MC Lago Workshop | 12. März 2026 DrKPI® | Urs E. Gattiker, Ph.D. | drkpi.com

Mehr Infos zum Workshop und den Learnings (Take-Aways) gibt es im **Blog vom Marketing Club Lago** und in den **News von DrKPI**.

Einführung

Diese Checkliste hilft dir, die Nutzung von KI bei deiner Arbeit oder in deinem Unternehmen besser zu strukturieren und die Governance zu verbessern. Dabei spielt natürlich auch für ein KMU Compliance eine wichtige Rolle.

Bitte berücksichtige, dass diese Checkliste im Frühjahr 2026 erstellt und getestet wurde. Die Dinge ändern sich sehr schnell, was z.B. KI und Regulierung betrifft. Deshalb halte dich auf dem Laufenden.

Wir alle nutzen KI — bewusst oder unbewusst

Hast du heute Morgen Siri oder Google Maps genutzt? Sprach-Assistenten eingesetzt oder in der S-Bahn Netflix geschaut? Vielleicht eine Spam-Mail nicht erhalten, weil dein E-Mail-Filter sie blockiert hat? Dann hast du heute bereits KI genutzt.

KI ist in unserem Alltag angekommen. Die Frage für KMU lautet nicht «ob», sondern «wie» KI im Unternehmen genutzt wird:

– **Sanktionierte KI** — Tools die dein Unternehmen offiziell eingeführt hat, mit klaren Regeln und DSGVO-Konformität.

– **Schatten-KI** — Tools die Mitarbeitende privat für die Arbeit nutzen, ohne dass die IT-Abteilung oder Geschäftsleitung es weiss. Beispiele: ChatGPT auf dem Privathandy, Grammarly im Browser, Google Translate für vertrauliche Dokumente.

Das Risiko: Schatten-KI ist ein nicht zu unterschätzendes Risiko. Kundendaten, interne Strategien und Verträge können ungewollt auf US-Servern landen. Dabei kann beispielsweise die DSGVO verletzt werden. Zudem können Copyright, Urheberrecht und Patentanmeldungen gefährdet werden, wenn vertrauliche Informationen zu früh über KI an Dritte gelangen.

Check 1 — KI-Modelle vergleichen + Kosten

Frage: Welches Tool passt zu meiner Aufgabe — und was kostet es wirklich?

Tabelle 1 — Proprietäre KI-Tools

Tool / Anbieter	Ungef. Kosten im Monat	Gratis-Version	DSGVO	Stärken	Läuft auf
ChatGPT (OpenAI)	ab USD 20	Ja, mit Limit	■ CLOUD Act	Texte, Code, Bilder, Agenten	W
Claude (Anthropic)	ab USD 20	Ja, mit Limit	■ CLOUD Act	Lange Texte, Analyse, Code	W
Mistral Le Chat	ab USD 15	Ja, mit Limit	■ bis 2027 *	EU-Hosting, Texte, schnell	W
Perplexity	ab USD 20	Ja, mit Limit	■ US-Server	Recherche, Quellen, aktuell	W
Gemini (Google)	ab USD 20	Ja, mit Limit	■ CLOUD Act	Suche, G-Suite, Bilder	W

Legende — Läuft auf: W = Web (Browser) | D = Desktop (macOS/Windows/Linux) | M = Mobil (iOS/Android)

> **Notiz:** Mistral: neue Rechenzentren in Frankreich geplant, DSGVO-Konformität ab Mitte 2027. Details: drkpi.com/.../tabelle-2-mistral-le-chat

Tabelle 2 — Open-Source-Tools

Tool / Anbieter	Kosten/ Monat	Gratis-Version	DSGVO	Stärken	Läuft auf
Ensu (Ente)	Gratis	Ja, unbegrenzt	✔ 100% lokal	Privat, offline, sicher	D / M
GPT4All (Nomic)	Gratis / Teams USD 40 *	Ja, unbegrenzt	✔ lokal	Docs indexieren, PDF, offline	D
Arena.ai (UC Berkeley)	Gratis	Ja, unbegrenzt	■ US-Server	2 Modelle vergleichen, testen	W
Nextcloud	Gratis **	Ja, unbegrenzt	✔ EU möglich	Daten intern, kollaborativ	D
Teuken-7B (Fraunhofer)	Gratis	Ja, unbegrenzt	✔ EU, lokal	Alle EU-Sprachen, Forschung	D
DeepSeek	Gratis	Ja, mit Limit	✘ China ***	Günstig, technisch, via Ollama	D / W

