MINDTRAIN · KI-WOCHENREPORT

# KI-Wochenreport für KMU im DACH-Raum

**Woche 41/2026** · 28. September bis 5. Oktober 2026

Sechs Themenfelder · 10 Meldungen

Mindtrain GmbH · Der KI-Mentor für KMU

mindtrain.ch

Der Schwerpunkt dieser Woche liegt auf drei Themen: der Schweizer KI-Regulierung, dem Übergang von Chatbots zu handlungsfähigen Agenten und dem Aufbau von Governance und Kontrollmechanismen. Für Geschäftsleitungen entscheidet damit weniger die Modellwahl als die Frage, welche Prozesse sicher, messbar und mit menschlicher Freigabe automatisiert werden können. Zu jeder Meldung finden Sie die Quellen.


📈 Markt & Politik

⚙️ Tools & Tech

🏭 Branchen

🤖 Agenten

🌍 International

🎯 Empfehlung

# 01 Markt & Politik

## Schweiz: Vernehmlassungsvorlage zur KI-Regulierung wird vorbereitet

Die Schweiz hat die KI-Konvention des Europarats am 27. März 2025 unterzeichnet. Der Bundesrat hat das Justizdepartement zusammen mit UVEK und EDA beauftragt, bis Ende 2026 eine Vernehmlassungsvorlage zu erarbeiten. Sie soll Transparenz, Datenschutz, Nichtdiskriminierung und Aufsicht regeln. Ein allgemeines KI-Gesetz ist nicht geplant: Sektorübergreifende Regeln sollen sich auf grundrechtsrelevante Bereiche wie den Datenschutz beschränken, alles Weitere soll branchenspezifisch geregelt werden. Bis dahin gibt es keine KI-spezifische Gesetzgebung, es gelten insbesondere das Datenschutzrecht und branchenspezifische Vorschriften.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Führen Sie schon jetzt ein einfaches KI-Inventar: Welche Systeme werden in welchen Prozessen mit welchen Daten und welcher menschlichen Kontrolle eingesetzt? Das senkt spätere Anpassungskosten und schafft eine belastbare Grundlage für die Kommunikation gegenüber Kunden und Mitarbeitenden.

Quellen: **Bundesamt für Justiz** · **swissinfo (Keystone-SDA)** · **law.ch**

## EU AI Act: Transparenzpflichten sind aktiv

Seit dem 2. August 2026 gelten die Transparenzregeln nach Artikel 50. Wer Chatbots oder Sprachassistenten einsetzt, muss offenlegen, dass Nutzerinnen und Nutzer mit einer KI sprechen. Deepfakes und bestimmte KI-Texte zu Themen von öffentlichem Interesse müssen gekennzeichnet werden, ausser ein Mensch hat den Text geprüft und trägt die redaktionelle Verantwortung. Die maschinenlesbare Kennzeichnung durch die Anbieter der KI-Systeme wurde laut IHK Nürnberg auf Dezember 2026 verschoben.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Auch Schweizer Unternehmen können betroffen sein, wenn sie KI-Systeme im EU-Markt anbieten oder dort nutzen. Prüfen Sie Chatbots, KI-Telefonassistenten, Marketinginhalte und automatisierte Kundenkommunikation und legen Sie eine verantwortliche Person fest. Den Rechtsstand klären Sie mit Ihrer Rechtsberatung.

Quellen: **IHK Nürnberg** · **EU AI Act, Leitfaden zu Artikel 50** · **LAUSEN**

## Schweiz: KI gehört zum Arbeitsalltag, oft ohne klare Regeln

Laut der EY-Erhebung vom Mai 2026 (604 Befragte aus Schweizer Unternehmen) nutzen 89 Prozent KI im Berufsalltag, am häufigsten integrierte Tools wie Copilot oder Gemini (70 Prozent). 29 Prozent dürfen KI über private Accounts wie ChatGPT nutzen, für 8 Prozent ist das die einzige Möglichkeit. Nur 3 Prozent geben an, dass KI im Unternehmen vollständig verboten ist. Das KMU-Portal des SECO hat die Ergebnisse am 15. Juli 2026 aufgegriffen.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Die Nutzung findet statt, teils informell. Wichtiger als allgemeine Verbote sind klare Spielregeln: Welche Daten sind vertraulich, welche Tools zugelassen, wie werden Ergebnisse geprüft und wer ist verantwortlich? Bitte beachten: Befragt wurden Beschäftigte aus Unternehmen verschiedener Grössen, nicht nur aus KMU.

