

PeakPrivacy

Leitfaden: Sichere KI-Einführung für Schweizer KMU

Wie euer Team KI produktiv nutzt, ohne die Kontrolle über eure Daten zu verlieren — mit Checkliste für die Anbieterwahl und einem klaren Fahrplan für die ersten 90 Tage.

1. Warum ~80 % der KI-Projekte an der Einführung scheitern

Das Muster kennen viele: Ein Tool wird gekauft, die Logins gehen an die Belegschaft — und nach drei Monaten nutzt es niemand mehr. Das Budget ist verbrannt, das Vertrauen in KI gleich mit.

Das Problem liegt selten an der Technologie. Es liegt daran, dass KI-Einführung als IT-Projekt behandelt wird — nicht als organisatorische Veränderung. Der Zugang ist leicht, aber:

- **Prozessaufbau und Training fehlen.** Niemand weiss, welche Aufgaben sich wirklich eignen.
- **Es gibt keine internen Vorbilder.** Ohne Kolleg*innen, die vorangehen, bleibt KI ein Fremdkörper.
- **Niemand misst, ob es wirkt.** Ohne dokumentierte Ergebnisse fehlt die Grundlage für den nächsten Schritt — es bleiben Frustration, Risiko und verschwendetes Geld.

Die Konsequenz für euer Team: Startet bei den Menschen, nicht bei der Technik. Die folgenden Kapitel zeigen, was sichere KI-Nutzung konkret heisst — und wie eine Einführung gelingt, die im Arbeitsalltag ankommt.

2. Was sichere KI-Nutzung heisst: Der Datenstandort entscheidet

Die wichtigste Frage bei jedem KI-Einsatz: **Wo werden eure Daten verarbeitet?** PeakPrivacy hat rund um diese Logik drei Sicherheitsstufen aufgebaut:

- **Swiss** — Die Verarbeitung bleibt in der Schweiz. Die sicherste der drei Stufen für sensible Daten.
- **EU** — Die Verarbeitung bleibt in der EU. Geeignet für Anfragen mit üblichen Schutzanforderungen.
- **US** — Die Verarbeitung kann die Schweiz bzw. die EU verlassen. Nur für nicht sensible Anfragen.

Zwei Prinzipien machen das im Alltag praktikabel:

1. **Standardmässig Schweiz.** PeakPrivacy wird standardmässig in der Schweiz betrieben. Eine Verarbeitung in der EU oder in den USA findet nur statt, wenn du dich ausdrücklich dafür entscheidest.

2. **Jedes Modell ist gekennzeichnet.** Jedes KI-Modell trägt sichtbar seine Sicherheitsstufe — jede Person im Team weiss jederzeit, wofür sie sich entscheidet.

Faustregel für euer Team: Besonders schützenswerte Daten → Swiss. Die Verarbeitung muss in der EU bleiben → EU. Aufgaben mit geringer Sensibilität → US ist möglich.

3. Ein Blick unter die Haube: eigene Server in der Schweiz

Sicherheitsstufen sind nur so glaubwürdig wie die Infrastruktur dahinter. Deshalb lohnt sich der Blick unter die Haube:

- **Eigene Server statt gemietete Cloud.** Wir betreiben eigene Server in Schweizer Swisscom-Rechenzentren — mit 24/7-Security und physischem Zutrittsschutz, ISO 27001 am DC-Standort (Swisscom).
- **Volle Kontrolle über den Betrieb.** Die Schweizer Modelle laufen auf unseren eigenen LLM-Servern ohne fremde Cloud-Dienste. So stellen wir sicher, dass eure Eingaben nicht für das Training von Modellen verwendet werden.
- **Tägliche Offsite-Backups innerhalb der Schweiz,** isoliert von der Produktion.
- **Verschlüsselung** bei der Übertragung (TLS 1.2/1.3) und für ruhende Daten.
- **Von Dritten geprüft:** kontinuierliche Schwachstellen-Scans und periodische externe Penetrationstests durch unabhängige Cyber-Security-Spezialisten. Die Berichte stehen Kunden auf Anfrage unter NDA zur Verfügung.

