

AI Governance

Recht, Organisation & Technologie für sichere KI

Ralf Angermann | Thomas Güntensperger | Fabienne Bouffé | Jan Niederhauser

online.ch

Donnerstag, 29. Oktober 2026

Bereit für mehr Sicherheit mit AI?

Programmpunkt	
Begrüssung & Vorstellung	Thomas «Günti» Güntensperger Client Partner
AI Governance für Frontier Firmen	Ralf Angermann Head of AI Solutions
AI Governance heisst, unternehmerische Verantwortung wahrzunehmen.	Fabienne Bouffé Head of PM & Consulting
Von der Governance zur technischen Durchsetzung	Jan Niederhauser Copilot Lead & Consultant
Q&A mit unseren Experten	Moderation: «Günti» Experten: Fabienne, Jan & Ralf

Building digital solutions people love.

Digitalisierung | Microsoft Cloud | AI Lösungen | IT-Outsourcing

Wir bauen digitale Lösungen, die Menschen lieben und dein Unternehmen noch erfolgreicher, intelligenter und effizienter machen.

30+

Neue Kunden
pro Jahr

70+

Experten

3+

Länder

Online macht Microsoft.



Copilot



Copilot Studio



Agent 365



Azure



Microsoft 365



SharePoint Online



Teams



Defender



Fabric



Power Platform



Power BI



Dynamics 365



Online macht ausgezeichnete Lösungen.



Data & AI
Azure



Digital & App Innovation
Azure



Infrastructure
Azure



Modern Work





WTT
YOUNG
LEADER
AWARD

WE
WON!

WTT YOUNG LEADER AWARD 2026

MANAGEMENTKONZEPTION



online
macht digital.

Unser AI-Ökosystem Von St.Gallen bis zum Silicon Valley

Innovation

Die Geschwindigkeit ist atemberaubend.

Qualität

Im B2B ist die Qualität entscheidend.

Partnerschaften

Um gemeinsam zu Wachsen.

Skalierbarkeit & Sicherheit

Microsoft Cloud, die führende AI-Plattform.



swiss made
software +AI



Online macht glückliche Kunden.



SWICA



BERNINA
made to create

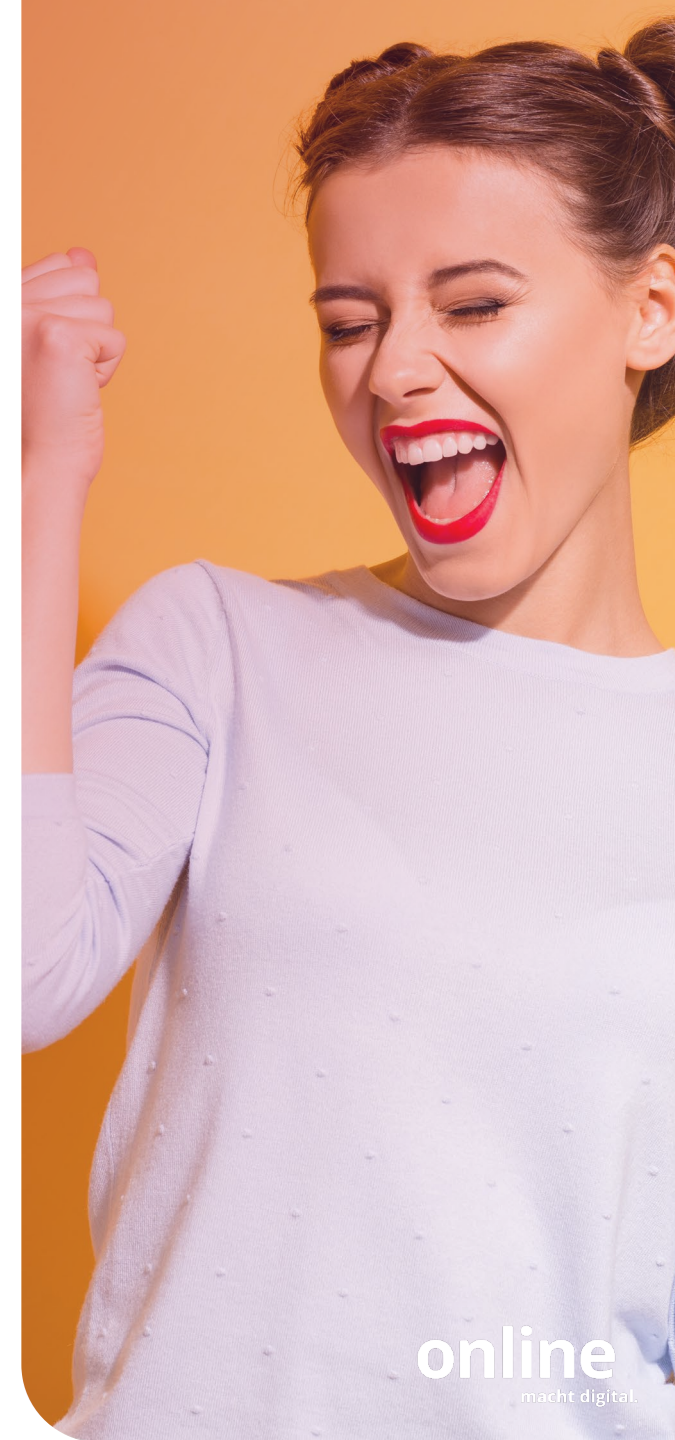
ARBONIA

Livit

Lindt
MAÎTRE CHOCOLATIER SUISSE
DEPUIS 1845

HEKS
Brot für alle.