Legende — Läuft auf: W = Web (Browser) | D = Desktop (macOS/Windows/Linux) | M = Mobil (iOS/Android)

> **Notiz:** GPT4All Teams: USD 40/Nutzer/Monat, mind. 25 Nutzer. Im Register «LocalDocs» Ordner angeben — GPT4All indexiert diese als eigene Datenbasis. Ideal für Verträge, Handbücher, internes Know-how.
>
> Nextcloud: kostenlos selbst hosten. Enterprise-Support ab EUR 71–100/Nutzer/Jahr.
>
> DeepSeek: Daten nach China — US House Committee Report bestätigt Sicherheitsrisiken.

Check 2 — Kosten-Falle: Gratis hat seinen Preis

Frage: Weiss ich was ich bekomme, wenn ich die kostenlose Version nutze?

– **Kostenlose Pläne** nutzen oft schwächere Modelle — nicht immer schwächer als neueste Versionen, aber beim Upgrade kann etwas schiefgehen (Bsp. ChatGPT).

– **Perplexity und andere:** Nach Erreichen des Limits wechselt das System auf ein schwächeres Modell — ohne Wahlmöglichkeit.

– **Claude:** Hat ein Tageslimit. Ist es erreicht, wartet man 5 Stunden. Das Programm zählt ab 05:00 Uhr — auch wenn du erst um 05:30 Uhr startest.

– **ChatGPT:** Nutzer der kostenlosen Version werden nach einer Weile auf ein schwächeres Modell umgestellt. Bei Aufbrauch folgt eine Wartezeit.

– **Chat-Limit:** Nach langen Konversationen erscheint «Kapazität voll — bitte neuen Chat starten». Der gesamte Kontext ist dann weg.

Tipp — Nie wieder Kontext verlieren: Markiere den Text den die KI generiert, kopiere ihn und füge ihn in eine .txt oder .md Datei ein. Noch besser: Fordere die KI am Schluss auf, das komplette Hand-out als .txt Datei zu generieren.

Check 3 — DSGVO + CLOUD Act + FISA 702

Frage: Wo landen meine Daten, wenn ich US-KI-Tools nutze?

– **CLOUD Act (2018):** US-Behörden können jederzeit auf Daten von US-Unternehmen zugreifen — auch wenn die Server in der EU stehen. Selbst «DSGVO-konforme» KI-Tools, deren Daten auf Amazon- oder Microsoft-Servern gehostet werden, schützen nicht vor dem CLOUD Act.

– **FISA 702:** US-Geheimdienste können ohne Gerichtsbeschluss auf Kommunikation von Nicht-US-Bürgern zugreifen. Im aktuellen geopolitischen Kontext kein theoretisches Risiko mehr.

– **DSGVO vs. US-Recht:** Kein US-Anbieter kann gleichzeitig DSGVO und CLOUD Act vollständig erfüllen. Beispiel: Sperrung des E-Mail-Kontos des Chefanklägers des Internationalen Strafgerichtshofs Karim Khan durch Microsoft im Jahr 2025.

Konkrete Lösungen für KMU:

– **Schweizer / EU-Hosting:** Nine.ch, Hetzner, Infomaniak — physisch und rechtlich ausserhalb des CLOUD Act.

– Sensible Daten nie direkt in ChatGPT & Co. eingeben — vorher anonymisieren.

– Lokale KI-Modelle nutzen (→ Bonus 9: Ensu & GPT4All).

Check 4 — Datenschutz-Einstellungen

Frage: Was muss ich in meinen KI-Tools deaktivieren?

– **ChatGPT:** Einstellungen → Datenkontrolle → «Modelltraining» ausschalten. So werden deine Eingaben nicht für das Training neuer Modelle verwendet.

– **Mistral Free:** Kein Online-Opt-Out möglich — Papierbrief nötig (CNIL-Beschwerde 2025). Nur Pro/Business hat Online-Opt-Out.

– **Grundregel:** Keine sensiblen Daten eingeben — auch mit deaktivierten Einstellungen bleibt das CLOUD-Act-Risiko bestehen (siehe Check 3).

Warum wichtig: Wer das Modelltraining nicht deaktiviert, gibt Kundendaten und Geschäftsgeheimnisse freiwillig an KI-Anbieter weiter.