Warum das zählt: Wer die Server selbst betreibt, muss sich nicht auf die Zusagen Dritter verlassen — und kann euch die Details offenlegen, statt auf ein Kleingedrucktes zu verweisen.

4. Datenkontrolle im Alltag: Zugriff, Governance, Audit

Sichere KI-Nutzung entscheidet sich nicht nur beim Hosting, sondern jeden Tag: Wer darf was — und lässt sich das nachvollziehen?

- **Zugriff:** Rollenbasierter Zugriff und Berechtigungen, mit SSO-/SAML-Optionen und IP-Allowlisting. Nur autorisierte Personen erreichen die Plattform und euer Wissen.
- **Governance:** Admins steuern, welche Modellklassen für Rollen, Teams und Assistenten verfügbar sind. Eure Organisation legt fest, welcher Verarbeitungsstandort für welche Datentypen erlaubt ist.
- **Daten:** Aufbewahrungsregeln und sichere Löschung — inklusive vollständiger Datenentfernung bei Bedarf.
- **Audit:** Audit-Logs und Nutzungstransparenz, einschliesslich eines Token-Usage-Dashboards. Du kannst prüfen, was passiert ist, wann und durch wen.

Praktisch heisst das: Ihr müsst nicht hoffen, dass sich alle an die Regeln halten. Ihr könnt die Regeln technisch durchsetzen — und die Nutzung gegenüber der Geschäftsleitung belegen.

5. Knowledge Boxes: Firmenwissen nutzen, ohne es preiszugeben

Der grösste Hebel für den Arbeitsalltag: eine KI, die auf Grundlage eurer eigenen Unterlagen antwortet — Dokumente, Richtlinien, Leitfäden. In PeakPrivacy heisst dieser sichere Bereich **Knowledge Box**.

Entscheidend ist, was dabei mit euren Daten passiert:

1. **Die Dokumente bleiben auf der Schweizer Infrastruktur** von PeakPrivacy.
2. Stellt jemand eine Frage, zieht PeakPrivacy **nur die relevanten Auszüge** aus der Knowledge Box.
3. Das KI-Modell erhält **nur die Frage und diese Auszüge** — nicht die vollständigen Dokumente und nicht eure gesamte Wissensbasis.

Dazu ist Nachvollziehbarkeit über Quellenangaben möglich: Euer Team kann sehen, worauf sich eine Antwort stützt, und sie nachprüfen — statt einer Blackbox blind zu vertrauen.

6. Doppelter Boden: Pseudonymisierung mit Presidio

Auch mit klaren Regeln kommt der Moment: Jemand will für eine Aufgabe ein externes Modell nutzen. Für diese Fälle gibt es einen doppelten Boden.

PeakPrivacy pseudonymisiert mit **Microsoft Presidio**: Sensible Angaben können entfernt werden, bevor eine Anfrage übermittelt wird. Zusätzlich werden die Inhalte, die an Drittanbieter gesendet werden, auf das Nötigste minimiert.

Das Prinzip dahinter: **Privacy by Default**.

- Die Standardeinstellungen bevorzugen die in der Schweiz gehosteten Modelle.
- Externe US-Closed-Source-Modelle erfordern ein klares Opt-in — mit jederzeitiger Opt-out-Möglichkeit.
- Wer mit sensiblen Daten arbeitet, kann jederzeit auf ein sichereres Modell wechseln.

So wird Datenschutz nicht zur Disziplinfrage jedes einzelnen Teammitglieds, sondern zur Voreinstellung des Systems.

