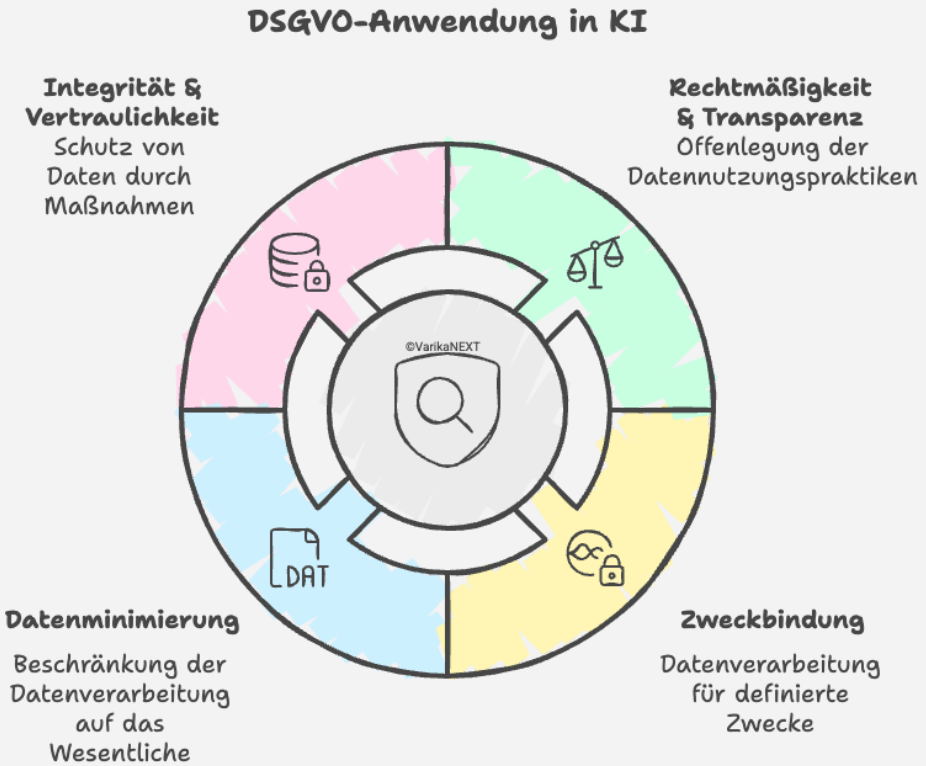
Die Datenschutz-Grundverordnung (DSGVO) wurde nicht für KI geschrieben – aber sie gilt trotzdem. Sobald personenbezogene Daten im Spiel sind, greifen ihre Regelungen, dazu gehören z. B. Namen, E-Mail-Adressen, Standortdaten, IP-Adressen oder auch Chatverläufe.

Und genau das ist bei generativer KI überraschend oft der Fall: Namen in Prompts, Projektinfos in generierten Texten, E-Mail-Daten aus Outlook – all das sind personenbezogene Daten.

Wichtige Grundprinzipien der DSGVO, die du bei KI kennen musst:

- **Rechtmäßigkeit & Transparenz:** Du musst offenlegen, wie und wofür du personenbezogene Daten nutzt.
- **Zweckbindung:** Daten dürfen nur für genau definierte Zwecke verarbeitet werden.
- **Datenminimierung:** Verarbeite nur, was wirklich nötig ist.
- **Integrität & Vertraulichkeit:** Technische & organisatorische Maßnahmen müssen greifen.

KI macht das komplexer, aber nicht unmöglich. Es braucht nur Struktur und Klarheit. Genau da setzt dieser Leitfaden an.



Kapitel 2: Microsofts Datenschutzstrategie im Überblick

Was sie versprechen – und was es für dich bedeutet

Microsoft zählt weltweit zu den führenden Anbietern für Unternehmenslösungen – und das bedeutet auch: maximale Verantwortung beim Thema Datenschutz. Mit dem zunehmenden Einsatz von KI, insbesondere durch Microsoft 365 Copilot und Azure OpenAI Services, stellt sich für viele Unternehmen die Frage: Kann ich diesen Tools vertrauen?

