Barth Datenschutz

HANDOUT – MODUL 2: Hochrisiko-KI & verbotene KI-Anwendungen

Dieser Handout beleuchtet die wichtigen Aspekte des AI-Act, der zwischen risikoarmen, hochriskanten und verbotenen KI-Systemen unterscheidet. Unternehmen, die KI-Anwendungen entwickeln und einsetzen, müssen wissen, welche Regeln für ihre KI-Systeme gelten und welche Systeme besonders reguliert oder sogar verboten sind.

von **Achim Barth**

Was ist Hochrisiko-KI?

Der AI-Act definiert Hochrisiko-KI als KI-Systeme mit erheblichen Auswirkungen auf Menschen oder gesellschaftliche Prozesse. Diese Systeme unterliegen strengen Prüf- und Dokumentationspflichten und müssen vor der Nutzung zertifiziert und regelmäßig überwacht werden.

Beispiele für Hochrisiko-KI-Anwendungen sind medizinische Diagnosesysteme, Bewerbungsscreening-KI, Kreditbewertungs-KI und Strafverfolgungs-KI. Unternehmen, die diese Systeme nutzen, müssen besonders auf Transparenz, menschliche Kontrolle und Fairness achten.

Pflichten für Unternehmen bei Hochrisiko-KI

Unternehmen, die Hochrisiko-KI einsetzen, müssen eine Reihe von Pflichten erfüllen, um die Risiken zu minimieren und die Rechte und Freiheiten von Menschen zu schützen.

- Risikomanagement: Risiken müssen bewertet und minimiert werden.
- Transparenz & Nachvollziehbarkeit: KI-Entscheidungen müssen nachvollziehbar sein.
- Menschliche Kontrolle: KI darf keine endgültigen Entscheidungen treffen.
- Datenqualität: KI darf nicht mit verzerrten oder diskriminierenden Daten trainiert werden.

Unternehmen, die diese Pflichten nicht einhalten, riskieren hohe Strafen und haften für Schäden durch KI.

Welche KI-Anwendungen sind verboten?

1 Unterschwellige Beeinflussung

KI, die Menschen manipuliert (z. B. versteckte Werbung).

2 Social Scoring

KI, die Menschen anhand ihres Verhaltens bewertet (wie in China).

3 Predictive Policing

KI, die Menschen als zukünftige Täter klassifiziert.

4 Echtzeit-Gesichtserkennung in der Öffentlichkeit

Außer für sehr enge Ausnahmen.

5 Emotionserkennung am Arbeitsplatz & in Schulen

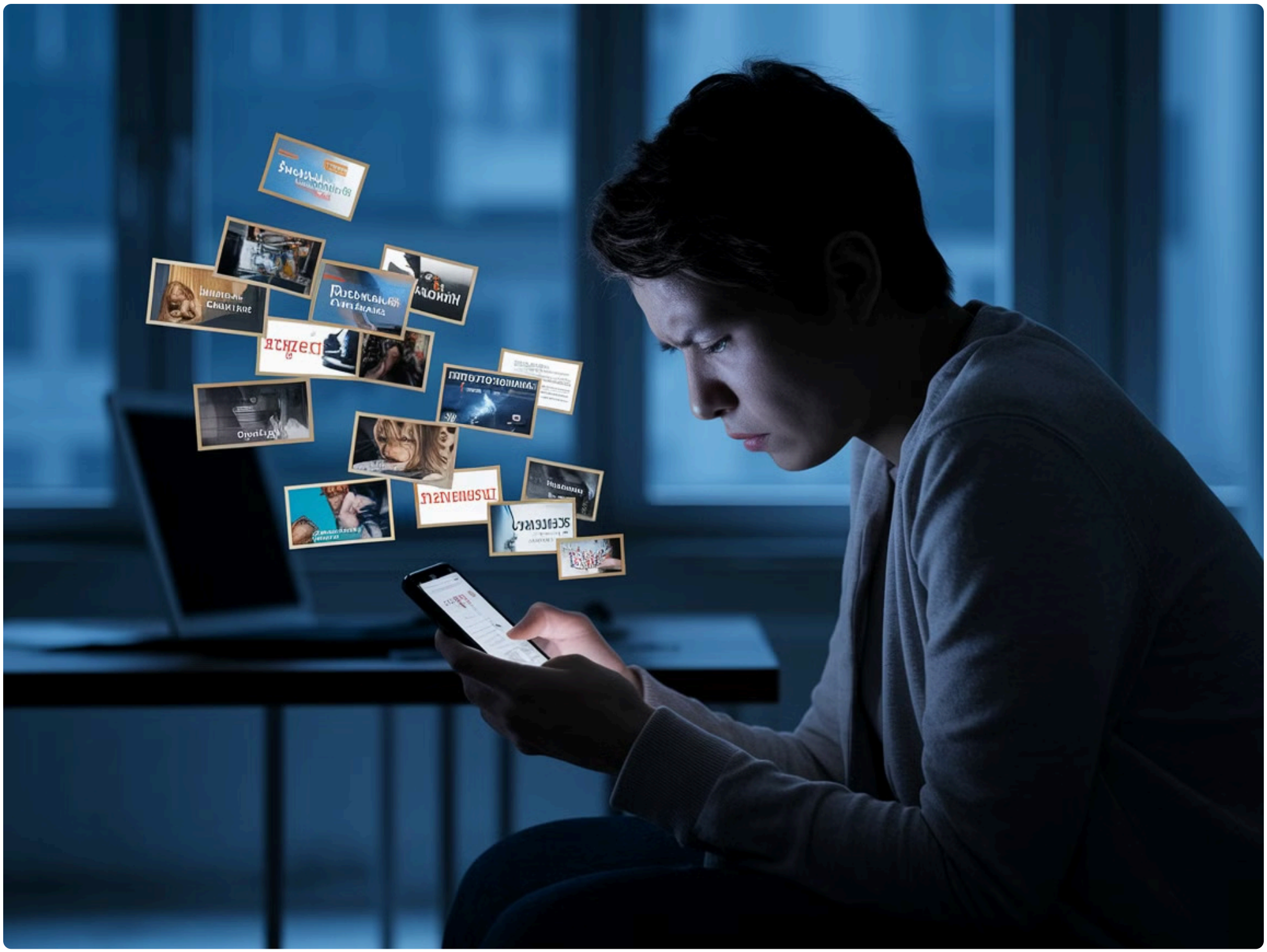
Schutz der Privatsphäre.