7. Das richtige Modell für jede Aufgabe

Nicht jedes Modell gehört in denselben Topf. PeakPrivacy arbeitet deshalb mit Modellklassen — jede mit klar zugeordnetem Verarbeitungsstandort:

- **Swiss Daily** — für den Arbeitsalltag: Chat, Meeting Bot, Zusammenfassungen, Dokumentararbeit und Standard-Assistenten. Verarbeitung in der Schweiz, **in den Paketen enthalten**.
- **Frontier (optional)** — für Deep Research, Premium-Reasoning und komplexe Analysen: die besten verfügbaren Modelle. Verarbeitung in der EU oder den USA — verlässt den Schweizer Pfad und ist entsprechend gekennzeichnet.
- **Optionale EU-Modelle** — schnelle, mehrsprachige Workloads. Verarbeitung in der EU, nur mit Admin-Freigabe.
- **Systemmodelle** — Transkription, Suche und RAG laufen im Hintergrund, ausschliesslich in der Schweiz oder EU.

Für euer Team bleibt es einfach: Mitarbeitende sehen nur die Modelle, die freigegeben sind — keine Kostenlogik, keine Konfigurationsfallen. Admins wählen die Balance aus Qualität, Geschwindigkeit, Standort und Datenschutz.

8. Kein Lock-in: die Exit-Garantie

Eine ehrliche Anbieterbeziehung schliesst das Ende mit ein. Falls ihr euch irgendwann für einen Wechsel entscheidet, gilt die **Exit-Garantie**: Ihr könnt eure Daten exportieren, und wir bestätigen die Löschung aus unserer Infrastruktur.

Dazu gehören Datenportabilität und ein klarer Exit-Prozess — festgehalten, bevor ihr startet, nicht erst wenn es so weit ist.

Und wenn eure Anforderungen über ein standardmässiges Cloud-Setup hinausgehen: Über das Enterprise-Angebot sind zusätzliche Deployment-Optionen möglich — **Private Cloud** (eine dedizierte Umgebung für eure Organisation) oder **On-Premises** (das System läuft in eurer eigenen Infrastruktur, unter eurer direkten Kontrolle).

9. Adoption ist Teil des Produkts: der begleitete Einführungsweg

Die sicherste Plattform nützt nichts, wenn sie niemand nutzt. Deshalb ist die Einführung bei PeakPrivacy kein Zubehör, sondern Teil des Produkts — begleitet von Anfang bis Ende:

- **Kickoff-Workshop** — gemeinsam die passenden Einsatzfelder für euer Team identifizieren.
- **KI-Botschafterinnen-Programm** — *interne Personen, die die KI-Transformation im Haus vorantreiben und Kolleginnen mitnehmen.*
- **Enablement** — Workshops, Help Center, Live-Chat und 1:1-Support, damit AI Literacy im Team nachhaltig entsteht.

> «PeakPrivacy entwickelt mit uns praxisnahe KI-Lösungen — nicht nur Standardprodukte. Das hohe Datenschutzniveau über verschiedene KI-Modelle hinweg ist entscheidend.»

> — Harry Witzthum, Head of Digital Transformation, Caritas Switzerland

Für die Pakete Growth und Scale gilt zusätzlich die **Team Success Guarantee**: Wenn die vereinbarten Erfolgskriterien nach 90 Tagen trotz aktiver Mitarbeit nicht erreicht sind, liefern wir einen 4-Wochen Success Sprint kostenlos — vertraglich festgehalten.

10. Der risikoarme Einstieg: der 90-Tage-Pilot

Wenn ihr zuerst testen wollt, bevor ihr euch festlegt: Der 90-Tage-Pilot ist eine ehrliche Standortbestimmung — keine Marketing-Versprechen, sondern 90 Tage echtes Testen.

Das Paket: CHF 4'500 einmalig · 10 Nutzerlizenzen · 2 Workshops (3 h + 2 h) · technisches Setup inkl. SSO und Knowledge Boxes · Schweizer Hosting ab Tag 1.

Die drei Phasen:

1. **Aktivierung (Monat 1):** Kickoff mit den Stakeholdern, technisches Setup, Discovery-Workshop — 5 bis 10 Mitarbeitende bauen ihren ersten AI-Assistenten.
2. **Ausarbeitung (Monat 2):** Scale-Workshop, Coaching, Usage-Review — erste validierte Use Cases.
3. **Nachweis (Monat 3):** KI-Botschafter*innen-Gruppe, aggregierte Use-Case-Übersicht, Abschluss-Call mit Fahrplan.

