

KI und Datenschutz im Mittelstand: Risiken erkennen – Verantwortung übernehmen

Bedingungen des Art. 6 Abs. 1		Kern	Beispiel	Risiko	Praxistipp
a)	Einwilligung	Die betroffene Person • hat ihre Einwilligung • zur Verarbeitung • ihrer personenbezogenen Daten gegeben.	Ein Unternehmen nutzt • ein KI-gestütztes Tool • zur Analyse von Bewerbungen, • das automatisiert Persönlichkeitsprofile erstellt. Die Bewerber geben vorab explizit ihre Einwilligung, dass ihre Daten zu diesem Zweck analysiert werden dürfen.	• Einwilligungen müssen - freiwillig, - informiert und - widerrufbar sein. • Viele KI-Systeme arbeiten intransparent; damit ist eine informierte Einwilligung schwer möglich. • Widerruf muss technisch umsetzbar sein.	KI darf nicht „still und heimlich“ personenbezogene Daten verarbeiten . Ohne • klaren Zweck und • Nachweis der Zustimmung riskieren Sie Bußgelder.
b)	Vertragserfüllung	Die Verarbeitung ist zur Erfüllung eines Vertrags erforderlich	Ein Onlinehändler nutzt KI, • um anhand von Bestelldaten • personalisierte Produktempfehlungen zu erstellen. Diese Empfehlungen sind • Bestandteil des Kundenservices, • wie im Kaufvertrag vereinbart.	Nur zulässig, wenn • die KI-Datenverarbeitung • unmittelbar notwendig für die Vertragserfüllung ist Dies könnte dann der Fall sein, wenn Produktempfehlungen explizit Teil des Vertrages sind wie z.B. „Wir wählen die für Sie individuell passenden Produkte anhand Ihres bisherigen Kaufverhaltens aus“	Nicht alles, • was technisch möglich ist, • ist auch datenschutzrechtlich erlaubt. Klare Zweckbindung ist zu beachten.
c)	Rechtliche Verpflichtung	Die Verarbeitung ist zur Erfüllung einer rechtlichen Pflicht notwendig.	Ein Unternehmen setzt KI ein, um • gesetzlich vorgeschriebene • Geldwäscheprüfungen • automatisiert (Erkennen von auffälligen Geldflüssen, Häufigkeit, Zielkonten) durchzuführen.	Nur zulässig, wenn konkrete rechtliche Verpflichtung besteht. KI-Einsatz muss dokumentiert und nachvollziehbar sein.	Nutzen Sie KI nur zur Unterstützung gesetzlicher Pflichten , nicht zur Datenoptimierung.
d)	Lebenswichtige Interessen	Die Verarbeitung ist erforderlich, um lebenswichtige Interessen zu schützen .	In einem Werk nutzt das Unternehmen eine • KI-gestützte Sicherheitsüberwachung, • die Gefahren (z.B. Gaslecks, Unfälle) erkennt und • sofort Alarm auslöst, • um Menschenleben zu schützen.	Nur in Notfall- oder Ausnahmesituationen zulässig.	Kein „Freibrief“ : Diese Rechtsgrundlage greift nur bei echten Notfällen (z.B. Schutz von Leib und Leben) ein.
e)	Öffentliche Aufgabe	Die Verarbeitung erfolgt im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt .	Ein kommunales Versorgungsunternehmen • setzt KI ein, • um Versorgungsnetze zu optimieren und • Krisenmanagementdaten zu analysieren (z.B. zur Sicherstellung der Wasserversorgung)	Nur anwendbar, wenn das Unternehmen eine öffentliche Aufgabe wahrnimmt .	Nur Unternehmen im öffentlichen Auftrag können sich hierauf berufen. Für private Unternehmen ist dies nahezu irrelevant .
f)	Berechtigtes Interesse	Die Verarbeitung ist zur Wahrung berechtigter Interessen erforderlich.	Ein Unternehmen nutzt eine KI, • um interne Prozesse wie Lagerhaltung oder Auslastungsprognosen • anhand von Kundendaten zu optimieren.	Die DSGVO erlaubt die Verarbeitung personenbezogener Daten, wenn drei Voraussetzungen erfüllt sind: 1. Es besteht ein berechtigtes Interesse des Unternehmens 2. Die Verarbeitung ist erforderlich, um dieses Interesse zu verfolgen. 3. Es überwiegen nicht die Interessen oder Grundrechte der betroffenen Person. Transparenz: Betroffene müssen lt. Art. 13 DSGVO erfahren, was, warum und wie ihre Daten verarbeitet werden. Bei KI ist das oft schwer abzubilden.	Dieser Rechtsgrund ist verlockend , aber nicht risikofrei . Führen Sie eine dokumentierte Interessensabwägung durch – im Zweifelsfall mit juristischer Unterstützung.