Microsoft antwortet darauf mit einem klaren „Ja“ – und belegt es durch sieben verbindliche Datenschutzversprechen. Diese bilden das Rückgrat ihrer KI-Strategie und richten sich direkt an Unternehmen, die in einem DSGVO-regulierten Umfeld arbeiten.

✅ Die 7 Datenschutzversprechen im Detail:

1. Deine Daten gehören dir

Microsoft erhebt keinen Besitzanspruch auf die Inhalte, die du mit ihren Tools generierst oder speicherst. Du bist und bleibst **Eigentümer deiner Daten** – egal ob E-Mails, Notizen, Präsentationen oder Prompts.
👉 Das bedeutet: Du entscheidest, was du mit deinen Daten machst – Microsoft nutzt sie nicht für eigene Zwecke.

2. Keine verdeckte Speicherung oder Nutzung

Microsoft verarbeitet nur das, was wirklich nötig ist – und ausschließlich im Rahmen deiner Einstellungen. Es erfolgt **keine verdeckte Protokollierung oder Weiterverwertung deiner Eingaben**.
👉 Deine Prompts, Befehle oder Dateien werden **nicht für die Verbesserung der KI** genutzt – es sei denn, du gibst deine ausdrückliche Zustimmung.

3. Keine Weitergabe an Dritte

Microsoft garantiert, dass sie **keine deiner Daten an Drittanbieter verkaufen oder weitergeben**, weder für Werbung noch für Profilbildung oder Analysezwecke.
👉 Das schützt dich vor Datenabfluss, rechtlichen Problemen und Vertrauensverlust bei Kunden.

Hinweis: Diese Zusagen gelten insbesondere für Unternehmenslizenzen (Microsoft 365 E3/E5, Azure AD etc.). Im privaten Umfeld können andere Bedingungen gelten

4. Kein Training der KI mit Kundendaten

Ein zentrales Versprechen: **Deine Inhalte trainieren keine KI-Modelle**. Microsoft trennt klar zwischen den Trainingsdaten ihrer Basismodelle und den Nutzungsdaten der Kunden.
👉 Du nutzt ein KI-System – aber das KI-System lernt **nicht aus Deinem Verhalten**, wenn Du das **nicht aktiv erlaubst.**

5. Verschlüsselung & Zugriffsschutz

Sowohl bei der Übertragung als auch bei der Speicherung verwendet Microsoft **modernste Verschlüsselungsstandards** (z. B. TLS 1.2+, BitLocker). Außerdem gibt es feingranulare **Zugriffskontrollen** für Administratoren und Endnutzer.
👉 So sind Deine Daten auch technisch gegen unbefugten Zugriff geschützt – selbst innerhalb Deines Unternehmens.

6. Privacy by Design & by Default

Datenschutz wird bei Microsoft **nicht nachträglich integriert**, sondern von Beginn an mitgedacht. Funktionen wie **Datenklassifizierung, Rechteverwaltung und Auditlogs** sind standardmäßig integriert.
👉 Du kannst KI nutzen – ohne auf eigene Risikoabschätzungen angewiesen zu sein. Microsoft liefert die Infrastruktur.

7. EU Data Boundary – Datenverarbeitung in Europa

Für Unternehmen in der EU ist besonders wichtig: **Microsoft bietet an, Deine Daten ausschließlich innerhalb der EU zu speichern und zu verarbeiten.**
👉 Damit wird der Umgang mit Drittlandübermittlungen erleichtert – und Du musst Dir weniger Sorgen um den berüchtigten „US-Cloud-Zugriff“ machen.

Warum das für Dich wichtig ist?