Das Ergebnis: 5+ Mitarbeitende, die KI wöchentlich an realen Aufgaben nutzen, eine zertifizierte KI-Botschafter*in, dokumentierte Zeitersparnis — und ein board-ready **Pilot Assessment Report** für die Geschäftsleitung.

Das Geld-zurück-Versprechen: Wenn am Ende des Pilots keine echte Erfolgsstory entsteht, bekommst du die Pilotgebühr zurück. Und bei einem Upgrade auf Growth oder Scale werden CHF 3'000 der Pilotgebühr angerechnet.

11. Checkliste: 10 Fragen an jeden KI-Anbieter

Egal, für welchen Anbieter ihr euch am Ende entscheidet — diese zehn Fragen solltet ihr vor der Unterschrift stellen. Sie trennen Marketing von überprüfbaren Fakten:

1. **Wo werden unsere Daten standardmässig verarbeitet** — und findet eine Verarbeitung im Ausland nur statt, wenn wir uns aktiv dafür entscheiden?
2. **Betreibt ihr eure Server selbst** oder mietet ihr die Infrastruktur eines Dritten? In welchem Rechenzentrum, mit welcher Zertifizierung am Standort?
3. **Werden unsere Eingaben für das Training von Modellen verwendet?**
4. **Sehen unsere Mitarbeitenden bei jedem Modell**, wo die Verarbeitung stattfindet — bevor sie es nutzen?
5. **Können wir pro Rolle und Team steuern**, wer welche Modelle und Verarbeitungsstandorte nutzen darf?
6. **Was genau erhält das KI-Modell**, wenn wir interne Dokumente anbinden — unsere ganze Wissensbasis oder nur die relevanten Auszüge?
7. **Was passiert mit sensiblen Angaben**, bevor eine Anfrage ein externes Modell erreicht — gibt es eine Pseudonymisierung?
8. **Gibt es Audit-Logs und Nutzungstransparenz**, damit wir nachvollziehen können, was wann durch wen passiert ist?
9. **Wie kommen wir wieder raus?** Gibt es einen Datenexport und eine bestätigte Löschung nach Vertragsende?
10. **Wie sieht die Einführung aus** — Logins verschicken, oder ein begleiteter Rollout mit Workshops, internen Botschafter*innen und messbaren Erfolgskriterien?

Fair ist fair: Diese Fragen kannst du auch uns stellen. Unsere Antworten stehen öffentlich auf peakprivacy.ch — vom Security Factsheet über die Sicherheitsstufen bis zum 90-Tage-Pilot.

12. Der nächste Schritt

Sichere KI-Einführung ist kein Hexenwerk — aber auch kein Selbstläufer. Es braucht drei Dinge: einen Datenstandort, den ihr kontrolliert, Regeln, die im Alltag technisch durchsetzbar sind, und eine Einführung, die bei den Menschen beginnt.

Wenn du besprechen willst, wie das für euer Team konkret aussieht: Buche ein **15-Min Kennenlernen** — unverbindlich. Wir beantworten deine Fragen und empfehlen den sichersten Weg für euren Anwendungsfall.

[15-Min Kennenlernen buchen →](<https://cal.com/team/peakprivacy/kennenlernen>)

Nächster Schritt: Buche ein 15-Min Kennenlernen — unverbindlich. Wir beantworten deine Fragen zu Sicherheit, Rollout und dem 90-Tage-Pilot und empfehlen den sichersten Weg für euren Anwendungsfall: <https://cal.com/team/peakprivacy/kennenlernen>
→ peakprivacy.ch — Button «15-Min Kennenlernen»

Alle Angaben basieren auf den publizierten Informationen von peakprivacy.ch (Security-Factsheet, Sicherheit, KI-Modelle, Pilot). © PeakPrivacy / freihandlabor GmbH, Zürich.