PH^{SG}



online
macht digital.

online
macht digital.

online
macht digital.

Hier
neuste
Episode
anhören!

BELIMO[®]

Unser
Podcast
shift
Das Signal im Rauschen



Universität St.Gallen



LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN



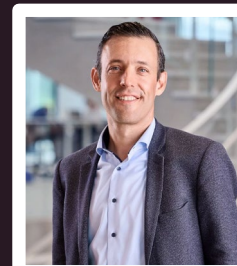
Microsoft



OST
Ostschweizer
Fachhochschule

vitra.

SWICA



Benchmark aus 500+ Firmen aus unserem AI-Readiness Check!

Wo steht dein Unternehmen 2026?

98%

der Unternehmen
schätzen AI als wichtig
für ihr Business ein.

81%

der Unternehmen
fehlt eine Liste von
priorisierten
Prozessen mit AI
Potenzial.

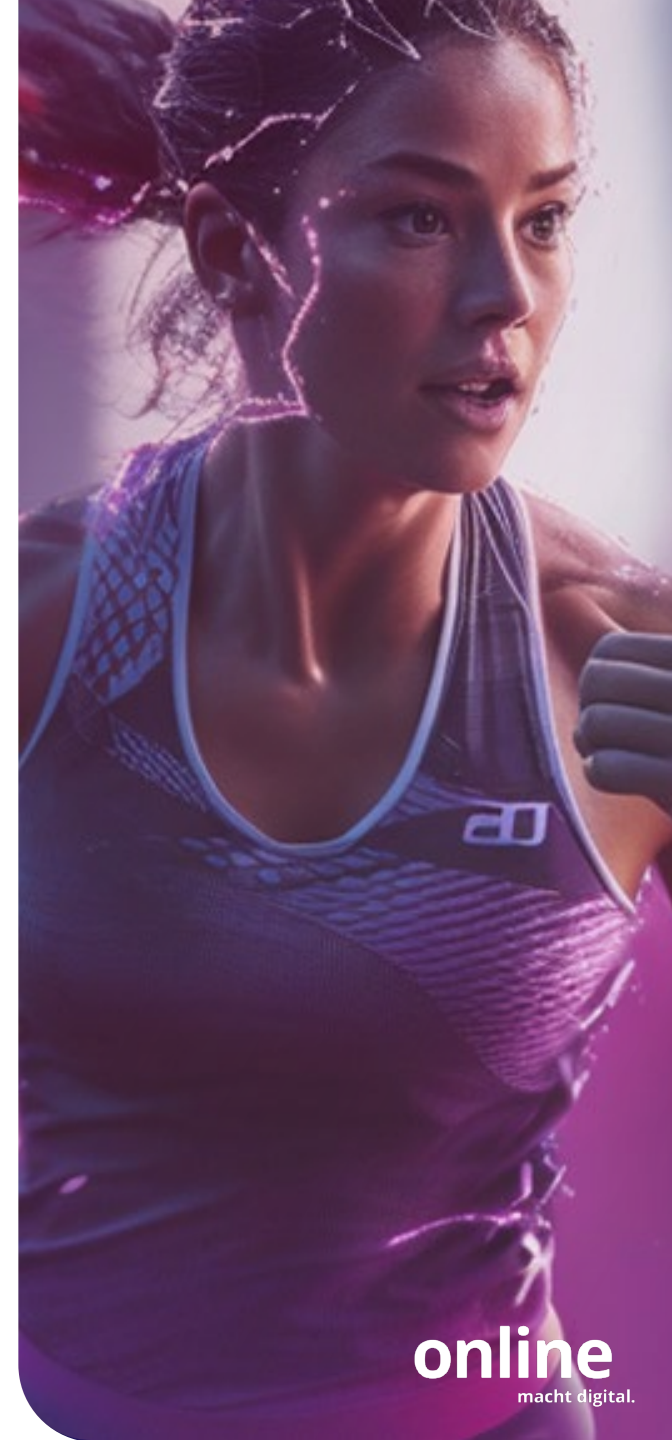
84%

der Unternehmen
beurteilen den
Ausbildungsstand der
Mitarbeitenden in
Bezug auf AI als
ungenügend.

Klick hier...

✓ Bestimme selbst die AI-Readiness deines Unternehmens!

Klick!



#HappyToConnect



Thomas Güntensperger

Client Partner

+41 71 913 31 71

thomas.guentensperger@online.ch



Vernetze dich mit mir auf LinkedIn.