Quellen: **KMU-Portal (SECO)** · **EY Schweiz**

## 02 Tools & Technologien

### OpenAI GPT-6.1 Sol: fast so leistungsstark wie Astra, zu einem Fünftel der Token-Preise

OpenAI hat am DevDay vom 29. September GPT-6.1 Sol vorgestellt, eine Weiterentwicklung von GPT-6 Sol für agentisches Programmieren, Computersteuerung und professionelle Arbeitsabläufe. Laut OpenAI erreicht das Modell fast die Leistung von GPT-6 Astra bei rund einem Fünftel der Token-Preise. Verfügbar ist es über die API sowie in ChatGPT Work und Codex für Plus, Pro, Business, Enterprise und Edu.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Leistungsfähige Agenten werden günstiger, das senkt die Hürde für Pilotprojekte. Die Leistungsangaben stammen von OpenAI selbst: Testen Sie mit eigenen Aufgaben, bevor Sie Entscheide treffen.

Quellen: **InfoQ** · **Decrypt**

## OpenAI Dots: dauerhaft aktive Agenten, in der Schweiz zunächst nur über Business Premium

Dots sind persönliche Agenten, die laut OpenAI auf GPT-6 Astra laufen, auf einem eigenen Cloud-Computer mit Browser arbeiten und auch nach dem Schliessen der Sitzung weiterarbeiten. Sie bringen eingebaute Regeln mit, wann sie selbstständig handeln und wann sie um Freigabe bitten. OpenAI weist selbst darauf hin, dass Dots Fehler machen können. Pro-Nutzer im EWR, in der Schweiz und in Grossbritannien erhalten Dots vorerst nicht. Über Business Premium ist der erste Dot in allen unterstützten Regionen enthalten, Enterprise-Kunden können eine Beta nach Freigabe durch den Administrator testen.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Für Schweizer Unternehmen ist der Zugang derzeit nur über Business- oder Enterprise-Pläne möglich. Falls Sie testen, dann mit einem einzelnen Pilotplatz, überwiegend lesenden Aufgaben und aktivierten Freigaberegeln. Daten- und Berechtigungsfragen klären Sie vorher.

Quellen: **The Next Web** · **Trending Topics**

## 03 Branchen & Praxisbeispiele

### Schweizer Unternehmen: Die Nutzung ist breit, die Integration in Prozesse hinkt hinterher

Dieselbe EY-Erhebung zeigt die Lücke zwischen Tool-Nutzung und Prozessintegration: 55 Prozent setzen KI gezielt in einem oder mehreren Geschäftsbereichen ein, 31 Prozent sind noch in der Pilotphase, 14 Prozent haben noch keine konkreten Initiativen gestartet. Nur 9 Prozent haben durch KI ihr Geschäftsmodell verändert. Als grösste Hürden nennen die Befragten Datenqualität und Datensilos (20 Prozent), Sicherheits- und Datenschutzbedenken (19 Prozent) und fehlende Fachkräfte (18 Prozent). Für 51 Prozent ist es wichtig, dass Daten in der Schweiz oder der EU verarbeitet werden.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Der nächste Produktivitätsschritt entsteht weniger durch ein stärkeres Modell als durch die Anbindung von KI an CRM, Dokumentenablage, Wissensbasis und klare Prozessstandards. Ein Agent auf schlecht gepflegten Stammdaten liefert vor allem schneller falsche Ergebnisse.

Quellen: **KMU-Portal (SECO)** · **EY Schweiz**

## 04 KI-Agenten & Automatisierung

### Vom Antworten zum Ausführen: Agents API mit Computer Use und Decisions API

OpenAI hat die Agents API als Public Beta gestartet. Agenten können damit über einen von OpenAI gehosteten Browser Websites und Anwendungen wie ein Mensch bedienen, also klicken, tippen und navigieren. Dazu kommt die Decisions API für enge Entscheidungsaufgaben wie Klassifikation und Weiterleitung, die laut Decrypt in den kommenden Tagen breit verfügbar werden soll. So können Agenten Informationen aus mehreren Systemen sammeln, einen Vorgang vorbereiten und ihn zur menschlichen Genehmigung vorlegen.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Gute Pilotprozesse sind wiederkehrend, regelbasiert und messbar, etwa Angebotsvorbereitung, Rechnungsvorprüfung, Terminqualifizierung oder interne Wissenssuche. Ein sinnvoller Pilot umfasst einen Prozess, eine verantwortliche Person, ein Freigabemodell und zwei bis drei Kennzahlen, zum Beispiel Bearbeitungszeit, Fehlerquote und Durchlaufdauer.

