MINDTRAIN · KI-WOCHENREPORT

KI-Wochenreport für KMU im DACH-Raum

Woche 45/2026 · 27. Oktober bis 2. November 2026

Sechs Themenfelder · 6 Meldungen

Mindtrain GmbH · Der KI-Mentor für KMU

mindtrain.ch

Die wichtigste Meldung der Woche kommt aus Bern: Der Bundesrat hat den Zwischenstand der KI-Regulierung zur Kenntnis genommen, die Vernehmlassung ist neu für das Frühjahr 2027 vorgesehen. Daneben zeigen Sicherheitslücken in PHP und neue Agentenplattformen, dass Kontrolle, Berechtigungen und Updates im Alltag wichtiger werden als noch autonomere Systeme. Zu jeder Meldung finden Sie die Quellen.

📈 Markt & Politik

⚙️ Tools & Tech

🏭 Branchen

🤖 Agenten

🌍 International

🎯 Empfehlung

01 Markt & Politik

Schweiz: Bundesrat nimmt Zwischenstand der KI-Regulierung zur Kenntnis, Vernehmlassung neu für Frühjahr 2027 vorgesehen

Der Bundesrat hat am 28. Oktober den Zwischenstand der KI-Regulierung zur Kenntnis genommen. Es ging nicht um einen Entscheid über neue Gesetze. Grundlage bleibt der Beschluss von Anfang 2025, die KI-Konvention des Europarats ins Schweizer Recht zu übernehmen. Die allgemeine Regulierung soll sich auf grundrechtsrelevante Bereiche wie Datenschutz, Transparenz und Nichtdiskriminierung beschränken. Weitere Anpassungen sollen möglichst sektorbezogen erfolgen. Der Zwischenstand besteht aus einem Bericht über sektorielle Massnahmen und einer Handreichung für einen KI-Kodex, einem «Werkzeugkasten» für freiwillige Massnahmen von Verbänden und Unternehmen. Das Bundesamt für Justiz arbeitet an den rechtlich verbindlichen Regeln. Für die Eröffnung der Vernehmlassung ist laut Berichten das Frühjahr 2027 vorgesehen. Wichtig: Frühere Ausgaben nannten «bis Ende 2026». Das gilt nach diesen Berichten nicht mehr.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Warten Sie nicht auf ein einzelnes KI-Gesetz. Verbindliche Regeln dauern länger als erwartet, aber die Richtung ist klar: Datenschutz, Transparenz, Nichtdiskriminierung und menschliche Aufsicht. Definieren Sie jetzt interne Leitlinien zu erlaubten Tools, Daten und Verantwortlichkeiten. Besonders betroffen sind Personalwesen, Kundensegmentierung, Kreditentscheide und Leistungsbeurteilung. Wer in die EU liefert, kann zusätzlich dem EU AI Act unterliegen. Hinweis: Die Details zum Zeitplan stammen aus Medienberichten, eine Primärquelle des Bundes konnte ich dazu nicht abrufen.

Quellen: IT Magazine · ictk.ch · ad-hoc-news (Zeitplan) · BAKOM, Übersicht KI

02 Tools & Technologien

SAP TechEd: Joule Work und Joule Studio bringen zielorientierte Agenten in SAP-Landschaften

SAP hat am 27. Oktober an der TechEd in Berlin «Joule Work» vorgestellt, eine Oberfläche, in der Nutzer ein Ziel beschreiben und KI-Agenten mehrstufige Aufgaben über SAP-Systeme hinweg ausführen. Mit «Joule Studio» erstellte Agenten laufen auf einer eigenen Runtime und erscheinen im «SAP AI Agent Hub». Beide Produkte werden schrittweise und je nach Systemlandschaft unterschiedlich verfügbar. Das «SAP Enterprise AI Gateway» für Authentifizierung, Richtlinien, Monitoring und Audit ist für das erste Quartal 2027 geplant, Preise sind nicht genannt. Der Betrieb eigener Agenten auf der Runtime ist für ausgewählte Kunden bis Dezember 2026 kostenlos.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Wer SAP einsetzt, sollte früh klären, welche Funktionen im eigenen System tatsächlich aktiv sind und was sie kosten. Die kostenlose Phase eignet sich für erste Prototypen, die Premium-Funktionen für Kontrolle sind noch nicht verfügbar. Dokumentieren Sie die Geschäftsregeln, die ein Agent einhalten muss, und testen Sie Ergebnisse gegen gesicherte Daten. Bitte beachten: Die Quelle spricht KMU nicht direkt an. Das ist eine Einschätzung von Mindtrain.