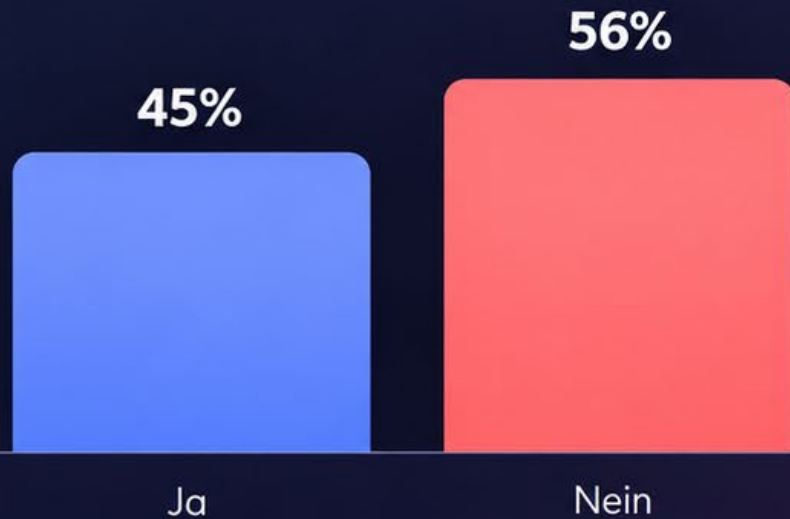
AI Governance für Frontier Firmen

Ralf Angermann | Head of AI Solutions

Resultate der Live-Umfrage

Ein Blick auf den aktuellen Stand

Wer benutzt für berufliche Zwecke
private KI Tools?



Hat dein Unternehmen eine
AI Governance / AI Policy?



AI Nutzung der Mitarbeiter

Shadow AI

75%

der Wissensmitarbeiter
in einem Unternehmen
nutzen bereits AI.

78%

Der AI-Nutzenden
bringen eigene AI-Tools
ins Unternehmen
(Schatten-AI).



1'300'000'000

Durch Governance zur Frontier Firm!

Die AI-Transformation jeder Organisation sieht unterschiedlich aus, die Governance muss diese Entwicklung absichern.

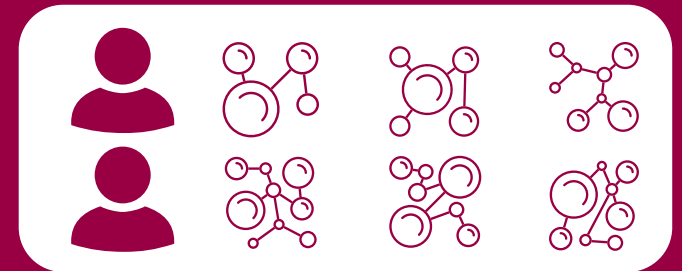
Phase 1 *Mensch mit Assistent*



Phase 2 Mensch - Agent - Teams



Phase 3 Mensch führt, Agenten führen aus



Zwei Ebenen

Menschen regeln, Technik setzt durch

MENSCH UND ORGANISATION

Ethik und Umgang

**Strategie
Schulung
Standards**

 **Microsoft** Teilweise im Produkt eingebaut

TECHNIK

Durchsetzen und kontrollieren

**Berechtigungen,
Kosten, Missbrauch**

Berechtigungen · Kosten · Missbrauch



Admin Center



Entra



Purview



Defender



Agent 365

Die Organisation legt fest, was richtig ist. Die Technik sorgt dafür, dass es eingehalten wird.

#HappyToConnect



Ralf Angermann

Head of AI Solutions

+41 71 913 31 61

ralf.angermann@online.ch



Vernetze dich mit mir auf LinkedIn.

Klick!

AI Governance heisst, unternehmerische Verantwortung wahrzunehmen.

Fabienne Bouffé | Head of PM & Consulting

AI verändert Unternehmensrisiken

AI verbessert nicht nur Produktivität, sondern beschleunigt auch die Sichtbarkeit bestehender Schwachstellen.

Risiken

- ✓ **Fehlentscheidungen auf falscher Grundlage**
- ✓ **Diskriminierung von Personen(-gruppen)**
- ✓ **Entscheidungen und Grenzen bleiben unverständlich**
- ✓ **Keine klare Verantwortung für Wirkung und Schaden**
- ✓ **Datenlecks und unerlaubte Zugriffe gefährden Vertrauen.**

Steuerung

- ✓ **Zuverlässigkeit**
- ✓ **Fairness**
- ✓ **Erklärbarkeit**
- ✓ **Rechenschaft**
- ✓ **Datenschutz**

AI Standards

Rechtliche Grundlagen



Schweiz

- ✓ DSG
- ✓ OR, UWG, URG, PrHG
ggf. Branchenvorgaben
usw.



Europäische Union

- ✓ EU AI Act (EU)
- ✓ DSGVO (EU)



International

- ✓ OECD AI Principles (+ 38 Länder)
- ✓ ISO/IEC 42001 (Global)
- ✓ NIST AI Risk Management (USA)

**Nicht der Firmensitz entscheidet,
welche Regeln gelten,
sondern wo und wie die AI
eingesetzt wird.**

Anwendbarkeit ist fallabhängig –
früh rechtlich abklären.

