MINDTRAIN · KI-WOCHENREPORT

KI-Wochenreport für KMU im DACH-Raum

Woche 42/2026 · 5. bis 12. Oktober 2026

Sechs Themenfelder · 8 Meldungen

Mindtrain GmbH · Der KI-Mentor für KMU

mindtrain.ch

Die wichtigste Entwicklung der Woche ist der Übergang von generativer KI zu steuerbaren KI-Agenten, die Aufgaben planen, Unternehmenssysteme nutzen und Arbeitsergebnisse selbstständig vorbereiten. Für Geschäftsleitungen steigt damit der potenzielle Nutzen, aber auch die Notwendigkeit von klaren Berechtigungen, menschlicher Kontrolle und dokumentierten Regeln. Zu jeder Meldung finden Sie die Quellen.

📈 Markt & Politik

⚙️ Tools & Tech

🏭 Branchen

🤖 Agenten

🌍 International

🎯 Empfehlung

01 Markt & Politik

Schweiz: Neue Parlamentarische Gruppe Künstliche Intelligenz gegründet

Am 5. Oktober wurde die Parlamentarische Gruppe Künstliche Intelligenz bekannt. Rund 30 National- und Ständerätinnen und -räte wollen die Schweiz als KI-Standort mit guten Rahmenbedingungen und einem verantwortungsvollen Umgang mit der Technologie stärken. Trägerorganisationen sind derzeit Salesforce und der Anwenderverband SwissAI. Der erste Anlass ist für die Wintersession 2026 vorgesehen. Zum Hintergrund: Der Bundesrat hat beauftragt, bis Ende 2026 eine Vernehmlassungsvorlage zur KI-Regulierung zu erarbeiten, und 2027 empfängt die Schweiz in Genf den internationalen KI-Gipfel.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Die Weichen für die Schweizer KI-Regeln werden in den kommenden Monaten gestellt. Bereiten Sie schon jetzt ein einfaches Governance-Modell vor: erlaubte Tools, Umgang mit vertraulichen Daten, menschliche Freigaben und Verantwortlichkeiten. Das senkt spätere Anpassungskosten und schafft Vertrauen bei Mitarbeitenden und Kunden.

Quellen: IT Reseller · PCtipp · Bundesamt für Justiz

EU: AI Office und Apply AI Strategy, Aufsicht und Förderung werden konkret

Das Europäische AI Office setzt den AI Act um und ist insbesondere für die Regeln zu KI-Modellen mit allgemeinem Verwendungszweck zuständig. Seine Durchsetzungsbefugnisse gegenüber diesen Anbietern, inklusive Bussgeldern, gelten laut Lawfare ab dem 2. August 2026. Parallel will die EU mit der im Oktober 2025 gestarteten «Apply AI Strategy» die KI-Nutzung gezielt bei KMU fördern, unter anderem über die Digital Innovation Hubs (Testmöglichkeiten, Reifegradchecks), die Initiative InvestAI und die KI-Fabriken für Rechenleistung. Zur Einordnung: Die Pflicht zur KI-Kompetenz gilt schon seit Februar 2025. Die Hochrisiko-Pflichten wurden laut IHK Nürnberg per «Digital Omnibus» auf Ende 2027 beziehungsweise Ende 2028 verschoben.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Aufsicht und Nachweispflichten werden zunehmend durch Leitfäden konkretisiert. Auch Schweizer Unternehmen können betroffen sein, wenn sie KI-Produkte in der EU anbieten oder dort einsetzen. Führen Sie deshalb eine Übersicht über alle KI-Anwendungen, Datenquellen und Entscheidungsprozesse und prüfen Sie bei Personalentscheiden, Kundenbewertung und sicherheitskritischen Prozessen, ob eine Anwendung in eine regulierte Risikokategorie fällt. Den Rechtsstand klären Sie mit Ihrer Rechtsberatung.

Quellen: EU-Kommission, AI Office · OECD.AI, Apply AI Strategy · Lawfare · IHK Nürnberg · urbanstudio

02 Tools & Technologien

Google Gemini Agent: universeller Agent für Unternehmen, zunächst als Private Preview

