Claude sicher nutzen - Checkliste für KMU

Der kompakte Prüf-Leitfaden für den sicheren Einsatz von Claude im Unternehmen

Diese Checkliste bündelt die zentralen Maßnahmen für den sicheren Einsatz der KI-Werkzeuge von Claude: vom richtigen Vertragsmodell über die organisatorische Governance bis zum abgesicherten Betrieb von Claude Code. Die zentralen Prüfpunkte geben eine erste Orientierung für relevante Aspekte, die für den sicheren Einsatz von KI-Tools wie Claude, Claude Cowork oder Claude Code berücksichtigt werden müssen.

10 zentrale Prüfpunkte für den sicheren Einsatz von Claude KI im Unternehmen

#	Prüfpunkt	Erledigt
1	**Nur Commercial-Verträge** (Enterprise/API) für dienstliche Nutzung: Es ist sichergestellt, dass keine privaten Pro-Konten durch Mitarbeiter eingesetzt werden.	☐
2	**Auftragsverarbeitungsvertrag** (AVV) / **Data Processing Agreement** (DPA) mit Anthropic abgeschlossen	☐
3	**Zero Data Retention** bei hohem Schutzbedarf aktiviert	☐
4	**Training-Opt-out** auf verbliebenen Consumer-Konten geprüft und dokumentiert	☐
5	**KI-Richtlinie inkl. Leitplanken** im Unternehmen verabschiedet und kommuniziert	☐
6	**KI-Inventar** erstellt, Shadow-AI-Konten identifiziert und gesperrt / ausgeschlossen	☐
7	**Art.-4-Schulung** durchgeführt und dokumentiert (ggf. mit Mitarbeiter-Zertifizierung)	☐
8	**Claude Code nur im Container/VM** mit Secret-Sperren und Egress-Allowlist betrieben	☐
9	Nur bei Claude Code: **Bypass-Modus gesperrt:** autonomer Modus ohne Sicherheitsabfragen außerhalb der Sandbox unterbunden	☐
10	**Audit-Logging & Reviews etabliert:** Nutzer-, Zugriffs- und (bei Claude Code) Tool-Aktivitäten werden protokolliert und regelmäßig überprüft.	☐

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