COMPLIANCE-BRIEFING

Muss mein Unternehmen wegen AI wirklich nichts tun?

Ein kurzer, ehrlicher Überblick, welche Pflichten bei der AI-Nutzung tatsächlich gelten — und welche nicht. Gedacht als Aufklärung, nicht als Verkaufsargument.

Der EU AI Act verbietet keiner Firma, ChatGPT, Copilot & Co. zu nutzen, und für einfache, alltägliche AI-Nutzung entstehen wenige verpflichtende Produktpflichten. **Aber „gar nichts" stimmt nicht.** Drei Pflichten gelten quer durch alle Firmen — und die DSGVO greift ohnehin, ab dem ersten Datensatz.

Was tatsächlich gilt

PFLICHT	FÜR WEN	WANN	WORUM ES GEHT
DSGVO Datenschutz	Jede Firma mit personenbezogenen Daten	immer	Mitarbeiter, die Kunden- oder Personendaten in ein nicht freigegebenes AI-Tool geben, verarbeiten sie ohne Rechtsgrundlage, ohne AV-Vertrag und ohne Nachweis.
AI Act • Art. 4 AI-Kompetenz	Alle, die AI einsetzen — keine Ausnahme	seit 02.02.2025	Das Personal muss ausreichende AI-Kompetenz haben — Grundverständnis von Chancen und Risiken der genutzten Tools.
AI Act • Art. 5 Verbote	Alle	seit 02.02.2025	Bestimmte Praktiken sind untersagt — z. B. Emotionserkennung am Arbeitsplatz oder Social Scoring.
AI Act • Art. 50 Transparenz	Wer Chatbots betreibt oder AI-Content veröffentlicht	ab 02.08.2026	Chatbots als AI kennzeichnen; AI-generierten oder -bearbeiteten Content sichtbar labeln.
AI Act • High-Risk Annex III	Nur bei einem High-Risk-Use-Case	ab 02.12.2027	Menschliche Aufsicht, Protokollierung, Information der Betroffenen. Greift z. B. bei AI im Recruiting (siehe unten).
Geheimhaltung Berufs- / Vertragsrecht	Mandats- oder vertragsgebundene Firmen	immer	Mandanten- oder Kundendaten in ein AI-Tool zu geben, kann Geheimhaltungs- und Geschäftsgeheimnis-Pflichten verletzen — unabhängig von der DSGVO.

Der AI Act hat Übergangsfristen. Die DSGVO nicht.

Sie gilt für jede Verarbeitung personenbezogener Daten — ab dem Moment, in dem jemand einen Kundennamen, eine E-Mail-Adresse oder einen Vertrag in ein AI-Tool kopiert. Das ist die Pflicht, die jede Firma sofort trifft — unabhängig von Größe, Branche oder AI-Act-Risikostufe.

Nicht der Regulator ist der übliche Auslöser, sondern der erste Kunde oder Auditor, der einen Nachweis verlangt.

High-Risk — für wen wirklich

Breit betroffen

HR & Worker-Management. Recruiting und CV-Screening, aber auch Beförderung, Aufgabenverteilung und Performance-Monitoring von Mitarbeitern.

Branchenspezifisch

Kreditwürdigkeit (wer Bonität prüft oder Kredit gewährt) und Versicherungs-Pricing (Leben / Kranken).

Nicht High-Risk

Support-Chatbots und Lead-Qualifizierung — hier greift nur die Transparenzpflicht (Art. 50), nicht das High-Risk-Regime.

Ab 02.12.2027 — was dann konkret gilt

Der 02.12.2027 macht nicht plötzlich jede Firma high-risk. Aber ab dann sind die Deployer-Pflichten für High-Risk-AI aktiv — und der häufigste Weg, in diese Kategorie zu rutschen, ist AI in der HR: Recruiting, Beförderung, Aufgabenverteilung oder Performance-Monitoring.

Den größten Aufwand (Conformity Assessment) trägt der Anbieter des Tools; wer AI dort einsetzt, wird zum High-Risk-Deployer und muss dann operativ:

- **Menschliche Aufsicht sicherstellen** — eine kompetente Person überwacht das System.
- **Anleitung befolgen** — das System gemäß Anbieter-Vorgaben betreiben, nicht zweckentfremden.
- **Betrieb überwachen** und bei Auffälligkeiten aussetzen.
- **Logs ≥ 6 Monate aufbewahren** — die automatisch erzeugten Protokolle.
- **Betroffene informieren**, wenn AI über sie mitentscheidet.
- **Mitarbeiter & Betriebsrat** vor dem Einsatz am Arbeitsplatz informieren.

Konkret aus Betreiber-Sicht — dieselben Pflichten bilden sich auf drei Ansichten in Qadar AI Shield ab:

Welche AI-Tools laufen bei uns — und mit welchen Daten?

Discovery

AI betriebsweit steuern oder blockieren, den Betrieb überwachen und bei Auffälligkeiten aussetzen.

Policies

Nutzung protokollieren und belegen — Logs mindestens 6 Monate.

Audit Log

Was das praktisch heißt

Für die meisten Firmen ist die Frage nicht „Sind wir reguliert?“, sondern: Wissen wir, welche AI-Tools unser Team nutzt — und mit welchen Daten? Und könnten wir es belegen, wenn jemand fragt? Meist lautet die ehrliche Antwort: nein.

Genau diese Lücke — Realtime-Sichtbarkeit, Policy-Durchsetzung und ein Audit Log über die AI-Nutzung — schließt Qadar AI. Nicht, weil ein Gesetz es erzwingt, sondern weil sich nicht kontrollieren lässt, was man nicht sieht.

Qadar AI Limited • DIFC, Dubai
www.qadar.ai • info@qadar.ai

Dieses Dokument dient der Aufklärung und ist kein Rechtsrat. Regulatorische Angaben mit Stand Juli 2026, EU AI Act in der Fassung nach dem Digital Omnibus (adoptiert; Veröffentlichung im EU-Amtsblatt zum Redaktionsstand ausstehend). Fristen können sich ändern. Für eine verbindliche Bewertung des eigenen Falls juristischen Rat einholen.