Checkliste: Private KI-Accounts im Unternehmen absichern

38 Prüfpunkte für IT-Leiter, DSBs und Geschäftsführung | Dezember 2025

Diese Checkliste hilft Ihnen, die Risiken durch private KI-Accounts wie ChatGPT, Jasper oder Midjourney systematisch zu erfassen und zu minimieren. Prüfen Sie alle Punkte und dokumentieren Sie Ihre Maßnahmen für Audits und Behördenanfragen.

1. Bestandsaufnahme: KI-Nutzung erfassen

- ☐ Inventur aller im Unternehmen genutzten KI-Tools durchführen
- ☐ Private Accounts von Mitarbeitenden identifizieren (ChatGPT, Jasper, Midjourney etc.)
- ☐ Abteilungen befragen, welche KI-Anwendungen parallel zur IT genutzt werden
- ☐ Datenflussanalyse: Welche Daten werden in externe KI-Tools eingegeben?
- ☐ Shadow-IT-Risiken durch KI dokumentieren

2. KI-Governance etablieren

- ☐ Interdisziplinäres KI-Komitee aus IT, Recht und Datenschutz einrichten
- ☐ KI-Verantwortlichkeiten auf Führungsebene verankern
- ☐ Eskalationswege für kritische KI-Vorfälle definieren
- ☐ Notfallpläne für Sicherheitsvorfälle mit KI-Bezug erstellen
- ☐ Regelmäßige KI-Governance-Meetings etablieren

3. Verbindliche KI-Richtlinie erstellen

- ☐ Erlaubte und verbotene KI-Tools klar definieren
- ☐ Anwendungsfälle für genehmigten KI-Einsatz beschreiben
- ☐ Freigabeprozesse für neue KI-Anwendungen festlegen
- ☐ Arbeitsrechtliche Konsequenzen bei Verstößen regeln
- ☐ KI-Richtlinie als Teil der Compliance-Strategie verankern

4. Technische Schutzmaßnahmen implementieren

- ☐ Firewalls zur Blockierung unkontrollierter externer Verbindungen konfigurieren
- ☐ Data Loss Prevention (DLP) Systeme für KI-Datenverkehr einrichten
- ☐ Cloud Access Security Broker (CASB) zur Echtzeitfilterung implementieren
- ☐ Log-Dateien für alle KI-Zugriffe aktivieren und überwachen
- ☐ Anomalie-Erkennung für verdächtige KI-Aktivitäten einsetzen

5. Rechtliche Compliance sicherstellen

- ☐ Auftragsverarbeitungsverträge (AVV) für genehmigte KI-Tools prüfen/abschließen
- ☐ Rechtsgrundlagen nach Art. 6 DSGVO für KI-Verarbeitungen dokumentieren
- ☐ Verzeichnis von Verarbeitungstätigkeiten (VVT) um KI-Tools erweitern
- ☐ Datenschutz-Folgenabschätzung für Hochrisiko-KI durchführen
- ☐ KI-Verordnung: Anforderungen ab 2026 prüfen und vorbereiten

6. Mitarbeitersensibilisierung durchführen

- ☐ Security Awareness Schulungen zu KI-Risiken durchführen
- ☐ Konkrete Beispiele für problematische KI-Nutzung kommunizieren
- ☐ Phishing-Simulationen mit KI-Bezug durchführen
- ☐ Regelmäßige Updates zu neuen KI-Bedrohungen bereitstellen

7. Monitoring und Kontrolle einrichten

- ☐ Kontinuierliche Überwachung der KI-Nutzung implementieren
- ☐ KI-Audit-Prozess für neue Anwendungen vor Freigabe etablieren
- ☐ Regelmäßige Penetrationstests mit KI-Fokus durchführen
- ☐ Schwachstellenanalysen für KI-spezifische Angriffsvektoren

8. Dokumentation und Nachweisführung

- ☐ Alle KI-bezogenen Maßnahmen dokumentieren
- ☐ Technische und organisatorische Maßnahmen (TOMs) für KI aktualisieren
- ☐ Audit-Trails für KI-Nutzung sicherstellen
- ☐ Betroffenenanfragen zu KI-Verarbeitungen vorbereiten