**Schweizer Recht ist die Basis.
Internationale Frameworks liefern
Werkzeugkasten für verantwortungsvolle
Umsetzung.**

AI Governance Operating Model

01 People

- ✓ Rollen
- ✓ Skills
- ✓ AI Literacy

02 Process

- ✓ Intake
- ✓ Bewertung
- ✓ Freigabe

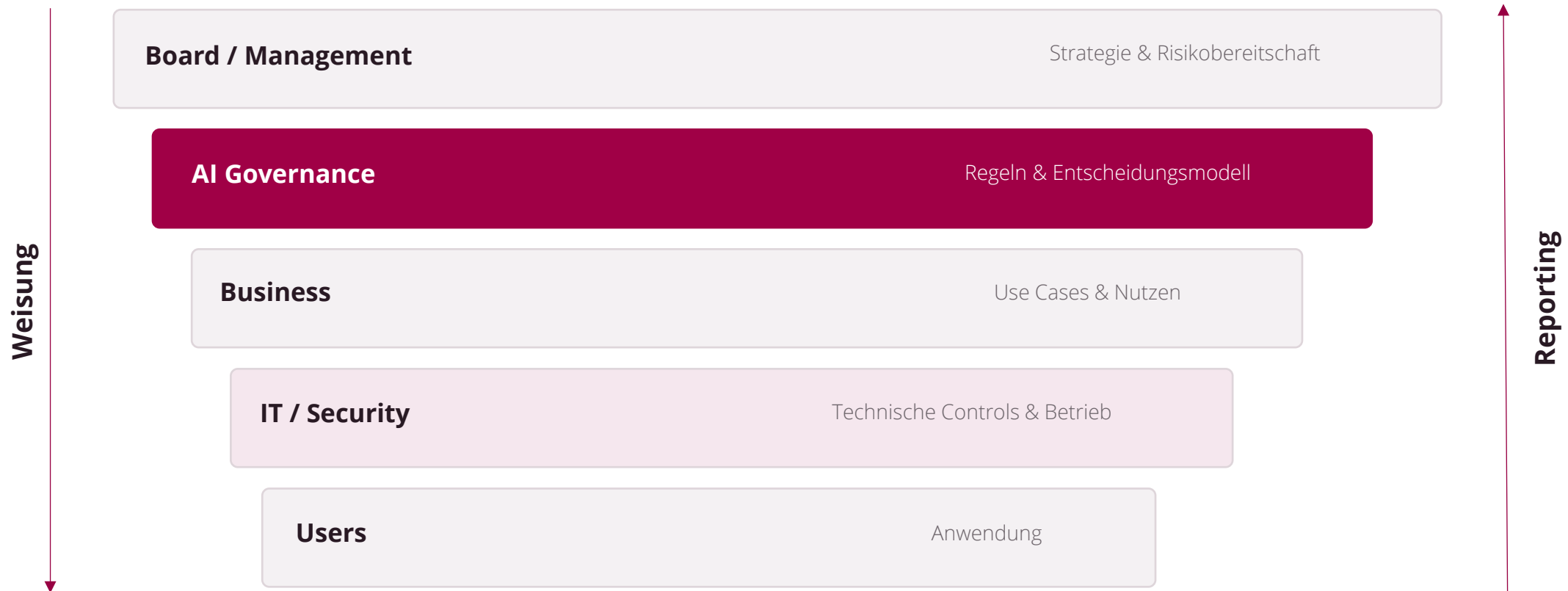
03 Policy

- ✓ Zulässige
Nutzung
- ✓ Standards

04 Technology

- ✓ Identity
- ✓ Data
- ✓ Security
- ✓ Monitoring

Wer trägt die Verantwortung für AI Einsatz?



PROFESSIONAL ATHLETES



AI TRANSFORMATION IN THE CORPORATE WORLD



That one
training day



Perform



Train

AI Literacy

Kompetenz als Teil der Governance

1

Alle Mitarbeitenden

Grundlagen & Policy

- ✓ Wie KI funktioniert – und wo ihre Grenzen liegen
- ✓ Erlaubte Tools und Umgang mit sensiblen Daten
- ✓ Ergebnisse kritisch prüfen, Fehler melden

2

Power User

Praxis im Arbeitsalltag

- ✓ Prompting und Use Cases am eigenen Prozess
- ✓ Copilot und Agenten sicher einsetzen
- ✓ AI Champions als Multiplikatoren im Team

3

Management & Business Owner

Steuerung & Verantwortung

- ✓ Risiken einstufen, Freigaben verantworten
- ✓ Pflichten und Rechte kennen
- ✓ Menschliche Aufsicht und Monitoring sichern

EU AI Act, Art. 4:

Anbieter und Betreiber von KI-Systemen müssen Massnahmen ergreifen, um die AI Literacy ihres Personals zu fördern – seit 2. Februar 2025, präzisiert durch den Digital Omnibus 2026. Relevant für Schweizer Firmen mit EU-Bezug.

5 Schritte zu einer funktionierenden AI Governance

Governance ist ein kontinuierlicher Lifecycle.



Gute AI Governance verhindert KI nicht.
Sie schafft den Rahmen, in dem Unternehmen KI sicher skalieren können.

Faustregel

AI Use Cases für Business

1

PERSONENDATEN?

Schweizer DSG direkt anwenden. Zweck, Transparenz, Datenminimierung, Sicherheit und Betroffenenrechte prüfen. Bei hohem Risiko: Datenschutz-Folgenabschätzung.

2

MENSCHEN BETROFFEN?

Entscheidet oder bewertet AI über Personen? Menschliche Prüfung, Nachvollziehbarkeit, Fairness und Anfechtbarkeit vorsehen.

3

ARBEITSPLATZ?

HR, Recruiting, Leistung oder Überwachung besonders kritisch prüfen. Verhaltensüberwachung von Mitarbeitenden ist unzulässig.

4

EU-BEZUG?

