PeakPrivacy

22. INFO SPRINT ONEGOV.CH · CLOUD UND EXITSTRATEGIEN

Ihre Daten. Aber wessen Spielregeln?

Warum KI-Agenten Datensouveränität und Open Source neu relevant machen.

Fabio Duò · Gründer freihandlabor GmbH / PeakPrivacy · Zürich, 27. Oktober 2026

Daten exportieren ist der halbe Exit.

DIE ÜBLICHE EXIT-FRAGE

Kriege ich meine Daten raus?

Export, Format, Löschbestätigung, Zertifikat. Wichtig – und meistens beantwortet.

DIE ANDERE HÄLFTE

Darf ich mit meinen Daten die Prozesse bauen, die ich brauche?

Mit den Werkzeugen, die ich will. Zu Bedingungen, die ich kenne.

Entschieden wird das nicht im Rechenzentrum, sondern an drei Stellen: **API, Lizenz, Nutzungsbedingungen.**

Open Source hat jahrelang an schlechten Oberflächen gelitten.

UNSERE EIGENE GESCHICHTE

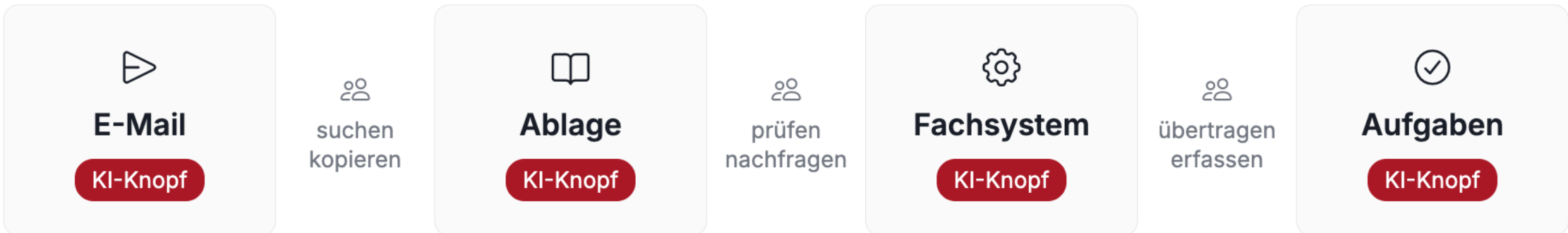
Der Code war offen. Die Funktionen waren da. Die Daten gehörten uns.

Und trotzdem gewann die hübschere Software aus dem SaaS-Katalog. Verständlich – dort arbeitet man den ganzen Tag.

Oberfläche	entschied
Offener Code	zählte wenig
Zugang zu den Daten	zählte wenig

Mit KI-Agenten dreht sich diese Reihenfolge zum ersten Mal um.

So kommt KI heute an: ein Knopf in jeder App.



Vier Knöpfe, drei Lücken. Die Arbeit **zwischen** den Apps bleibt beim Menschen.

Vier KIs, je ein Viertel der Information.

MAIL-ASSISTENT

kennt das Dossier nicht

ABLAGE-KI

weiss nicht, was in der Mail stand

COPILOT IM FACHSYSTEM

sieht die Anhänge nicht

AUFGABEN-KI

kennt den Fall gar nicht

Jede antwortet selbstbewusst. Keine hat das ganze Bild.

Was früher ein Mensch im Kopf zusammenhielt, hält jetzt niemand mehr zusammen. Die Ergebnisse werden schlechter, nicht besser.

Eingebaute KI ohne Kontext: viel Nutzung, wenig Wirkung.

≈ 0 %

Effekt auf Löhne und Stunden – trotz breiter Chatbot-Nutzung

Dänische Registerdaten, zwei Jahre nach ChatGPT. Effekte über 2 % ausgeschlossen.

Humlum & Vestergaard, NBER, rev. 2026

−2 Std.

E-Mail pro Woche mit Office-Copilot – sonst keine Verschiebung

RCT, 7'137 Personen, 66 Firmen. Welche Aufgaben erledigt werden: unverändert.

Dillon et al., NBER 2025

+19 %

langsamer mit KI-Tools – und fühlten sich 20 % schneller

RCT, 16 erfahrene Entwickler, 246 echte Aufgaben. Hauptgrund: Der KI fehlte der implizite Kontext.

METR, Juli 2025

95 %

der Firmen ohne messbaren Return aus GenAI-Piloten

Gründe: Tools lernen nicht, kein Kontext, nicht in Prozesse eingebettet. 153 Leader, 53 Interviews.

MIT NANDA, «The GenAI Divide», Aug. 2025

Vier Studien, ein gemeinsamer Nenner: **Die KI sieht nur einen Ausschnitt.**

Der Wendepunkt: ein Auftrag statt vier Apps.