Viele Unternehmen verlassen sich auf technische Anbieter – ohne deren Datenschutzkonzepte genau zu prüfen. **Mit Microsoft bekommst Du Transparenz, Kontrolle und Schutz – aber nur, wenn Du aktiv mitspielst.**

Das heißt konkret:

- Aktiviere die richtigen Richtlinien in Microsoft Preview
- Nutze die Verschlüsselungsoptionen
- Vereinbare einen **Auftragsverarbeitungsvertrag (AVV)**
- Integriere die KI-Nutzung in Dein bestehendes Datenschutzkonzept

Fazit Kapitel 2

Microsoft liefert Dir die **Bausteine für einen sicheren KI-Einsatz** – aber das Haus baust Du.
Mit diesen sieben Versprechen und klaren Verantwortlichkeiten schaffst Du eine solide Grundlage für DSGVO-konformes Arbeiten mit Copilot & Co.

Kapitel 3. Nutzungsregeln

Der DSGVO-konforme Einsatz von KI erfordert klare Spielregeln – nicht nur auf dem Papier, sondern auch im Alltag. Diese Nutzungsregeln sollten für alle Mitarbeitenden verbindlich sein und aktiv gelebt werden.

🚦 Grundregeln für den Umgang mit KI-Tools

- Verwende **keine sensiblen Daten** in Prompts (z. B. Gesundheitsdaten, Religionszugehörigkeit, Persönlichkeitsprofile).
- Nutze KI **nur für eindeutig definierte Zwecke** – z. B. Texterstellung, Ideengenerierung oder Datenanalyse.
- **Dokumentiere jede Nutzung** in einem zentralen Nutzungstagebuch oder Log.
  Hole vor der Einführung neuer KI-Anwendungen intern eine Freigabe ein.
- Setze **technische Schutzmaßnahmen** ein und halte sie aktuell.

🛡️ Technische Schutzmaßnahmen – konkret und notwendig

Damit KI-Anwendungen DSGVO-konform bleiben, braucht es mehr als nur Regeln – es braucht Technik. Diese Maßnahmen sind zentral:

- **Ende-zu-Ende-Verschlüsselung**: Alle Daten zwischen Nutzer:in und KI-System sollten durchgängig verschlüsselt sein – mindestens via TLS 1.2. Für gespeicherte Daten empfiehlt sich z. B. BitLocker.
- **Zugriffssteuerung (RBAC)**: Rollenbasierte Berechtigungssysteme stellen sicher, dass nur autorisierte Personen Zugriff auf sensible Daten oder KI-Funktionen haben. Rechte sollten regelmäßig geprüft und angepasst werden.
- **Audit-Logs & Nachvollziehbarkeit**: Jeder KI-Einsatz muss rückverfolgbar sein. Logs ermöglichen im Ernstfall schnelles Handeln, z. B. bei Datenschutzpannen.
- **Systemtrennung & Sandbox-Modus**: Für risikobehaftete Tests sollte eine getrennte Testumgebung genutzt werden, um die Produktivsysteme zu schützen.
- **Datenklassifizierung**: Tools wie Microsoft Purview helfen, Inhalte automatisch nach Vertraulichkeit zu kennzeichnen und mit passenden Schutzmaßnahmen zu verknüpfen.

💡 **Praxistipp:**
Implementiere ein zentrales Dashboard zur Überwachung aller KI-Aktivitäten im Unternehmen – so behältst du auch bei mehreren Abteilungen oder Standorten den Überblick.

Kapitel 4. Rollen & Verantwortlichkeiten

Damit KI im Unternehmen sicher und datenschutzkonform eingesetzt werden kann, braucht es klare Zuständigkeiten. Viele Risiken entstehen nicht durch bösen Willen, sondern durch Unklarheit – wer was darf, wer was tun muss, und wer im Fall der Fälle den Hut aufhat.

