revDSG & KI: Das Schatten-KI-Playbook für Schweizer KMU

Wo unkontrollierte KI-Nutzung mit dem Datenschutzgesetz kollidiert — inklusive persönlicher Haftung — und das Governance-Framework, das es behebt.

Die Ein-Absatz-Version: Ihre Mitarbeitenden nutzen bereits KI-Tools — bewilligt oder nicht. Jedes Einfügen von Kundendaten in ein privates ChatGPT- oder Claude-Konto ist Datenbearbeitung ausserhalb Ihrer Verträge, Verzeichnisse und Kontrollen. Unter dem revidierten Datenschutzgesetz (revDSG) verletzt das gleich mehrere Artikel — und anders als bei der DSGVO können Bussen bis **CHF 250'000 direkt gegen verantwortliche Personen** verhängt werden (Quelle: EDÖB-Bericht 2024). Die Lösung ist kein KI-Verbot — sondern bewilligte KI, die einfacher und sicherer ist als die Schatten-Variante.

Wo Schatten-KI das revDSG verletzt

revDSG-Bestimmung	Wie Schatten-KI sie verletzt
Art. 7 — Privacy by Design/Default	Beliebige Datenflüsse an ungeprüfte Plattformen widersprechen dem Prinzip direkt
Art. 9 — Auftragsbearbeitung	Private KI-Konten haben keinen Bearbeitungsvertrag mit Ihrer Firma
Art. 16 — Auslandtransfers	Transfers in Länder ohne Angemessenheit brauchen Garantien — Schattennutzung umgeht sie
Art. 12 — Bearbeitungsverzeichnis	Bearbeitung, von der Ihr Verzeichnis nichts weiss = sofortiger Audit-Befund
Art. 22 — Folgenabschätzung	Risikoreiche Bearbeitung braucht eine DSFA — unmöglich für unbekannte Tools

Die persönliche Dimension: revDSG-Bussen treffen verantwortliche Personen — Geschäftsleitung, IT-Leitung, Compliance — bis CHF 250'000. Für FINMA-regulierte Firmen kollidiert Schatten-KI zusätzlich mit Outsourcing- und Betriebsrisiko-Anforderungen (Rundschreiben 2018/3).

Die fünf Zero-Trust-Prinzipien für KI

- ☐ **Kein impliziertes Vertrauen** — technische Kontrollen statt guter Vorsätze: unbewilligte Plattformen blockieren, Authentifizierung verlangen, KI-Interaktionen loggen
- ☐ **Kontinuierlich verifizieren** — laufend prüfen, welche Tools welche Daten berühren, statt einmaliger Freigabe
- ☐ **Zugriff explizit begrenzen** — Least Privilege für Tools und für die Daten, die jedes Tool erreichen kann
- ☐ **Jeden KI-Agenten als Identität führen** — inventarisiert, mit Owner, gesteuert wie ein menschliches Konto

- ☐ **Policy-bewusster Datenzugriff** — Zugriffsprüfung vor dem Abruf; sensible Daten getaggt und segmentiert

Der Umsetzungspfad: 60–90 Tage

1. **Discovery (Woche 1–2):** Sichtbarkeit auf Netzwerkebene über genutzte KI-Plattformen; anonyme Mitarbeiterumfrage (Ehrlichkeit schlägt Schuldzuweisung); Inventar bewilligter Tools; klassifizieren, welche Daten das Haus nie verlassen dürfen.
2. **Policy (Woche 3–4):** eine kurze, schriftliche KI-Nutzungsrichtlinie — bewilligte Tools, verbotene Datenkategorien, Eskalationsweg. Eine Seite schlägt zwanzig.
3. **Bewilligte Alternative (Woche 4–8):** Teams ein konformes KI-Setup geben, das wirklich besser ist als die Schatten-Tools — kommerzielle API-Bedingungen (kein Training auf Ihren Daten), Schweizer/EU-Hosting wo Residenz gefordert ist, MCP-Konnektoren mit Lesezugriff statt Copy-Paste.
4. **Kontrollen & Monitoring (Woche 8–12):** Blockierlisten für unbewilligte Plattformen, Logging für bewilligte, quartalsweises Review der Nutzungsmuster.

Ihre KI-Nutzungsrichtlinie — das Gerüst

- Bewilligte Tools und Konten (nur Firmenkonten — nie private Konten für Geschäftsdaten)
- Datenkategorien, die externe KI nie erreichen dürfen (Kundenidentitäten, Gesundheit, Finanzdaten, Zugangsdaten)
- Prüfpflicht: KI-Output wird von einem Menschen geprüft, bevor er das Haus verlässt
- Wer neue Tools bewilligt — und wie schnell (ein langsamer Prozess erzeugt neue Schatten-KI)
- Was bei Verstössen passiert — verhältnismässig und vorab bekannt

---

Dieser Leitfaden ist die kompakte Fassung unseres publizierten Fachartikels — Quellen und Vertiefung: **eflury.com/de/blog/schatten-ki-sicherheit-schweizer-kmu/**. Stand: Juli 2026. Keine Rechtsberatung.

Fragen zur Umsetzung in Ihrem Betrieb?

Kostenloses 30-Minuten-Gespräch: eflury.com/de/kontakt/ · me@eflury.com · +41 79 910 77 87