Bei EU-Markt, EU-Nutzung oder Wirkung in der EU die Anwendbarkeit und Rolle nach EU AI Act sowie gegebenenfalls DSGVO separat klären.

5

SENSITIVER SEKTOR?

Gesundheit, Finance, Versicherung, Behörden, Bildung oder kritische Infrastruktur: zusätzliche Fachgesetze und Aufsichtsvorgaben prüfen.

6

INHALTE & DRITTE?

Urheberrechte, Geschäftsgeheimnisse, Verträge, Lizenzen, Datenquellen und Anbieterbedingungen vor Input, Training und Publikation klären.

Faustregel: Kein Go-live ohne Owner, dokumentierten Zweck, Datenfreigabe, Risikoeinstufung, menschliche Kontrolle und Monitoring.

Von Governance Policies zu **technischen Controls**

Abstrakte Anforderungen werden erst durch klare technische Kontrollen und Nachweise operativ.

GOVERNANCE FRAGE

Wer darf Copilot nutzen?

Auf welche Informationen darf Copilot zugreifen?

Welche Daten sind sensitiv?

Wie verhindern wir Datenabfluss?

Wie sehen wir, was mit AI passiert?

Wie steuern wir Agents?



TECHNISCHE UMSETZUNG

Entra ID · Groups · Licensing · Conditional Access

M365 Permissions · SharePoint · OneDrive

Purview Sensitivity Labels · Encryption

Data Loss Prevention (Purview, PP Admin)

Audit · DSPM for AI (Purview)

M365 Admin · Copilot Studio · Power Platform Admin Center · Azure / Foundry

#HappyToConnect



Fabienne Bouffé

Head of PM & Consulting

+41 71 913 31 57

fabienne.bouffe@online.ch



Vernetze dich mit mir auf LinkedIn.

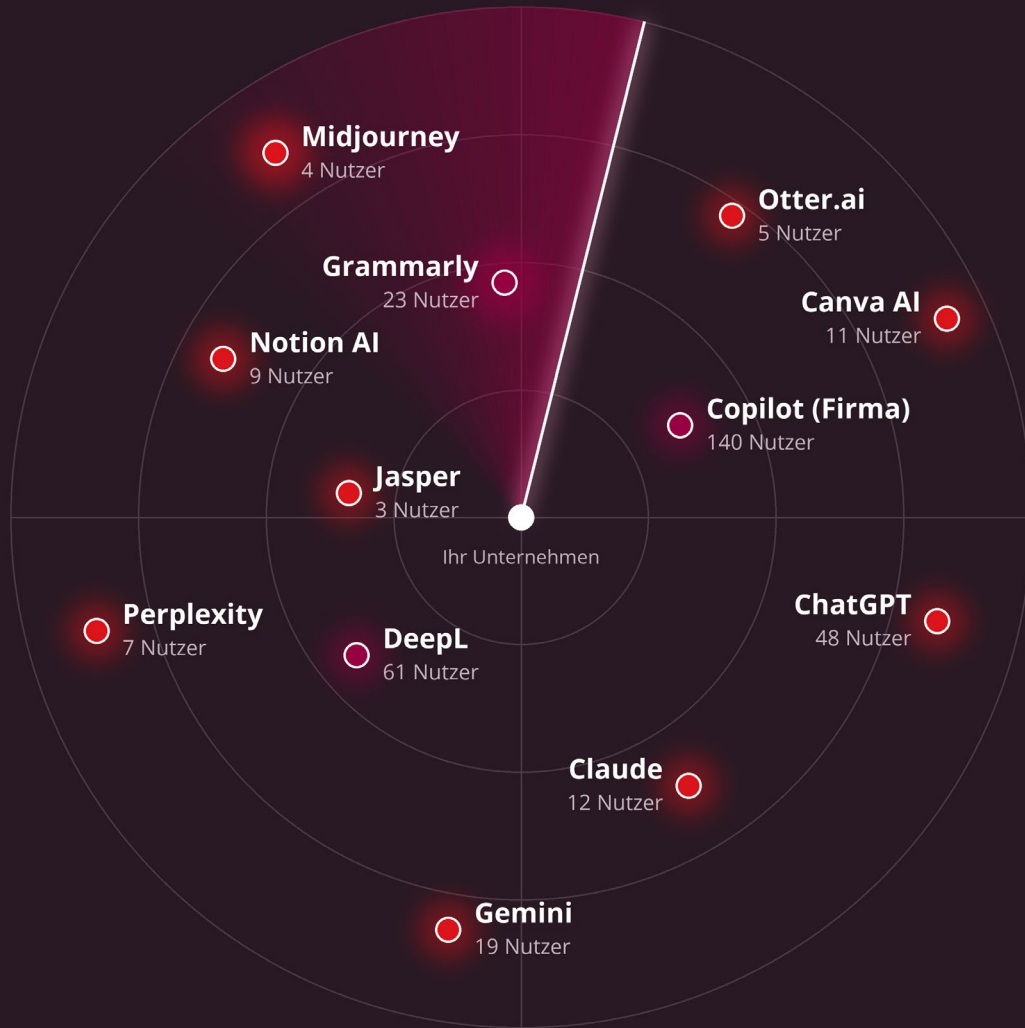
Klick!

Von der Governance zur technischen Realisierung

Jan Niederhauser | Copilot Lead & Consultant

1'300'000'000

Wege schliessen – und bessere öffnen.



