ChatGPT sicher nutzen - Checkliste für KMU

Der kompakte Prüf-Leitfaden für den DSGVO- und AI-Act-konformen Einsatz von ChatGPT im Unternehmen

Diese Checkliste bündelt die zentralen Maßnahmen für den sicheren ChatGPT-Einsatz – vom richtigen Vertragsmodell über die organisatorische Governance bis zum abgesicherten Betrieb von Codex. Zum Abhaken und vorzeigbar bei einer Prüfung.

10 zentrale Prüfpunkte für den sicheren Einsatz von ChatGPT + Codex im Unternehmen

#	Prüfpunkt	Erledigt
1	**Nur Business-/Enterprise-Verträge** oder API für dienstliche Nutzung – keine privaten Plus-Konten	☐
2	**AVV/DPA** mit OpenAI abgeschlossen	☐
3	**Zero Data Retention** (API) bzw. konfigurierte Aufbewahrung bei hohem Schutzbedarf aktiviert	☐
4	**Training-Opt-out** auf verbliebenen Consumer-Konten geprüft und dokumentiert (inkl. Feedback-Regel)	☐
5	**KI-Richtlinie** verabschiedet und kommuniziert	☐
6	**KI-Inventar** erstellt – Shadow-AI-Konten, Custom GPTs und Connectors identifiziert	☐
7	**Art.-4-Schulung** durchgeführt und dokumentiert	☐
8	**Codex nur mit aktiver Sandbox** im Container/VM mit Secret-Sperren und Egress-Kontrolle betrieben	☐
9	**(Nur Codex) Full-Access-Modus gesperrt:** --yolo / danger-full-access außerhalb der Sandbox unterbunden	☐
10	**Audit-Logging** und regelmäßige Reviews etabliert	☐

Die Übersicht aller Prüfpunkte im Detail findet sich unter: **elsengrc.com/journal/chatgpt-sicher-nutzen/**

Wichtige Regeln für die Praxis

- Sobald personenbezogene oder vertrauliche Daten ins Spiel kommen, gehört der Einsatz auf einen **Commercial-Vertrag** (Enterprise oder API) - idealerweise mit **AVV**
- Bei hohem Schutzbedarf mit **Zero Data Retention** Regelung
- Private Pro-Konten haben im Unternehmen nichts zu suchen.

So unterstützt Elsen GRC bei dem Einsatz von KI-Werkzeugen

✓ **KI-Kompetenzschulung nach Art. 4:** Erfüllt die gesetzliche Schulungspflicht, inkl. Zertifikat für Mitarbeiter, Schulungsregister und KI-Richtlinien-Entwurf (KI Leitplanken).

✓ **AI Act Readiness Scan:** KI-Inventar, Risikoklassifizierung und Fahrplan bis August 2026. Allgemeine AI Act Beratung über den konformen Einsatz von KI-Tools im Unternehmen.

✓ **KI-Governance-Beratung:** Vollständiges Framework mit Policies, Rollen und Freigabeprozessen.

→ Buchen Sie jetzt Ihr unverbindliches Erstgespräch unter www.elsengrc.com/contact