Barth Datenschutz

Schritt-für-Schritt-Anleitung zur Risikobewertung von KI-Systemen gemäß AI-Act

Diese Anleitung hilft Unternehmen dabei, KI-Risiken systematisch zu bewerten und zu dokumentieren, um die Anforderungen des AI-Acts zu erfüllen.

von Achim Barth

1. Identifikation des KI-Systems

Fragen zur Einstufung:

- Welche Funktion hat das KI-System?
- Wird das System für kritische Entscheidungen (z. B. Kreditvergabe, Einstellung, Gesundheitsdiagnosen) eingesetzt?
- Welche Daten werden verarbeitet (personenbezogen, sensibel, öffentlich)?
- Wer sind die Nutzer? (Mitarbeiter, Kunden, Behörden etc.)
- In welchen Bereichen/Prozessen wird die KI eingesetzt?

Ergebnis: Kategorisierung des KI-Systems (z. B. allgemeine KI, Hochrisiko-KI, verbotene KI-Anwendung).

2. Risikoklassifizierung nach AI-Act

Einstufung gemäß Risikoklassen:

- Minimales Risiko → KI-Anwendungen mit geringem Einfluss (z. B. KI-gestützte Texterstellung, Chatbots).
- Hohes Risiko → KI in sicherheitskritischen oder entscheidungsrelevanten Bereichen (z. B. Bewerberauswahl, Kreditentscheidungen, Strafverfolgung).
- Verbotene KI → Anwendungen, die gegen Menschenrechte oder ethische Prinzipien verstoßen (z. B. unterschwellige Manipulation, Social Scoring).

Ergebnis: Zuweisung einer Risikokategorie & Entscheidung, ob das System weiter geprüft werden muss.

3. Identifikation potenzieller Risiken

Typische Risiken im KI-Einsatz:

- Diskriminierung/Bias (Bevorzugung oder Benachteiligung bestimmter Gruppen)
- Datenschutzrisiken (Verarbeitung personenbezogener Daten ohne Einwilligung)
- Fehlentscheidungen der KI (z. B. Ablehnung von Krediten ohne menschliche Prüfung)
- Manipulation durch Dritte (Cyberangriffe, KI-Manipulationen)
- Fehlende Erklärbarkeit (Black-Box-Problem)

Ergebnis: Detaillierte Risikoanalyse je nach Anwendungsszenario.

4. Maßnahmen zur Risikominderung

Schutzmaßnahmen implementieren:

- Transparenz erhöhen: Klare Erklärung der KI-Entscheidungen für Nutzer.
- Menschliche Aufsicht: KI-gestützte Entscheidungen regelmäßig überprüfen.
- Bias-Reduktion: Vielfältige & repräsentative Trainingsdaten nutzen.
- Datenschutz & IT-Sicherheit: Anonymisierung & Verschlüsselung sensibler Daten.
- Dokumentation: Nachvollziehbare Aufzeichnungen über Entscheidungen & Updates.

Ergebnis: Definition konkreter Schutzmaßnahmen zur Risikominimierung.

5. Dokumentation & Compliance-Prüfung

Nachweise für die AI-Act-Compliance:

- Gibt es eine schriftliche Dokumentation der Risikobewertung?
- Wurden die Sicherheits- & Datenschutzmaßnahmen nachgewiesen?
- Existiert eine Schulungsstrategie für Mitarbeitende zur sicheren Nutzung?
- Gibt es ein Monitoring & Audit-System für laufende Kontrollen?

Ergebnis: Rechtskonforme Dokumentation der KI-Risiken & ergriffenen Maßnahmen.

6. Regelmäßige Überprüfung & Anpassung

Fortlaufendes Monitoring & Updates:

- Quartalsweise oder jährliche Überprüfung der KI-Risiken
- Anpassung der Schutzmaßnahmen bei Änderungen im System
- Dokumentation neuer Risiken & Maßnahmen

Ergebnis: Dynamische Risikoanpassung zur kontinuierlichen Compliance.

Risikobewertung sichert rechtskonforme KI-Nutzung

✅ Die systematische Risikobewertung hilft, Verstöße & Bußgelder zu vermeiden.

✅ Hochrisiko-KI erfordert besondere Prüfpflichten & Dokumentation.

✅ Unternehmen sollten regelmäßig KI-Risiken evaluieren & anpassen.