Deshalb gilt: **Definiere Verantwortlichkeiten von Anfang an – und dokumentiere sie.**

🔑 Zentrale Rollen und ihre Aufgaben

1. Datenschutzbeauftragte:r

- Prüfung neuer KI-Tools auf DSGVO-Konformität
- Durchführung und Pflege der Datenschutz-Folgenabschätzung (DSFA)
- Regelmäßige Kontrolle und Bewertung der eingesetzten Maßnahmen
- Ansprechperson für alle datenschutzbezogenen Fragen

2. IT-Abteilung

- Technische Implementierung von KI-Systemen
- Einrichtung und Wartung von Schutzmaßnahmen (z. B. Verschlüsselung, Zugriffskontrolle)
- Monitoring und Logging aller KI-Aktivitäten
- Unterstützung bei technischen Fragen oder Störungen

3. Fachabteilungen

- Nutzung der KI-Tools gemäß den festgelegten Richtlinien
- Melden neuer Anwendungsfälle oder Probleme
- Sensibler Umgang mit Daten in Prompts
- Mitarbeit bei der laufenden Evaluation

4. Führungskräfte

- Verantwortung für die Awareness und Regelbefolgung im eigenen Team
- Integration der KI-Nutzungsregeln in bestehende Prozesse
- Ansprechperson bei Eskalationen oder Unklarheiten
- Vorbildfunktion bei der sicheren Anwendung

🧩 Ergänzend empfohlen: Das KI-Lenkungsteam

Ein interdisziplinäres **KI-Lenkungsteam**, bestehend aus Datenschutz, IT und Fachbereichen, kann folgende Aufgaben übernehmen:

- Prüfung und Bewertung neuer KI-Anwendungsfälle
- Freigabe und Risikoabschätzung
- Kontinuierliche Verbesserung von Richtlinien und Prozessen
- Unterstützung bei der Einführung neuer Tools

💡 **Praxistipp:**
Erstelle zu jeder neuen KI-Anwendung eine **„Rollenkarte“**, auf der kurz und prägnant steht, wer wofür zuständig ist. Diese kann Teil der Projektdokumentation oder in ein internes Wiki eingebunden werden. Das erhöht Transparenz, erleichtert Schulung und hilft im Alltag.

Kapitel 5: Schulung & Awareness

Ein entscheidender Erfolgsfaktor für den DSGVO-konformen Einsatz von KI ist das Bewusstsein der Mitarbeitenden. Technik allein schützt nicht – Wissen, Haltung und Handlungskompetenz sind essenziell.

🎯 Zentrale Bausteine einer erfolgreichen Awareness-Strategie:

- **!!Pflichtschulung bei Einführung:** Vor dem ersten Einsatz von KI-Tools ist eine Basisschulung verpflichtend. Inhalte: Datenschutz-Grundlagen, typische Risiken, sichere Prompting-Strategien.
- 🔁**Jährliche Auffrischungsschulung:** Regelmäßige Trainings helfen, Wissen zu festigen, neue regulatorische Entwicklungen zu verstehen und Anwendungssicherheit zu verbessern.
- 👩‍💻**E-Learning-Module & Mikrotrainings:** Kurze Lerneinheiten (5–10 Minuten) zu praxisnahen Themen wie „Was darf ich prompten?“, „Was ist eine DSFA?“, oder „Wie erkenne ich KI-generierte Inhalte?“ fördern nachhaltiges Lernen.
- 🤖**Interaktive Awareness-Formate:** Lunch & Learn, KI-Quizze oder simulierte Datenschutzpannen (z. B. durch falsche Prompteingaben) stärken die Kompetenz auf spielerische Weise.
- 👩‍🏫**Führungskräfte als Multiplikator:innen:** Führungskräfte sollen als Vorbilder agieren, selbst geschult sein und aktiv in die Awareness-Strategie eingebunden werden.
- 👫👫**KI-Supportteam:** Ein internes Team, das Fragen beantwortet, Probleme entgegennimmt und Lerninhalte bereitstellt, erhöht Akzeptanz und reduziert Fehlnutzung.

- 🏆**Interne Champions:** Benenne „KI-Champions“ oder „KI-Scouts“ pro Abteilung, die als erste Anlaufstelle bei Fragen und Unsicherheiten agieren.