Wer nur verbietet, verschiebt die KI ins Private.
Wer nur öffnet, verliert den Überblick.

12

KI-Apps entdeckt

9

davon mit privaten Konten

Privates Konto: Daten fließen ab

Freigegeben oder unkritisch

SCHLIESSEN

Sichtbar machen, private Konten sperren.

ÖFFNEN

Bessere Alternativen im Unternehmen anbieten.

Kontrolle heisst nicht Verbot.

Kontrolle heisst: wissen, wohin die Daten fließen.

Governance, Compliance, Security.

Drei Disziplinen, die oft vermischt werden – und nur zusammen wirken.

GOVERNANCE

Wer entscheidet?

Regeln, Rollen, Verantwortung: Wer darf Agenten bauen, nutzen und teilen? Wer ist Owner, wer trägt die Kosten?



Admin Center



Agent 365



Power Platform

COMPLIANCE

Können wir es belegen?

Regeln einhalten und nachweisen: Aufbewahrung, Audit und eDiscovery – für DSG, EU AI Act und Branchenvorgaben.



Purview

SECURITY

Sind wir geschützt?

Identitäten, Geräte und Daten gegen Angriffe, Missbrauch und Abfluss schützen.



Entra



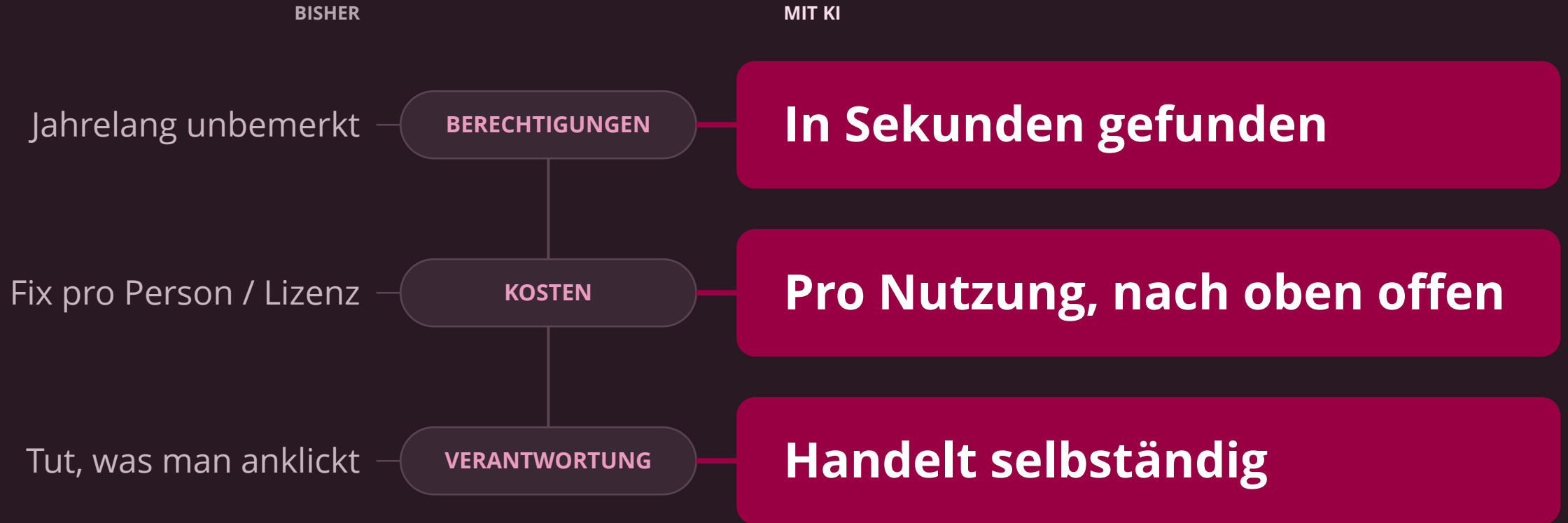
Defender



Intune

Governance legt fest, wer was darf. Compliance belegt es, Security setzt es durch.