Quellen: ERP Today (SAP TechEd 2026) · CIO.com

Sicherheitsupdate: Kritische PHP-Lücken, entdeckt mit KI-Unterstützung

Am 21. Oktober hat das PHP-Projekt Sicherheitsupdates für zwei kritische Lücken veröffentlicht, mit denen Angreifer aus der Ferne Code ausführen könnten (Schweregrad 9,2 von 10). Gepatcht sind PHP 8.5.12, 8.4.27, 8.3.36 und 8.2.35. Für ältere, nicht mehr unterstützte Versionen gab es minimale Korrekturen. Laut Berichten sind alle PHP-Installationen betroffen, die Webanfragen verarbeiten. Das Sicherheitsunternehmen Calif meldete Angriffe ohne Anmeldung unter anderem bei WordPress, Drupal und Joomla. Entdeckt wurden die Lücken unabhängig von OpenAI-geführten Forschern und vom Sicherheitsunternehmen Wiz, beide mit Hilfe von KI-Modellen. Das PHP-Projekt hält Updates für die einzige sichere Lösung. Vor der Veröffentlichung kursierten Proof-of-Concepts, funktionierende Angriffe fand das PHP-Team zum Zeitpunkt der Veröffentlichung nicht.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Das ist ein konkreter Handlungspunkt: Fragen Sie Ihren Hosting-Anbieter oder Ihre IT, ob Ihre Websites, Webshops und Portale auf einer gepatchten PHP-Version laufen. Prüfen Sie dabei auch Systeme, die niemand aktiv betreut. Die Meldung zeigt ausserdem, dass KI Schwachstellen schneller findet, was für Verteidiger und Angreifer gilt. Die Meldung stammt vom 21. Oktober, also kurz vor dem Berichtszeitraum, bleibt aber aktuell.

Quellen: Unite.AI · Forklog · Let's Data Science

03 Branchen & Praxisbeispiele

Swiss AI Jobs Report: KMU treiben die Nachfrage nach KI-Fachkräften

Laut dem Swiss AI Jobs Report der Hochschule Luzern wurden zwischen Juli 2025 und Juni 2026 knapp 5000 KI-Stellen ausgeschrieben. KMU verantworteten 76 Prozent des Stellenzuwachses und machten 62 Prozent aller KI-Ausschreibungen aus. Die meisten Stellen schrieben IT-Firmen aus (1211), am stärksten wuchs der öffentliche Sektor (plus 67 Prozent). Gesucht werden vor allem erfahrene Fachleute: Senior-Stellen nahmen um 42 Prozent zu, unbefristete Junior-Stellen machten nur 5 Prozent der Inserate aus. Zur Einordnung: Keystone-SDA meldet 32 Prozent mehr Stellen als im Vorjahr. Die Netzwoche nennt als Vorjahreswert 4703 Stellen, das ergäbe nur rund 6 Prozent. Die Zahlen widersprechen sich, deshalb ist die Wachstumsrate unsicher. Gezählt werden zudem ausgeschriebene Stellen, nicht Anstellungen. Die Meldung stammt vom 8. und 9. Oktober, also vor dem Berichtszeitraum.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> KI ist kein Thema nur für Grosskonzerne mehr. Der Wettbewerb um erfahrene KI-Fachleute ist hart. Für viele KMU ist es wirtschaftlicher, bestehende Mitarbeitende gezielt weiterzubilden und externe Spezialisten projektbezogen einzusetzen. Beginnen Sie nicht mit einer isolierten Tool-Anschaffung, sondern mit einer Analyse Ihrer wichtigsten Kosten-, Qualitäts- und Engpassprozesse.