Beispielhafte Schulungsstruktur			
Format	**Zielgruppe**	**Frequenz**	**Inhalt**
Basisschulung	Alle Mitarbeitenden	Einmalig	Datenschutz, DSGVO, Prompt-Guidelines
Auffrischung	Alle Mitarbeitenden	jährlich	Updates, neue Tools, Lessons Learned
Führungs-kräftetraining	Lead	jährlich	Rollenvorbild, Risikoverantwortung
Mikrotraining	Projektteams	laufend	Situationsspezifisches Wissen

Praxistipps:

Baue ein internes Wiki oder eine Knowledge Base auf, in dem häufige Fragen zum KI-Einsatz gesammelt und beantwortet werden.

Führe eine anonymisierte Feedbackschleife ein, in der Unsicherheiten beim KI-Einsatz geteilt werden dürfen – ohne Konsequenzen.

Stelle „KI-Nutzungskarten“ als physische Reminder am Arbeitsplatz zur Verfügung, z. B. mit den fünf wichtigsten Prompt-Regeln.

Das Ziel: Mitarbeitende sollen sich sicher fühlen, aber auch verantwortlich handeln. Nur so entsteht ein Klima, in dem Innovation und Datenschutz Hand in Hand gehen.

Kapitel 6: Datenschutz-Folgenabschätzung (DSFA) – kurz erklärt und direkt umsetzbar

Die Datenschutz-Folgenabschätzung (DSFA) ist ein zentrales Werkzeug der DSGVO. Sie ist immer dann erforderlich, wenn durch den Einsatz von KI ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen entstehen kann – etwa bei der Verarbeitung sensibler Daten oder bei automatisierten Entscheidunge**n.**

Wann ist eine DSFA notwendig? Eine DSFA musst du durchführen, wenn:

- personenbezogene oder sensible Daten verarbeitet werden (z. B. Gesundheitsdaten, Verhaltensprofile),
- automatisierte Entscheidungen getroffen werden, die reale Auswirkungen auf Personen haben,
- systematische Beobachtung oder Überwachung stattfindet, oder du neue Technologien nutzt, deren Risiken für Betroffene noch unklar sind.

Was gehört in eine DSFA? Eine DSFA ist eine strukturierte Analyse. Folgende Punkte müssen enthalten sein:

- **Zweck der Verarbeitung:** Wofür wird die KI eingesetzt?
- **Betroffene Gruppen:** z. B. Kunden, Mitarbeitende, externe Partner
- **Datenarten:** Welche Daten sind betroffen? (z. B. personenbezogene Daten, besondere Kategorien)
- **Risikoeinschätzung:** niedrig, mittel oder hoch
- **Schutzmaßnahmen:** z. B. Zugriffskontrollen, Schulungen, technische Barrieren

Verantwortliche & Beteiligte: Wer ist in den Prozess eingebunden?

Praxisbeispiel

Projekt: Einführung von Microsoft Copilot im Vertrieb
Ziel: Unterstützung bei der Texterstellung für Kundenkommunikation
Betroffene Daten: Kundennamen, E-Mail-Adressen, Notizen aus Gesprächen
Risikoeinstufung: mittel
Schutzmaßnahmen:

- Prompteingaben-Richtlinie (Whitelist)
- Rollenbasierte Zugriffssteuerung (RBAC)
- OneNote-Logbuch zur Nachvollziehbarkeit
- Mitarbeiterschulung vor der Einführung Ergebnis: Risiko akzeptabel bei Einhaltung der Maßnahmen Beteiligte: Datenschutz, IT-Sicherheit, Vertriebsleitung

Tipp: Dokumentiere deine DSFA unbedingt vor der produktiven Einführung. Halte sie aktuell und prüfe sie regelmäßig – auch bei späteren Funktionsänderungen.