Referenz: ChatGPT & Mistral Le Chat: Kritische KI Risiken 2026

Check 5 — Vendor Lock-in vermeiden

Frage: Bin ich von einem einzigen KI-Anbieter abhängig?

Verschiedene KI für verschiedene Aufgaben nutzen:

– **Code & Agenten** → Claude

– **Texte & EU-Daten** → Mistral Le Chat

– **Recherche & Quellen** → Perplexity

– **Vergleich & Testen** → Arena.ai — 2 Modelle parallel, Open Source

Arena.ai Workflow: 2 Modelle bearbeiten dieselbe Aufgabe gleichzeitig. Man wählt die bessere Lösung — oder kombiniert Elemente aus beiden. Wer alles auf einen Anbieter aufbaut, zahlt beim Wechsel mit Zeit und Geld.

– Daten jederzeit exportierbar? Eigene Prompts und Outputs lokal speichern.

– Kein proprietäres Format für Wissensdatenbanken nutzen.

Check 6 — KI-Outputs prüfen mit Ai2 (Open Source)

Frage: Wie erkenne ich ob eine KI-Aussage stimmt?

– **Problem:** KI halluziniert — erfindet Fakten, Quellen, Zahlen.

– **Lösung: SciFact** (Allen Institute for AI — Ai2, Open Source): Behauptung eingeben → SciFact durchsucht tausende Studien. Ergebnis: unterstützend oder widerlegend — mit farbig markierten Textstellen. Basiert auf 1.409 wissenschaftlichen Claims + 5.183 Abstracts.

– **Asta (Ai2, Open Source):** 200 Millionen wissenschaftliche Publikationen (Semantic Scholar). Für Literaturrecherche, Hypothesen, Paper-Suche.

– **Grundregel:** Statt KI für das Fakten-Prüfen wissenschaftlicher Artikel zu nutzen, ist es besser, dies selbst zu tun.

Referenz: Hao, K. (2020-05-29). AI could help scientists fact-check covid claims. *MIT Technology Review.* technologyreview.com

Check 7 — Regulierungen weltweit

Frage: Welche KI-Gesetze gelten für mein Unternehmen?

EU AI Act

– Risikobasierter Ansatz: Verboten / Hochrisiko / Begrenzt / Minimal.

– Hochrisiko-KI (HR, Medizin, Justiz): Pflicht zu Transparenz, Logs, menschlicher Aufsicht.

– AI Omnibus 2025: Vereinfachung geplant — Hochrisiko-Regeln erst ab Dez. 2027/Aug. 2028 verbindlich; KMU und kleine Mid-Caps erhalten Erleichterungen.

– Bussgelder bis EUR 35 Mio. oder 7% Jahresumsatz.

Der EU AI Act entpuppt sich immer mehr als bürokratischer Papiertiger. Die zeitliche Verzögerung macht es KMU zwar einfacher, schützt uns aber wenig. Ein Beispiel ist die DSGVO: Zwar werden grosse Bussgelder gesprochen — bis heute aber eigentlich noch nichts einbezahlt von Amazon, Facebook und Co.

Referenz: EU AI Act: 3 Gründe warum ihre Firma eine KI Richtlinie braucht

Kalifornien — Gouverneur Newsom unterzeichnet mehrere KI-Gesetze

Tabelle 3 — Kalifornien: KI-Gesetze in Kraft seit Januar 2026

Gesetz	Inhalt	Link
SB 53	Frontier-KI-Entwickler: Sicherheitsrahmen veröffentlichen, Zwischenfälle melden, Whistleblower schützen.	leginfo.legislature. ca.gov
AB 489	KI darf sich nicht als lizenzierter Arzt / Anwalt ausgeben.	leginfo.legislature. ca.gov
SB 243	Chatbots und Minderjährige — Schutzpflichten.	leginfo.legislature. ca.gov
SB 524	Polizeiberichte mit KI — Kennzeichnungspflicht.	leginfo.legislature. ca.gov

Notiz: Alle 4 Gesetze seit Januar 2026 in Kraft. Quelle: gov.ca.gov — Gouverneur Newsom unterzeichnet KI-Gesetze, Sept. 2025.

Warum wichtig für KMU: Wer Software aus den USA nutzt oder US-Kunden hat, ist indirekt betroffen. Es lohnt sich ausserdem, als **KMU eine eigene**

KI-Transparenz-Angabe zu machen (siehe ganz unten für ein Beispiel).