> DER AUFTRAG
>
> *«Bereite diese Anfrage vor. Was ist da, was fehlt, was steht im Dossier? Lege mir Entwurf und nächste Schritte zur Freigabe vor.»*



Dazwischen eine kontrollierte Zugriffsschicht: Identität, minimale Rechte, erlaubte Aktionen, Protokoll. Keine Berechtigung per Prompt. Lesend beginnen. Keine automatische Verfügung.

Mit Kontext und Werkzeugen: Agenten bringen mehr.

ASSISTENT VS. AGENT

−62 %

Bearbeitungszeit mit Agent statt Assistent

Belastung −57 %, Korrektheit unverändert. 24 Entwickler, kontrolliertes Experiment.

Appelt & Glauben, TU Darmstadt, PACIS 2026

MENSCH + AGENT VS. MENSCH + MENSCH

+50 %

Output pro Person im Team mit KI-Agent

Randomisiert, 2'234 Personen. Textqualität höher, Bildqualität tiefer, Wirkung im Feld gleich.

Ju & Aral, MIT / Johns Hopkins, 2025

WER PROFITIERT

3×

so oft skalieren KI-Spitzenunternehmen Agenten

¾ gestalten Prozesse neu (vs. ¼). Fast die Hälfte baut Software selbst statt zu kaufen (vs. 31 %).

McKinsey, State of AI, Aug. 2026, n = 1'719

Derselbe Hersteller, dasselbe Modell – der Unterschied ist Kontext und Handlungsspielraum. Kleine Stichproben, oft Softwarearbeit; der Beweis für Verwaltungsprozesse steht aus.

In diesem Bild arbeitet niemand mehr in der Oberfläche.

BISHER GEWANN

die beste oder verbreiteste Oberfläche

Weil dort Menschen den ganzen Tag gearbeitet haben.



JETZT GEWINNT

die Software, mit der ich bauen darf

Weil der Agent über die Schnittstelle arbeitet.

Was zählt: Was darf ich über die API lesen und schreiben – wie oft, zu welchem Preis, unter welchen Bedingungen?

Was Anbieter mit ihren Schnittstellen machen.

Drosseln

Wie oft darf ich zugreifen?

Slack · Atlassian

Erlauben

Darf ein Agent das überhaupt?

SAP · Google Workspace

Verrechnen

Was kostet der Zugriff extra?

Salesforce · HubSpot · CMI

Sieben dokumentierte Fälle, Stand 27.10.2026. Vier Änderungen, drei bestehende Modelle. Keine Aussage über Absichten.

DROSSELN

Wie oft darf ich zugreifen?

Slack

1 Request / Minute

Maximal 15 Objekte pro Aufruf für Nachrichtenverläufe – bei bestimmten Apps ausserhalb des Marketplace, bei Neuinstallation.

Der Zugriff hängt vom Vertriebskanal der Integration ab.

Atlassian

Punkte-Kontingent

Für Jira- und Confluence-Cloud-Apps seit 2. März 2026. Kontingent erschöpft: Anfragen bis zum Reset abgewiesen.

Keine Gebühr – aber eine Kapazitätsregel für jede Integration.

Ausnahmen: bestehende Slack-Installationen, interne und Marketplace-Apps; Atlassian API-Token-Traffic. Quellen im Anhang.

ERLAUBEN

Darf ein Agent das überhaupt?

SAP

API Policy 2.2.2

Agenten, die API-Aufrufe planen oder ausführen, nur auf SAP-unterstützten Wegen. Version 4.2026a. DSAG kritisiert fehlende Klarheit.

Ob ein Agent mit dem ERP arbeiten darf, ist nicht nur technisch.

Google Workspace

Neue Kontingente

Für neue Projekte seit Mai 2026. Gebühren oberhalb täglicher Schwellen angekündigt, 90 Tage Vorlauf – noch nicht eingeführt.

Auch längst eingesetzte Bürosoftware kann morgen kontingentiert sein.

Kein Totalverbot bei SAP; gesetzliche Exportpflichten unberührt. Google: Übergangsregeln für bestehende Projekte. Quellen im Anhang.

VERRECHNEN

Was kostet der Zugriff extra?

Salesforce

+25 USD

pro Nutzer und Monat für die Web Services API in der Pro Suite.

Nutzen und Zugreifen sind zwei Produkte.

HubSpot

500 USD

pro Monat für 1 Mio. zusätzliche API-Aufrufe pro Tag. Basisvolumen inklusive.

API-Kapazität wird ein eigener Kostenposten.

CMI

API-Lizenz

Eigene Lizenz laut FAQ – On-Premises wie in der Cloud. Preis nicht öffentlich.

Auch Schweizer Software im eigenen Rechenzentrum.

Tarifmodelle, keine belegten Preissprünge. CMI hält niemandem Daten zurück. Quellen im Anhang.

Datenbesitz ist nicht dasselbe wie Handlungsfreiheit.

Die Daten können uns gehören – und trotzdem bestimmt der Anbieter,
was wir damit automatisieren dürfen.