Google Cloud hat am 8. Oktober an der Veranstaltung «Gemini at Work 2026» einen universellen Gemini-Agenten für Unternehmen vorgestellt. Man gibt ihm ein Ziel statt einzelner Anweisungen, er plant die Arbeit, nutzt Werkzeuge und arbeitet mit Systemen wie Google Workspace, Microsoft 365, Slack, Jira, BigQuery, Snowflake und beliebigen MCP-Servern. Er wählt standardmässig das passende Modell, Nutzer können andere wählen, zunächst unter anderem Claude-Modelle von Anthropic. Zur Kostenkontrolle gibt es Ausgabenlimits, bei deren Erreichen der Agent pausiert. Verfügbar ist der Agent vorerst nur als Private Preview für Unternehmenskunden, einen öffentlichen Preis gibt es laut Berichten nicht.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Perspektivisch eignet sich ein solcher Agent für Recherche, Angebotsvorbereitung, interne Wissenssuche, Dokumentenerstellung und die Koordination wiederkehrender Abläufe. Kurzfristig planbar ist das für Schweizer KMU noch nicht: Preis und Lizenzfragen sind offen. Vor einer Einführung müssen Datenzugriffe, Rollenrechte und Freigabeschritte definiert werden.

Quellen: Unite.AI · The AI Insider · Let's Data Science (nach The Verge) · TechJack Solutions

Nous Research: «Hermes for Businesses» soll Open-Source-Agenten in Unternehmen bringen

Nous Research hat am 7. Oktober eine Finanzierungsrunde über 90 Millionen US-Dollar bestätigt. Laut Wall Street Journal liegt die Bewertung bei 1,5 Milliarden US-Dollar. Das Geld fliesst in «Hermes for Businesses», die Unternehmensversion des quelloffenen Hermes-Agenten (MIT-Lizenz, seit Februar 2026). Laut Nous können Unternehmen Modelle nach Preis und Ziel wählen, ihre KI-Nutzung privat halten und ihr Unternehmenswissen behalten. Der Agent läuft lokal oder in der Cloud. Hermes wurde laut Nous mehr als 24 Millionen Mal kopiert, das misst aber das Interesse von Entwicklern, nicht zahlende Kunden.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Interessant ist der Trend zu anpassbaren und potenziell datensouveräneren Agenten, falls Standardassistenten branchenspezifisches Wissen oder Integrationen nicht ausreichend abdecken. Belegte Unternehmenseinsätze, Preise und die technische Architektur sind noch offen: Prüfen Sie Datenflüsse und Sicherheitszusagen unabhängig, bevor Sie sich festlegen.

Quellen: The Next Web · Runtime Wire · Dealroom

03 Branchen & Praxisbeispiele

On, Shopify und PayPal testen den neuen Gemini-Agenten

Google nennt als frühe Tester des Gemini-Agenten den Schweizer Sportartikelanbieter On, der die dynamische Modellauswahl testete, Shopify, das für Millionen von Händlern Spitzenmodelle kombiniert, und PayPal, das laut Google pro Woche 10 Millionen Multi-Modell-Anfragen weiterleitet. Der Agent soll Unternehmenskontext nutzen, Aufgaben über mehrere Systeme hinweg ausführen und Ergebnisse direkt in bestehenden Arbeitsumgebungen bereitstellen.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Der praktische Nutzen entsteht durch die Verbindung von KI mit vorhandenen Systemen wie CRM, E-Mail, Projektmanagement und Wissensdatenbanken. Für kleinere Unternehmen empfiehlt sich zunächst ein begrenzter End-to-End-Prozess, zum Beispiel von der Kundenanfrage bis zur Angebotsvorbereitung. Bitte beachten: Das sind Angaben von Google zu Grossunternehmen, keine unabhängig belegten Ergebnisse.

Quellen: Unite.AI · The AI Insider

04 KI-Agenten & Automatisierung

Vertrauen in autonome Produktionsänderungen durch KI-Agenten sinkt

Laut einer VentureBeat-Umfrage vom 8. Oktober ist der Anteil der Unternehmen, die KI-Agenten Änderungen in Produktionssystemen allein auf Basis automatischer Prüfungen erlauben oder anstreben, von 75 Prozent im Juli auf 56 Prozent im August gesunken. Bei den finalen Kaufentscheidern fiel der Wert von 88 auf 61 Prozent. 27 Prozent lassen risikoarme Agenten bereits ohne menschliche Prüfung Änderungen einspielen. Gleichzeitig investieren Unternehmen weiter in Werkzeuge zur Prüfung und Überwachung von Agenten. Die Stichprobe ist klein: Es sind jeweils rund 100 Befragte, die autonome Agenten einsetzen.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Der Markt bewegt sich nicht weg von Agenten, sondern hin zu kontrollierter Autonomie. Ein «Human-in-the-loop»-Modell ist sinnvoll: Agenten dürfen vorbereiten und ausführen, aber Zahlungen, Personalentscheide und externe Zusagen benötigen zunächst eine menschliche Freigabe, dazu Protokollierung und eine Rückfallmöglichkeit.