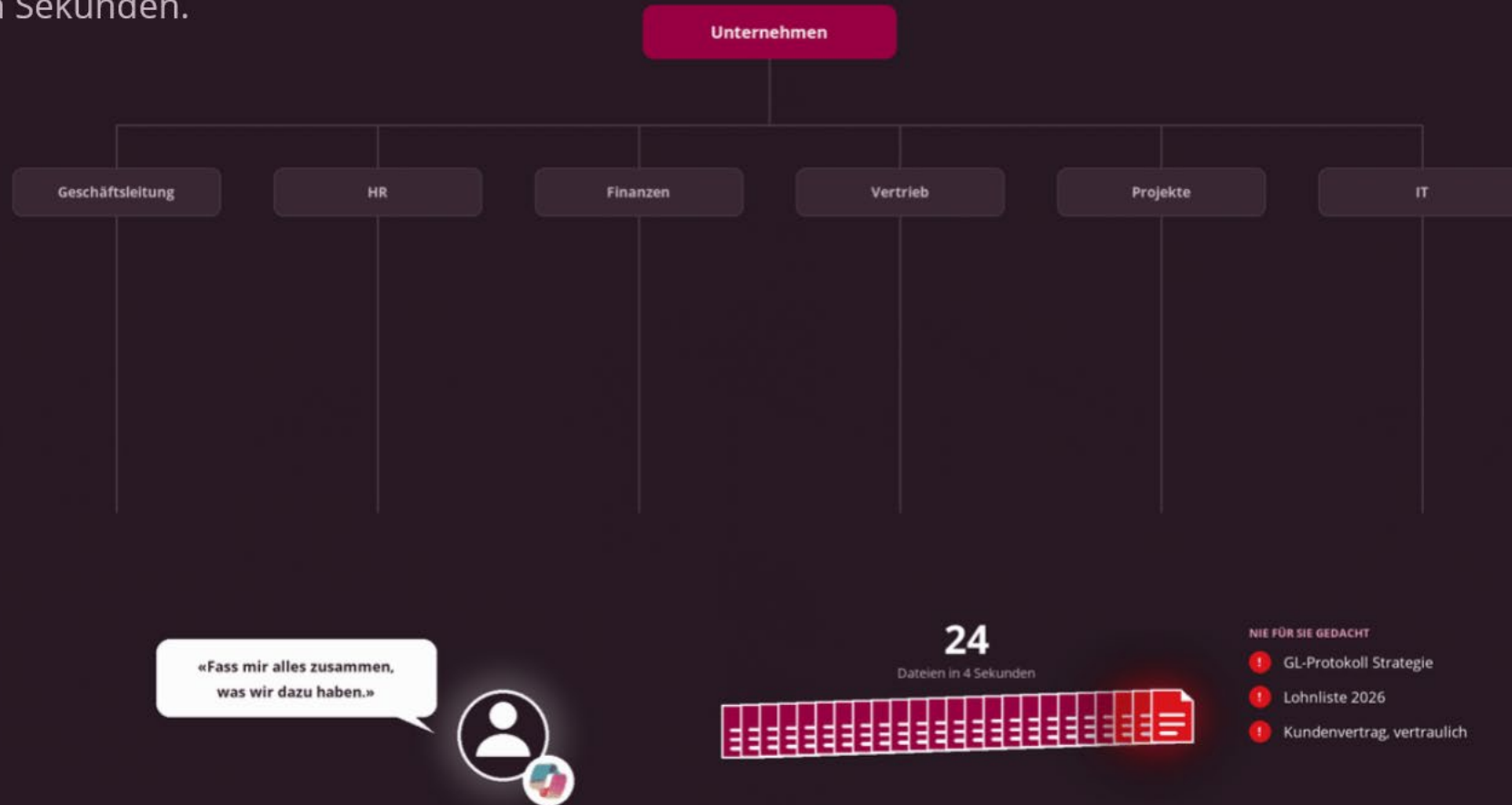
AI-Governance ist Microsoft-365-Governance.



KI verstärkt den Effekt: Was liegen blieb, rückt jetzt in den Fokus.

Ein Agent sieht, was sein Benutzer sehen darf.

Oversharing in Sekunden.



Wer Berechtigungen und Labels im Griff hat, hat auch die Agenten im Griff.

Wo was verwaltet wird.

Jede Plattform hat ihr eigenes Admin Center. Identität, Daten und Sicherheit laufen über alle hinweg.

PRO PLATTFORM

ÜBER ALLE PLATTFORMEN

 MICROSOFT 365 Endanwender	 Copilot	 Cowork	 Agent Builder	 SharePoint	 Microsoft 365 Admin Center
 POWER PLATFORM Power User	 Copilot Studio	 Power Automate	 AI Builder	 Dataverse	 Power Platform Admin Center
 AZURE Entwickler	 Foundry	 Agent Service	 GitHub Copilot		 Azure-Portal

 Agent 365 Register und Überblick über alle Agenten	GOVERNANCE
 Entra Admin Center Identität und Zugriff für Menschen und Agenten	SECURITY
 Purview-Portal Labels, DLP, Audit und Aufbewahrung	COMPLIANCE
 Defender-Portal Bedrohungen und Schatten-KI erkennen	SECURITY

Gebaut wird in drei Welten. Gesteuert, geschützt und belegt wird über alle hinweg.

Technische KI-Governance für Agenten (Agent 365)

Agenten verwalten wie Mitarbeitende.

Microsoft erweitert die Werkzeuge, die heute Benutzer schützen, auf Agenten.



Agent 365



ÜBERWACHEN · ADMIN CENTER

Jeder Agent im Register

Agent map, Besitzer, Nutzung und Risiken auf einen Blick.



STEUERN · ENTRA UND PURVIEW

Identität und Daten im Griff

Eigene Identität für Agenten, Labels und DLP gelten auch für sie.



SCHÜTZEN · DEFENDER

Angriffe erkennen

Bedrohungsschutz und Schatten-KI-Erkennung auf den Geräten.



Allgemein verfügbar seit 1. Mai 2026 · einzeln oder als Teil von Microsoft 365 E7

AI-Ökosystem in Microsoft.



Microsoft 365
Admin Center

1

Agent map

395 Agents in einer Demo-Umgebung

2

Drittanbieter

326 davon nicht von Microsoft

3

Alle Agenten

Status, Besitzer, Nutzung

4

Schatten-KI

Lokale KI-Apps wie Claude oder ChatGPT

5

Einstellungen

Wer darf nutzen, teilen, freigeben

Was inklusive ist – und was Agent 365 (E7) dazu bringt.