Bexio bleibt. Odoo kommt.

BEHALTEN UND VERBINDEN

Bexio · Buchhaltung

Alternativen geprüft: hübscher, KI-naher, aber unvollständig. Die Schnittstelle reicht für unsere Agenten – also bleibt Bexio.

ÖFFNEN UND ERWEITERN

Odoo · CRM, Projekte, Zeit

Open Source, Code in der Hand. Die Oberfläche ist uns weniger wichtig als vor drei Jahren – der Agent übernimmt die Routine.

Behalten, was über die Schnittstelle erreichbar ist. Öffnen, wo wir anpassen wollen.

Praxisbericht, keine Studie. Odoo Community unter LGPLv3; Enterprise und Hosting-Tarife getrennt betrachten. Migration läuft.

Kaufen Sie nicht Funktionen. Sichern Sie Handlungsfreiheit.

Zugriff

Sind Daten und Fachfunktionen über dokumentierte Schnittstellen wirklich nutzbar – nicht nur «es gibt eine API»?

Bedingungen

Sind Agentennutzung, Kontingente und Kosten vorhersehbar und im Vertrag festgehalten?

Portabilität

Kommen Beziehungen, Metadaten und Konfiguration mit – nicht nur Dateien?

Kontrolle

Können wir Rechte durchsetzen, Aktionen nachvollziehen, Komponenten austauschen?

Gilt für jede Agentenplattform – unsere eingeschlossen. Prozessdefinitionen, Integrationen, Rechte und Protokolle müssen exportierbar bleiben.

Dieselben vier Fragen – an jede Agentenplattform.

	Anthropic · Claude	OpenAI · ChatGPT	Mistral	PeakPrivacy
Sitz	USA	USA	Frankreich	Schweiz
Modelle	proprietär	proprietär	offene Gewichte und proprietär	offene Modelle
Betrieb	Cloud des Anbieters	Cloud des Anbieters	Cloud oder On-Premises	selbst betrieben, CH-Rechenzentrum
Werkzeuge	MCP, offener Standard	Agents SDK, MCP	Agents API	MCP
Wechsel	Prozesse und Daten exportierbar?	Prozesse und Daten exportierbar?	Prozesse und Daten exportierbar?	Prozesse und Daten exportierbar

Illustration, kein Ranking und keine Empfehlung. Die letzte Zeile beantwortet keine Website – nur ein Wechseltest.

So starten Sie – ohne eine einzige KI-Lizenz zu kaufen.

1

Einen Prozess wählen

Viele Übergaben, viel Suchen, viel Nacharbeit.

2

Heute messen

Bearbeitungszeit, Wartezeit, Nacharbeit, Kosten.

3

Begrenzter Pilot

Lesend und vorbereitend, mit Freigabe durch Menschen.

4

Nachmessen

Dieselben vier Kennzahlen, derselbe Prozess.

5

Wechseltest

Export und Umzug probieren – bevor Sie skalieren.

Der Wechseltest ist der Schritt, den alle auslassen. Er ist der einzige, der Ihre Exitstrategie beweist.

PeakPrivacy

Souveränität ist die Freiheit, mit den eigenen Daten zu handeln.

Wir wollen nicht nur unsere Daten behalten. Wir wollen selbst bestimmen, wie daraus Arbeit wird.

Danke. Fabio Duò · freihandlabor GmbH / PeakPrivacy · peakprivacy.ch

Quellen

Slack: Rate limit changes for non-Marketplace apps, 29.05.2025

Atlassian: Confluence Cloud rate limiting

SAP: API Policy v.4.2026a, Abschnitt 2.2.2 · DSAG-Stellungnahme, 29.04.2026

Google: Workspace standardized model for agent tools and APIs

Salesforce: Sales Pricing, Web Services API

HubSpot: Product & Services Catalog, Technical Limits

CMI: CMI API, FAQ

Odoo: Odoo 19 licences · External API

Dillon et al.: Shifting Work Patterns with Generative AI, NBER 33795, 2025

Brynjolfsson, Li, Raymond: Generative AI at Work, QJE 2025

McKinsey: The State of AI in 2026, 25.08.2026

Appelt, Glauben: From Assistants to Agents, PACIS 2026

Ju, Aral: Collaborating with AI Agents, arXiv 2025

Humlum, Vestergaard: Still Waters, Rapid Currents, NBER 33777, rev. 2026

METR: Early-2025 AI and experienced developer productivity, 10.07.2025

MIT NANDA: The GenAI Divide: State of AI in Business 2025, Aug. 2025

Anthropic: Economic Index report, Nov. 2025 · Microsoft: Work Trend Index 2025

Event: OneGov.ch, 22. Info Sprint, 27.10.2026

Recherchestand 27. Oktober 2026. Angekündigte Gebühren sind als angekündigt, nicht als eingeführt dargestellt.