



KI und Datenschutz

Künstliche Intelligenz (KI) und Datenschutz sind in der EU eng miteinander verbunden. Besonders wichtig ist dabei die Datenschutz-Grundverordnung (DSGVO), weil viele KI-Systeme personenbezogene Daten verarbeiten.

Für Unternehmen – auch kleine Betriebe – entstehen dadurch rechtliche, technische und organisatorische Risiken.

Warum KI datenschutzrechtlich kritisch ist

KI-Systeme arbeiten oft mit großen Datenmengen:

- Kundendaten
- Mitarbeiterdaten
- Chatverläufe
- Bilder, Stimmen oder Videos
- Verhaltensdaten
- Standortdaten

Die DSGVO verlangt dabei:

- klare Rechtsgrundlage
- Transparenz
- Datensparsamkeit
- Zweckbindung
- Sicherheit der Verarbeitung

Viele KI-Anwendungen stehen genau hier unter Beobachtung.



Zentrale DSGVO-Risiken bei KI

1. Verarbeitung personenbezogener Daten ohne Rechtsgrundlage

Eine KI darf personenbezogene Daten nicht „einfach so“ nutzen.

Es braucht z. B.:

- Einwilligung
- Vertragserfüllung
- berechtigtes Interesse

Problematisch:

- Training mit Kundendaten
- automatische Profilbildung
- Nutzung von E-Mails oder Chats für KI-Training

Beispiel:

Ein Unternehmen lädt Kundenlisten in ein öffentliches KI-Tool hoch → möglicher DSGVO-Verstoß.

2. Fehlende Transparenz

Die DSGVO verlangt verständliche Informationen:

- Welche Daten werden verarbeitet?
- Wofür?
- Wie lange?
- Werden Daten an Dritte übertragen?

Viele KI-Systeme sind jedoch „Black Boxes“.

Risiko:

Betroffene verstehen nicht:

- wie Entscheidungen entstehen
- welche Daten genutzt wurden
- ob Profiling stattfindet



3. Datenübertragung in Drittstaaten

Viele KI-Anbieter sitzen in den USA.

Dann stellt sich die Frage:

- Werden Daten außerhalb der EU verarbeitet?
- Gibt es ausreichende Schutzmechanismen?

Relevant sind:

- EU-Standardvertragsklauseln
- EU-US Data Privacy Framework

Besonders kritisch:

- öffentliche KI-Chatbots
- Cloud-KI-Dienste
- Sprachassistenten

4. Automatisierte Entscheidungen und Profiling

Artikel 22 DSGVO regelt automatisierte Entscheidungen.

Beispiele:

- Bewerberauswahl durch KI
- Bonitätsbewertung
- automatische Preisgestaltung
- Leistungsüberwachung von Mitarbeitern

Risiko:

Menschen dürfen nicht ausschließlich automatisierten Entscheidungen mit erheblicher Wirkung unterworfen werden.



5. Sicherheitsrisiken

KI-Systeme können sensible Daten offenlegen:

- Prompt-Leaks
- Datenpannen
- unsichere APIs
- Modellmanipulation
- unkontrollierte Speicherung

Beispiel:

Mitarbeiter geben vertrauliche Vertragsdaten in einen öffentlichen Chatbot ein.

6. Fehlende Löschung und Kontrolle

DSGVO-Rechte:

- Auskunft
- Berichtigung
- Löschung
- Datenübertragbarkeit

Schwierigkeit bei KI:

Einmal trainierte Modelle können Daten indirekt „behalten“.

Das macht Löschung technisch kompliziert.

KI und DSGVO im Unternehmen: typische Problemfelder

KI-Chatbots

Risiken:

- Eingabe sensibler Daten
- Speicherung auf externen Servern
- Nutzung der Daten zum Modelltraining



Maßnahmen:

- keine personenbezogenen Daten eingeben
 - Unternehmensrichtlinien definieren
 - Enterprise-Versionen mit Datenschutzoptionen nutzen
-

Bewerbungs-KI

Risiken:

- Diskriminierung
- unzulässiges Profiling
- fehlende Transparenz

Hier gelten besonders strenge Anforderungen.

Marketing-KI

Risiken:

- Tracking ohne Einwilligung
- automatisierte Kundenprofile
- personalisierte Werbung

Relevant sind zusätzlich:

- ePrivacy-Regeln
 - Cookie-Einwilligungen
-

DSGVO-konformer Einsatz von KI

Wichtige Maßnahmen:

Organisatorisch

- KI-Richtlinie erstellen
- Mitarbeiterschulungen
- Freigabeprozesse definieren



Technisch

- Daten minimieren
- Pseudonymisierung
- Verschlüsselung
- Zugriffskontrollen
- Protokollierung

Rechtlich

- Auftragsverarbeitungsverträge prüfen
- Datenschutzerklärung anpassen
- Datenschutz-Folgenabschätzung durchführen (bei hohem Risiko)

Zusätzlich wichtig: EU AI Act

Neben der DSGVO kommt schrittweise der Artificial Intelligence Act (EU AI Act).

Er regelt:

- Hochrisiko-KI
- Transparenzpflichten
- Dokumentation
- KI-Verbote
- Anforderungen an Anbieter und Nutzer

Besonders betroffen:

- HR-Systeme
- Überwachung
- Biometrie
- kritische Infrastruktur

Die DSGVO bleibt trotzdem weiterhin gültig.



Praktische Empfehlung für Unternehmen

Sicherer Umgang mit KI:

- keine sensiblen Daten in öffentliche KI-Tools eingeben
- interne Richtlinien definieren
- DSGVO-konforme Anbieter auswählen
- Mitarbeiter sensibilisieren
- KI-Einsatz dokumentieren
- Risiken vor Einführung prüfen

Gerade kleine Unternehmen unterschätzen häufig, dass schon einfache KI-Tools datenschutzrechtlich relevant sein können.