Quellen: **InfoQ** · **Runtime Wire** · **Decrypt**

## Nvidia startet die Open Agent Safety Platform für KI-Agenten

Nvidia hat am 28. September eine Sicherheitsplattform vorgestellt, die Agenten technisch begrenzen soll. Der quelloffene Teil OpenShell führt Agenten in einer Sandbox aus und kontrolliert Dateizugriffe, Netzwerkverbindungen, Werkzeuge und Zugangsdaten über vorab definierte Regeln. Ein separater Hardware-Wächter namens Sentry greift bei Ausbruchsversuchen ein, dieser Teil läuft nur auf Nvidia-Systemen. Laut Nvidia arbeiten über 100 Organisationen mit, darunter Anthropic, SpaceXAI und JPMorganChase. Auslöser sind die Vorfälle der letzten Monate mit ausgebrochenen Agenten.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Agentensicherheit wird zum eigenen Technologiefeld. Auch kleinere Unternehmen brauchen Mindestregeln, sobald Agenten auf E-Mail, CRM, ERP oder Finanzdaten zugreifen: minimale Berechtigungen, menschliche Freigabe bei Zahlungen, Vertragsänderungen und externen Zusagen, Protokollierung jeder Aktion, Testbetrieb mit künstlichen oder stark eingeschränkten Daten sowie ein Abbruch- und Eskalationsmechanismus. Bei der Anbieterwahl prüfen Sie Berechtigungsmodell, Audit-Logs und Datenresidenz.

Quellen: **Euronews** · **drweb.de (nach Reuters)** · **Notebookcheck**

## 05 Internationale Trends

### Persönliche Agenten: Meta Muse und OpenAI Dots starten in den USA, Europa wartet

Meta hat an der Connect Ende September den persönlichen Agenten Muse in den Mittelpunkt gestellt. Er soll laufende Aufgaben wie Buchungen oder Formulare übernehmen und läuft in einer eigenen virtuellen Maschine in Metas Cloud. Muse ist derzeit in den USA und Kanada verfügbar, in Europa noch nicht. Die Einbindung in Metas KI-Brillen ist für die kommenden Monate angekündigt. OpenAI geht mit Dots in dieselbe Richtung, ebenfalls mit eingeschränkter Verfügbarkeit in Europa.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Mitarbeitende werden solche Werkzeuge wahrscheinlich privat nutzen, bevor das Unternehmen sie freigibt. Regeln für die private KI-Nutzung (Bring your own AI), Datenschutzvorgaben und eine sichere Unternehmensalternative sind deshalb jetzt sinnvoll.

Quellen: **Meta** · **all-ai.de** · **Trending Topics**

## OECD: KMU nutzen KI vor allem als Standardprodukt, die Integration bleibt ungleich

Die D4SME-Erhebung 2026 der OECD (über 2'000 KMU aus 12 OECD-Ländern, nicht repräsentative Stichprobe) bestätigt die breite Nutzung von KI-Standardanwendungen. Einzelne KMU experimentieren auch mit massgeschneiderten Lösungen bis hin zu KI-Agenten. Die strategische, gezielte und sichere Einbindung in die Geschäftsabläufe bleibt jedoch ungleich verteilt. Zeitmangel, Wartungskosten und fehlende Kompetenzen bremsen die Umsetzung, Cybersicherheit bleibt eine Herausforderung.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Die Herausforderung ist nicht allein technologisch. Kompetenzen, Prozessdesign, Datenschutz, Veränderungsmanagement und Wirtschaftlichkeit müssen gemeinsam gesteuert werden. Bitte beachten: Das Papier erschien im ersten Halbjahr 2026 und ist keine Neuigkeit dieser Woche.

Quelle: **OECD**

## 06 Handlungsempfehlung für diese Woche

**1** **KI-Inventar erstellen**

Tools, Daten, Nutzerinnen und Nutzer sowie Anwendungsfälle erfassen, inklusive privat genutzter Tools.

BASIS: MELDUNGEN 01 UND 03

**2** **Einen Prozess auswählen**

Hoher manueller Aufwand, geringes Risiko, klares und messbares Ergebnis.

BASIS: MELDUNGEN 02 UND 04

**3** **Agenten begrenzen**

Nur notwendige Zugriffe, menschliche Freigabe bei finanziell oder rechtlich relevanten Aktionen, vollständige Protokollierung.

BASIS: MELDUNG 04

**4** **Wirkung messen**

Bearbeitungszeit, Fehlerquote, Durchlaufzeit und Akzeptanz vor und nach dem Pilot vergleichen.

EINSCHÄTZUNG MINDTRAIN