Quellen: Crypto Briefing (nach VentureBeat) · Ecosistema Startup

Nicht-menschliche Identitäten: Agenten ohne Besitzer und Regeln sind ein Risiko

KI-Agenten greifen auf ähnliche Daten und Systeme zu wie Mitarbeitende, werden aber oft nicht mit gleichwertigen Identitäts- und Berechtigungskontrollen verwaltet. Die Cloud Security Alliance zitiert in einer Forschungsnotiz vom Juni 2026 Umfragedaten vom Januar 2026: 78 Prozent der Organisationen haben keine dokumentierte Regel, wie KI-Identitäten erstellt und entfernt werden, 51 Prozent berichten über keine klare Verantwortung für KI-Identitäten, und 16 Prozent erfassen nicht einmal, wann neue KI-Identitäten entstehen. Für KI-Agenten empfiehlt die CSA einen menschlichen Verantwortlichen, minimale Rechte, definierte Handlungsgrenzen mit Freigabeprozessen vor dem Zugriff und eine rasche Entziehung von Rechten.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Jeder Agent sollte einen eindeutigen Besitzer, ein definiertes Aufgabengebiet, minimale Systemrechte und ein Ablaufdatum für Berechtigungen haben. Eine einfache Agentenliste mit Zweck, Datenzugriff, Freigabeprozess und Protokollierung ist ein sinnvoller Start. Bitte beachten: Die Umfragen stammen überwiegend aus grösseren Unternehmen, nicht aus KMU.

Quellen: Cloud Security Alliance (Forschungsnotiz Juni 2026) · THE Journal

05 Internationale Trends

USA: Google und Microsoft verankern Identität, Protokoll und Kostenlimits direkt im Agenten

Google gibt seinem Agenten ein eigenes Workspace-Konto mit eigener E-Mail-Adresse und schreibt jede Aktion in ein Protokoll, das dem Agenten statt einer Person zugeordnet wird. Agenten laufen in einer Sandbox, der Datenverkehr führt über einen zentralen «KI-Firewall»-Gateway. Microsoft bietet mit Agent 365 seit dem 1. Mai 2026 eine zentrale Steuerungsebene: Jeder Agent erhält über Entra Agent ID eine eigene Identität und lässt sich wie ein Benutzer mit Zugriffsrichtlinien und Lebenszyklusregeln verwalten. Agenten aus AWS Bedrock und Google Cloud lassen sich inventarisieren. Laut einem Fachbericht kostet Agent 365 15 US-Dollar pro Nutzer und Monat oder ist im Paket Microsoft 365 E7 enthalten.

> **RELEVANZ FÜR DIE GESCHÄFTSLEITUNG**
>
> Eigene Identität und Protokoll pro Agent werden zum Standard. Bei der Auswahl eines Agenten zählen deshalb nicht nur Funktionsumfang und Preis, sondern auch Berechtigungsmodell, Audit-Logs, Datenresidenz und Integrationskontrollen. Wer Microsoft 365 nutzt, hat mit Agent 365 eine praktikable Verwaltungsoption. Legen Sie bei Pilotprojekten von Anfang an fest, welche Agenten auf welche Systeme zugreifen dürfen und wer ihre Aktivitäten kontrolliert.

Quellen: Unite.AI · Microsoft Learn, Entra Agent ID · Arvato Systems · ITNEXT (Preisangabe)

06 Praktische Impulse für diese Woche

1 **Drei Prozesse auswählen**

Je einen Prozess aus Vertrieb, Administration und Kundenservice, der häufig, regelbasiert und messbar ist.

BASIS: ABSCHNITTE 02 UND 03

2 **Agentenkarte erstellen**

Für jeden geplanten Agenten Zweck, Datenzugriff, erlaubte Aktionen, menschliche Freigaben und Verantwortliche dokumentieren.

BASIS: ABSCHNITTE 04 UND 05

3 **Pilot mit Kennzahlen durchführen**

Vorher-nachher-Werte für Zeitaufwand, Fehlerquote, Durchlaufzeit und Ergebnisqualität erfassen.

EINSCHÄTZUNG MINDTRAIN

4 **KI-Kompetenz organisieren**

Mitarbeitende nicht nur in der Tool-Bedienung schulen, sondern auch in Datenschutz, Quellenprüfung, Entscheidungsgrenzen und sicherem Umgang mit Unternehmensdaten.

BASIS: ABSCHNITT 01