Der AI-Act verbietet diese KI-Systeme aufgrund ihres hohen Risikos für Menschen und die Gesellschaft. Unternehmen, die verbotene KI nutzen, müssen mit massiven Bußgeldern und rechtlichen Konsequenzen rechnen.

Praxisbeispiel: Verbotene KI in der Werbung

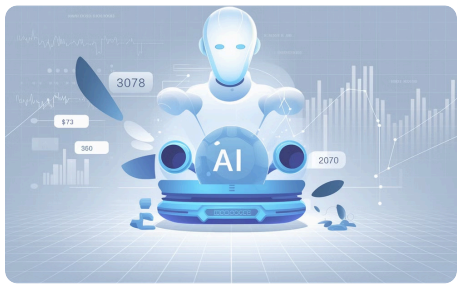
Ein Online-Händler setzte eine KI-gestützte Werbung ein, die Emotionserkennung nutzte. Die KI erkannte traurige oder unsichere Kunden und spielte gezielt Werbeanzeigen für Selbsthilfe-Produkte aus.

Das Ergebnis war eine Strafe durch Verbraucherschutzbehörden wegen unzulässiger Manipulation. Dieses Beispiel verdeutlicht, dass KI nicht gezielt Emotionen ausnutzen darf, um Kaufentscheidungen zu beeinflussen.



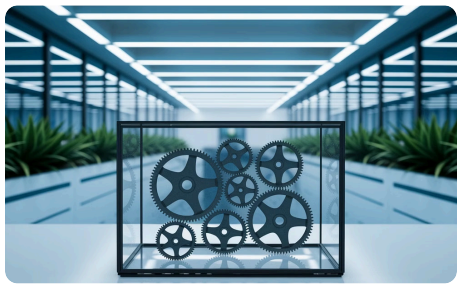
Checkliste: Risikobewertung für KI-Anwendungen

Diese Checkliste hilft Unternehmen, das Risiko einer KI-Anwendung einzuschätzen und geeignete Maßnahmen zu ergreifen.



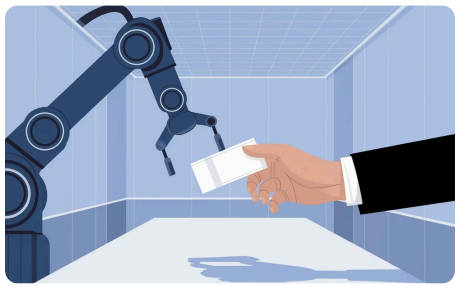
Hochrisiko-KI?

Wird die KI für sensible Bereiche eingesetzt?



Transparenz & Nachvollziehbarkeit

Können Nutzer die KI-Entscheidungen verstehen?



Menschliche Aufsicht

Kann eine Person KI-Entscheidungen korrigieren?

Datenschutz & IT-Sicherheit

Werden Daten DSGVO-konform verarbeitet?

Diese Checkliste hilft Unternehmen, zu prüfen, ob ihre KI-Anwendung rechtssicher und regelkonform ist.

Fazit

Hochrisiko-KI unterliegt strengen Regeln. Unternehmen müssen Transparenz und Fairness sicherstellen. Verbotene KI darf in der EU nicht eingesetzt werden. Verstöße führen zu hohen Strafen.

Die Checkliste zur Risikobewertung hilft Unternehmen, ihre KI-Systeme korrekt einzuordnen. Unternehmen sollten sich mit den Vorgaben des AI-Act vertraut machen und ihre KI-Systeme entsprechend anpassen.