



SOUVERAIGN ACADEMY

**TIPPS FÜR DEN VERANTWORTUNGSVOLLEN
EINSATZ VON KI IM UNTERNEHMEN**



1. Nur geprüfte und freigegebene KI-Tools verwenden

Nicht jedes frei verfügbare KI-Tool entspricht den Sicherheits- und Datenschutzstandards oder den Anforderungen des AI Acts. Nutzen Sie ausschließlich Lösungen, die offiziell vom Unternehmen (z.B. IT, Rechtsabteilung, KI-Governance) geprüft und freigegeben wurden.

2. Kein Account-Sharing – Persönliche Zugänge nutzen

Die Nutzung von KI-Tools muss nachvollziehbar sein. Teilen Sie Ihre Zugangsdaten nicht. Persönliche Accounts helfen, Verantwortlichkeiten zuzuordnen und die Nutzung im Rahmen von Lizenzen und Richtlinien sicherzustellen.

3. Sensible Daten rigoros schützen

Geben Sie **niemals** personenbezogene Daten, vertrauliche Unternehmensinformationen oder Geschäftsgeheimnisse in öffentliche oder nicht explizit dafür freigegebene KI-Systeme ein. Achten Sie auf spezifische Freigaben für interne ("souveräne") oder gesicherte Umgebungen. Im Zweifel gilt: Keine sensiblen Daten eingeben.

4. KI-Ergebnisse kritisch prüfen und hinterfragen

KI-Systeme können Fehler machen oder ungenaue Informationen liefern ("halluzinieren"). Verlassen Sie sich nie blind auf die Ergebnisse. Überprüfen Sie Fakten, Plausibilität und Logik. KI ist ein Werkzeug, keine alleinige Wahrheitsquelle.

5. Transparenz bei KI-generierten Inhalten schaffen

Machen Sie kenntlich, wenn Inhalte (Texte, Bilder etc.) maßgeblich durch KI erstellt wurden, besonders bei externer Kommunikation oder wichtigen internen Dokumenten. Befolgen Sie interne Kennzeichnungsrichtlinien.

6. Gesprächspartner über KI-Interaktion informieren

Wenn Sie KI-Systeme (z.B. Chatbots) im direkten Kontakt einsetzen, stellen Sie sicher, dass Ihr Gegenüber weiß, dass es mit einer KI interagiert, sofern dies nicht offensichtlich ist. Der AI Act fordert dies für bestimmte Systeme.

7. Menschliche Kontrolle und Entscheidung sicherstellen

Besonders bei Entscheidungen mit signifikanten Auswirkungen (z.B. HR, Kundenbewertung) darf KI nur unterstützen. Eine finale Überprüfung und



Entscheidung durch einen Menschen ist oft nicht nur sinnvoll, sondern für Hochrisiko-Systeme gemäß AI Act zwingend erforderlich.

8. Risikoklassen von KI-Systemen beachten

Der AI Act teilt KI in Risikoklassen ein. Informieren Sie sich, ob genutzte Tools besonderen Regeln unterliegen (insbesondere Hochrisiko-Systeme), da für diese strengere Anforderungen gelten.

9. Diskriminierung und unethischen Einsatz vermeiden

Achten Sie darauf, dass KI nicht diskriminierend wirkt. Setzen Sie KI nicht zur Manipulation, Täuschung oder Ausnutzung von Schwachstellen ein. Dies ist ethisch inakzeptabel und oft gemäß AI Act verboten.

10. Bedenken und Vorfälle aktiv melden

Melden Sie unerwartete Ergebnisse, Fehlfunktionen, Sicherheitslücken, ethische Bedenken oder vermutete Richtlinienverstöße im Zusammenhang mit KI unverzüglich den zuständigen Stellen (Vorgesetzte, IT, Compliance etc.).

11. Interne KI-Richtlinien und Schulungen befolgen

Machen Sie sich mit den spezifischen KI-Leitlinien Ihres Unternehmens vertraut und halten Sie diese ein. Nutzen Sie angebotene Schulungen zum Thema KI und AI Act.

12. Kontinuierlich lernen und informiert bleiben

Die KI-Technologie und die Regulierung entwickeln sich schnell. Bleiben Sie neugierig, bilden Sie sich weiter und tauschen Sie sich über Best Practices im Umgang mit KI aus.