Bonus 8 — Schatten-KI im Griff

Frage: Welche KI nutzen meine Mitarbeitenden, ohne Wissen der IT-Abteilung?

Unter Schatten-KI versteht man die nicht genehmigte Nutzung von KI-Tools durch Mitarbeitende ohne formelle Genehmigung oder Aufsicht durch die IT-Abteilung. Konkrete Beispiele: ChatGPT, Gemini oder Copilot für Arbeitsaufgaben — ohne Datenschutz-Check oder Genehmigung.

Sofort-Massnahmen:

– Mitarbeitende befragen: «Welche KI-Tools nutzt ihr privat für die Arbeit?»

– Spesenabrechnungen und Firmenkreditkarten prüfen (KI-Abos!).

– Browser-Extensions inventarisieren — oft unbemerkte Datenabflüsse.

– DSGVO-Risiko prüfen: Welche Schatten-KI verarbeitet Kundendaten?

3 einfache Governance-Regeln (EU AI Act konform):

– Liste erlaubter KI-Tools definieren (z.B. Mistral Business oder Open-Source-Optionen wie in Tabelle 2).

– Klare Regel: Keine Kundendaten in nicht zuvor genehmigten Tools.

– Vorfälle melden — Pflicht ab 2027 für Hochrisiko-KI.

Warum wichtig: Gemäss Zylo 2026: Unternehmen nutzen durchschnittlich 269 SaaS-Tools; die IT-Abteilung kennt davon nur die Hälfte. Ein DSGVO-Verstoss auf dem privaten Handy bedeutet persönliche Haftung.

Referenz: EU AI Act: 3 Gründe warum ihre Firma eine KI Richtlinie braucht

Bonus 9 — Ensu & GPT4All: Lokale KI ohne Cloud

Beide Tools laufen vollständig auf deinem Gerät. Keine Daten verlassen deinen Computer.

Ensu (Ente)

Ensu ist ein kostenloser KI-Assistent für dein Gerät — kein Internet nötig, kein Cloud-Zugang. Ideal für private Gedanken, Notizen oder Gespräche über Bücher. Die App läuft auf iOS, Android, macOS, Linux, Windows und im Browser. Der Kern ist in Rust geschrieben — schnell und sicher. E2EE-Synchronisation zwischen Geräten ist in Entwicklung.

Noch nicht so stark wie ChatGPT — aber 100% privat. Download: ente.io/download

GPT4All (Nomic AI)

GPT4All ist kein Chatbot — es ist ein intelligentes Archiv. Du indexierst deine eigenen Dokumente (PDF, Word, TXT, Markdown) und stellst dann Fragen, die nur mit deinen Inhalten beantwortet werden.

So funktioniert es:

1. Ordner mit Dokumenten auswählen
2. Im Register «LocalDocs» Ordner von Mac oder PC angeben
3. GPT4All indexiert alles (kann mehrere Stunden dauern)
4. Fragen stellen — Antworten kommen nur aus deinen Docs

Ideal für: Verträge durchsuchen, internes Know-how nutzen, Handbücher auswerten. Für Firmen mit mehr als 25 Nutzern: Nomic Teams ab USD 40/Nutzer/Monat. Download: gpt4all.io

Referenz: Wolski, D. & Freist, R. (2025-05-18). 11 Gratis-KI-Tools, die lokal auf dem PC laufen. *PC Welt.* pcwelt.de

Erklärung zur KI-Nutzung

Verantwortlichkeitserklärung zur KI Nutzung: Alle Kernideen, die kreative Ausrichtung und der intellektuelle Inhalt stammen vom Autor. KI-Tools wurden ausschliesslich zur Unterstützung bei Grammatik, Verständlichkeit und struktureller Überarbeitung eingesetzt. Jedes Element des endgültigen Werkes wurde von Urs E. Gattiker, Ph.D., DrKPI®, **geprüft und genehmigt**.

Version 1.0 — 2026-03-12 | DrKPI® | drkpi.com | MC Lago Workshop

Accurate, reliable and valid measurement is the fuel that powers smart decision-making.

— Urs E. Gattiker, Ph.D., DrKPI®

Genaue, zuverlässige und valide Messung ist der Treibstoff für intelligente Entscheidungen.

— Urs E. Gattiker, Ph.D., DrKPI®