Kapitel 7: Rechtsgrundlagen für den Einsatz von KI nach DSGVO

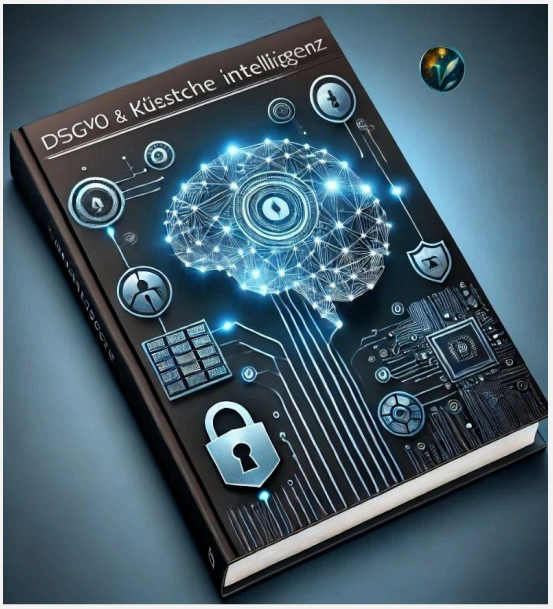
Die DSGVO erlaubt Datenverarbeitung nur, wenn eine rechtliche Grundlage vorliegt. Das gilt auch für KI – jede einzelne Anwendung muss auf **Art. 6 DSGVO** gestützt sein. Es reicht nicht, „KI hilft uns halt“ zu sagen. Es braucht eine klare Begründung.

Diese vier Rechtsgrundlagen brauchst du im Alltag

1. **Einwilligung (Art. 6 Abs. 1 a)**
   Wird verwendet, wenn jemand freiwillig zustimmt – z. B. wenn Mitarbeitende ein KI-Tool auf freiwilliger Basis nutzen oder ein Kunde einer Analyse zustimmt.

2. **Vertragserfüllung (Art. 6 Abs. 1 b)**
   Wenn die Verarbeitung notwendig ist, um einen Vertrag zu erfüllen – z. B. automatische Antwortsysteme im Kundenservice, die Teil der Leistung sind.

3. **Gesetzliche Verpflichtung (Art. 6 Abs. 1 c)**
   Gilt, wenn die Verarbeitung gesetzlich vorgeschrieben ist – z. B. im Rahmen gesetzlicher Aufbewahrungsfristen. Kommt bei KI eher selten vor.



4. **Berechtigtes Interesse (Art. 6 Abs. 1 f)**
   Am häufigsten verwendet. Gilt, wenn das Unternehmen ein nachvollziehbares Interesse hat – z. B. Effizienzsteigerung, interne Prozessoptimierung oder Schutz vor Missbrauch.

Wie funktioniert die Interessenabwägung?

Wenn du dich auf „berechtigtes Interesse“ stützt, musst du zeigen, dass:

- dein Interesse legitim und nachvollziehbar ist,
- die betroffenen Personen nicht unverhältnismäßig beeinträchtigt werden,
- und du Maßnahmen getroffen hast, um Risiken zu verringern.

Praxisbeispiel

Ziel: Copilot soll Texte für Marketingkampagnen vorbereiten

Betroffene Daten: Projektinfos, ggf. einzelne Kundenreferenzen
Risiko: Daten könnten versehentlich in Prompts landen
Schutzmaßnahmen:

- Mitarbeiterschulung
- technische Eingabekontrollen
- keine Nutzung personenbezogener Daten
  Ergebnis der Abwägung: Berechtigtes Interesse ist gegeben, Risiko ist vertretbar

---

Merksatz: Jede KI braucht eine rechtliche Grundlage – ohne DSGVO-Anker kein sicherer Einsatz.

Kapitel 8: Best Practice – So gelingt die Umsetzung im Alltag

Die Theorie ist wichtig – aber entscheidend ist, wie du DSGVO-konforme KI-Nutzung in deinem Unternehmensalltag verankerst. Deshalb zeigen wir dir hier ein bewährtes Umsetzungsbeispiel – von der Idee bis zur gelebten Praxis.