Quellen: **swissinfo (Keystone-SDA)** · **Netzwoche** · **nau.ch**

04 KI-Agenten & Automatisierung

Akamai: Agent Sandbox soll Code von KI-Agenten abschotten

Akamai hat am 27. Oktober «Akamai Inference» und die «Agent Sandbox» als Beta vorgestellt. Die Sandbox ist eine isolierte Umgebung, in der Agenten und der von ihnen geschriebene Code laufen. Sie basiert auf WebAssembly, ist Open Source und begrenzt Rechenleistung, Speicher, ausgehende Verbindungen und Systemfunktionen. Zusätzliche Kontrollen dazu, worauf Agenten zugreifen und wer sie nutzen darf, sind laut Medienmitteilung erst geplant. Preise nennt Akamai nicht. Eine vollständige Sperre ausgehender Verbindungen beschreibt die Mitteilung nicht, sondern Begrenzungen.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Isolation und begrenzte Zugriffe werden Standard bei Agentenplattformen. Fragen Sie jeden Anbieter, wo Agenten laufen, welche Verbindungen sie nach aussen aufbauen dürfen und wie Sie sie stoppen. Ein Agent, der E-Mails versenden, Bestellungen auslösen oder Kundendaten ändern darf, braucht strengere Kontrollen als ein reines Recherchewerkzeug. Beta-Produkte eignen sich für Tests, nicht für produktive Kernprozesse.

Quellen: Akamai (Medienmitteilung, 27. Oktober 2026) · Techzine

05 Internationale Trends

USA: DoorDash erhält erst «einige Hundert» Bestellungen über fremde KI-Agenten

Im Rahmen der Quartalszahlen sagte DoorDash am 30. Oktober, dass über Drittanbieter-KI-Agenten bisher nur «several hundred» Bestellungen eingegangen sind. Zum Vergleich: Das Unternehmen wickelt laut Geschäftsbericht 2025 rund 3 Millionen Lieferungen pro Tag ab. Kunden bestellen weiterhin überwiegend über die eigene App. CEO Tony Xu sagte sinngemäss, man solle sich dieser Entwicklung nicht entgegenstellen, dürfe den Stand der Technik aber auch nicht überschätzen. DoorDash betreibt eigene KI-Angebote und will mehr über agentische Anwendungsfälle lernen.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Die Meldung ist eine nützliche Gegenprobe zum Agenten-Hype: Ob Kunden über KI-Agenten bei Ihnen bestellen, ist heute eher ein Zukunftsthema. Messen Sie bei eigenen Agenten abgeschlossene Vorgänge, Wiederholung und Supportaufwand, nicht die Zahl der Integrationen. Bereiten Sie Ihr Angebot dennoch so vor, dass es maschinenlesbar und eindeutig beschrieben ist. Bitte beachten: Es handelt sich um einen einzelnen Plattformbetreiber in den USA.

Quellen: TechCrunch · The Next Web · Magica

06 Praktische Impulse für diese Woche

1 PHP-Updates prüfen lassen

Fragen Sie Ihre IT oder Ihren Hosting-Anbieter, ob alle Websites und Webanwendungen auf einer gepatchten PHP-Version laufen.

BASIS: ABSCHNITT 02

2 Internes KI-Regelwerk verabschieden

Legen Sie fest, welche Tools erlaubt sind, welche Daten hineingehören und wer verantwortlich ist, ohne auf ein Schweizer KI-Gesetz zu warten.

BASIS: ABSCHNITT 01

3 Agenten eng begrenzen

Starten Sie mit zwei bis drei Prozessen mit hohem Volumen und geringem Risiko. Zahlungen und externe Zusagen bleiben bei einer menschlichen Freigabe.

BASIS: ABSCHNITTE 02, 04 UND 05

4 KI-Kompetenz intern aufbauen

Bilden Sie bestehende Mitarbeitende gezielt weiter und planen Sie bei neuen Lösungen Datenschutz, Protokollierung, Berechtigungen und Ausstiegsszenarien von Anfang an ein.

BASIS: ABSCHNITT 03