

PRAKTISCHES WERKZEUG · VERANTWORTUNGSVOLLER KI-EINSATZ

KI-Beschaffungsraster für KMU

Eine E-Mail · 7 Fragen · Eine schriftliche Spur · Keine mündlichen Versprechen.

Dieses Werkzeug verhindert, dass eine KI-Funktion auf blosses Verkaufsversprechen hin gekauft wird. Es zwingt den Anbieter zu schriftlichen Antworten – zu Daten, Hosting, Training, Unterauftragnehmern, Logs, Garantien und Vertragsausstieg.

Anleitung

1

Anwendungsfall beschreiben
Ein konkreter Satz: Tool + Team + unterstützte Aufgabe + betroffene Daten. Bsp.: Support-Tickets zusammenfassen, damit das Team priorisieren kann.

2

Muster-E-Mail senden
Die untenstehende E-Mail an den Anbieter kopieren. Nicht mündlich verhandeln: Antworten schriftlich, mit beigelegten Dokumenten (AVV/DPA, Unterauftragnehmer, Sicherheit).

3

Jede Antwort einordnen
Eine Zeile pro Frage, drei mögliche Status: OK, Zu klären, Blockierend.

4

Entscheiden
GO: Kauf freigegeben · GO mit Auflagen: mit Klausel oder schriftlicher Freigabe · NO-GO: abgelehnt. Bei rechtlichen Zweifeln oder sensiblen Daten: vor der Unterschrift Stellungnahme der/des KI-Verantwortlichen / Rechtsabteilung / DSB einholen.

Muster-E-Mail an den Anbieter

Guten Tag, wir prüfen Ihre Lösung **[Name des Tools]** für folgenden Anwendungsfall: **[Anwendung in einem Satz]**. Können Sie vor jedem Kaufentscheid die 7 folgenden Fragen schriftlich beantworten?

1. Welche Daten werden von Ihrer KI-Funktion gesendet, gespeichert oder verarbeitet?

2. Wo werden diese Daten gehostet und in welchen Rechtsräumen?

3. Können unsere Daten zum Trainieren, Verbessern oder Bewerten Ihrer Modelle verwendet werden? Falls ja: Lässt sich dies vertraglich deaktivieren?

4. Welche Unterauftragnehmer, Drittmodelle oder Cloud-Anbieter sind an der KI-Verarbeitung beteiligt?

5. Welche Logs, Prompt-Verläufe, KI-Ausgaben oder Spuren werden aufbewahrt, wie lange, und wer hat Zugriff darauf?

6. Welche Garantien bieten Sie bei Fehlen, Halluzinationen, Datenlecks oder schädlichen Ausgaben?

7. Wie können wir unsere Daten exportieren, löschen oder löschen lassen, wenn wir Ihre Lösung verlassen?

Bitte legen Sie zudem Ihre Sicherheitsdokumente, den AVV/DPA, spezifische KI-Bedingungen, die Liste der Unterauftragnehmer und verfügbare Compliance-Unterlagen bei. — Freundliche Grüsse, **[Name]**

Entscheidungsraster – 7 Fragen an den Anbieter

Ordnen Sie jede schriftliche Antwort ein und entscheiden Sie dann: GO · GO mit Auflagen · NO-GO.

FRAGE AN DEN ANBIETER	STATUS	AUFLAGE / VERANTWORTLICH
1 Verarbeitete Daten?	OK Zu klären Blockierend	Welche Felder / Datentypen lassen sich bereits bei der Konfiguration ausschliessen? Wer validiert die zugelassene Liste (KI-Verantwortliche + Fachbereich)?
2 Hosting / Rechtsraum?	OK Zu klären Blockierend	Muss CH / EU / EWR vertraglich verlangt werden? Wer prüft Übermittlungen ausserhalb des Raums (Rechtsabteilung / DSB)?
3 Training mit unseren Daten?	OK Zu klären Blockierend	Ist das Opt-out durch uns aktivierbar oder muss es vertraglich geregelt werden? Wer stellt sicher, dass es bei jeder Verlängerung aktiv bleibt (KI-Verantwortliche)?
4 KI-/Cloud-Unterauftragnehmer?	OK Zu klären Blockierend	Meldet der Anbieter jeden Wechsel von Unterauftragnehmern? Wer pflegt die interne Liste der Abhängigkeiten (IT / KI-Verantwortliche)?
5 Logs: Dauer / Zugriff?	OK Zu klären Blockierend	Welche maximale Aufbewahrung ist für unsere Prompts akzeptabel (30 / 90 / 180 Tage)? Wer kann die Löschung verlangen und nach welchem Verfahren?
6 Garantie bei Fehler / Leck?	OK Zu klären Blockierend	Welche Haftungsobergrenze im Verhältnis zum Jahresbudget? Wer ist die Ansprechperson bei Vorfällen (Anbieter / KMU)?
7 Export / Löschung der Daten?	OK Zu klären Blockierend	Ist das Exportformat wiederverwendbar (CSV, JSON) oder proprietär? Wer testet das Ausstiegsverfahren einmal pro Jahr (KI-Verantwortliche)?

QUELLEN

NIST (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. DOI: <https://doi.org/10.6028/NIST.AI.100-1>
Mantelero, A. (2022). *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*. DOI: <https://doi.org/10.1007/978-94-6265-531-7>