Beispiel: Einführung von Microsoft 365 Copilot in einem mittelständischen Unternehmen

Ausgangslage: Ein Unternehmen mit 120 Mitarbeitenden wollte Microsoft Copilot zur Textgenerierung in Vertrieb und Marketing nutzen. Bisher gab es keine definierte KI-Richtlinie.

So wurde vorgegangen:

1. **Workshop & Awareness-Training:** Alle Mitarbeitenden wurden in einem 90-minütigen Workshop über Chancen, Risiken und Regeln aufgeklärt.
2. **Prompt-Richtlinie definiert:** Eine hausinterne „KI-Nutzungsrichtlinie“ regelt seitdem, welche Informationen in Prompts erlaubt sind (z. B. keine Kundendaten, keine Gesundheitsinfos).
3. **Testphase eingeführt:** Ein Pilotteam testete Copilot 4 Wochen lang, mit Fokus auf datensensible Situationen. Rückmeldungen wurden zentral gesammelt.
4. **Governance eingebunden:** Ein interdisziplinäres „KI-Lenkungsteam“ übernahm die Verantwortung für Pflege, Kontrolle und Nachverfolgung der Nutzung.
5. **Dokumentation & Auditierung:** Alle KI-Einsätze mit Personenbezug werden in einem OneNote-Logbuch dokumentiert.

Ergebnis:

- Keine Datenschutzverstöße
- Hohe Akzeptanz durch Mitarbeitende
- Erhöhte Effizienz bei gleichzeitiger Sicherheit

Praxistipp: Starte nicht mit Tools, sondern mit Menschen. Hole dir frühzeitig das Commitment von Führungskräften und Datenschutz. Und beginne lieber klein und sauber – statt groß und unkontrolliert.

Fazit: DSGVO-konforme KI ist machbar

Ja, KI ist komplex. Und ja, die DSGVO stellt hohe Anforderungen.
Aber: Wer strukturiert vorgeht, kann beides miteinander verbinden. Microsoft zeigt, dass der Datenschutz in der KI-Welt machbar ist – wenn man ihn ernst nimmt.

Mit den richtigen Maßnahmen, etwas Disziplin und einem klaren Fahrplan wird aus KI keine Bedrohung, sondern ein echter Wettbewerbsvorteil.

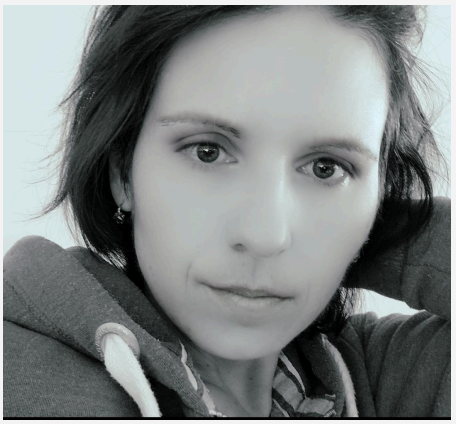
✅ Dein nächster Schritt: Klarheit schaffen!

Du willst KI in Deinem Unternehmen sicher und smart nutzen?
Dann warte nicht, bis die nächste Verordnung kommt – **geh jetzt die ersten Schritte!**

- 🔹 Überprüfe Deine aktuellen Prozesse
- 🔹 Definiere klare Regeln für den KI-Einsatz
- 🔹 Hole Deine Mitarbeitenden ins Boot
- 🔹 Und wenn Du Unterstützung brauchst: **Ich helfe Dir gern.**

📬 **rika@varika-next.com**
🌐 **www.varika-next.com oder mein www.dies-und-das-blog.de für "Dies & Das und irgendwas dazwischen." ;-)**

alternativ QR Code Scannen



Quellen

- kostenfreies Training
- DSGVO - für sehr gelangweilte!:-)
- Leitfaden (extern)
- Leitfaden 2.0 (hältst Du in den Händen ;-))
- Wer nicht lesen mag:
  - DSGVO in 5 Minuten erklärt – mit Christian Solmecke