Das Inventar gibt es mit jeder Lizenz. Sehen und absichern, was Agenten tun, kostet extra.



IN JEDER MICROSOFT-365-LIZENZ

Agenten verwalten

- ✓ Register aller Agenten mit Export
- ✓ Agenten ohne Besitzer erkennen
- ✓ Freigeben, blockieren, Besitzer wechseln
- ✓ Regeln für den Lebenszyklus
- ✓ Eigene Identität für Agenten (Entra Agent ID)



MIT AGENT 365 ODER E7

Sehen und absichern, was Agenten tun



Risiko, Nutzung und Laufzeitdaten jedes Agenten



Conditional Access und Lebenszyklus mit Sponsor



DLP, Labels und Insider Risk auch für Agenten



Angriffe erkennen, verdächtige Tool-Aufrufe blockieren



Festlegen, welche Tools und MCP-Server erlaubt sind

MICROSOFT 365 E7

das Bündel



E5

+



Copilot

+



Agent 365

+



Entra Suite

KMU BIS 300 PERSONEN

Business Premium + Copilot + Agent 365

Lizenziert pro Person, nicht pro Agent · Voraussetzung: E5 bzw. Business Premium · Stand Oktober 2026

Token-Kosten im Griff

(AI Governance – FinOps)

1 Credit $\approx$ 0.65 Rappen.



knapp ein Rappen

SO VIEL BRAUCHT EINE ABFRAGE

Einfache Antwort

Eine kurze Frage an einen Agenten

ab 1 Credit

unter 1 Rappen

Antwort mit Firmendaten

Der Agent durchsucht Dateien und Mails

rund 10 Credits

$\approx$ 7 Rappen

Ganzer Auftrag

Cowork erledigt mehrere Schritte selbst

100–1'500 Credits

65 Rp. bis CHF 10

Microsoft vereinfacht: eine Währung für alle Agenten. Mehr Arbeit, mehr Credits.

Chat ist inklusive. Agenten kosten nach Verbrauch.

COPILOT



Copilot Chat +

Fragen, schreiben,
zusammenfassen

In der Lizenz

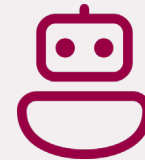
fix pro Person und Monat

AGENTEN VON MICROSOFT



Cowork

Erledigt ganze Aufträge im
Auftrag einer Person



BALD

Autopilot

Arbeitet selbständig im
Hintergrund



Eigene Agenten

Von Ihrem Unternehmen
gebaut, z. B. in Copilot Studio

+ Credits nach Verbrauch

bezahlt wird pro Abfrage und Auftrag

Die Lizenz ist planbar. Der Verbrauch braucht ein Budget.

Drei Ebenen, drei Einstellungen.



Oben das Gesamtbudget, unten die Limits. Warnung bei 80 %, Stopp bei 100 %.

Wichtig für die Geschäftsleitung

Erwünscht, geprüft, verboten.

Drei Listen, die die Geschäftsleitung festlegt – die IT setzt sie technisch um.



ERWÜNSCHT

Fördern und befähigen

- › Copilot im Arbeitsalltag für alle
- › Persönliche Agenten für die eigene Arbeit
- › Freigegebene Agenten aus dem Store
- › Use Cases mit messbarem Nutzen



Lizenz, Schulung, Agent Builder freischalten



SICHTBAR UND GEPRÜFT

Erst prüfen, dann freigeben

- › Agenten, die geteilt werden
- › Agenten mit Firmendaten oder Aktionen
- › Externe Tools und MCP-Server
- › Agenten, die Credits verbrauchen



Freigabe, Owner, Register, Kosten-Limit



VERBOTEN

Technisch sperren

- › Kundendaten in privaten KI-Konten
- › Agenten ohne Owner
- › Automatische Entscheide über Personen
- › Nicht freigegebene Apps



DLP, Konnektor-Regeln, Apps blockieren

Was verboten ist, braucht eine Alternative. Je klarer die drei Listen, desto weniger Schatten-KI.

Drei Fragen für die nächste GL-Sitzung.

1

Wer darf bei uns Agenten bauen und teilen?

Benutzerzugriff, Teilen, Maker-Rollen

2

Wer ist Owner für KI-Kosten – und wo liegt das Limit?

Budget pro Person, Limit pro Agent

3

Wissen wir, welche Agenten und KI-Apps heute schon laufen?

Agent 365, Schatten-KI, Netzwerk

Governance bremst nicht. Sie ist die Voraussetzung, dass KI skalieren darf.

#HappyToConnect



Jan Niederhauser

Copilot Lead & Consultant

+41 71 913 31 73

jan.niederhauser@online.ch



Vernetze dich mit mir auf LinkedIn.



AI Nutzung der Mitarbeiter

Shadow AI

75%

der Wissensmitarbeiter
in einem Unternehmen
nutzen bereits AI.

78%

Der AI-Nutzenden
bringen eigene AI-Tools
ins Unternehmen
(Schatten-AI).



Wrap-up

5 Key Learnings

AI Governance wird wirksam, wenn Verantwortung, Risiko und technische Umsetzung durchgängig verbunden sind.

- 1 FÜHRUNGSAUFGABE** AI Governance ist keine reine IT-Aufgabe. Management definiert Risk Appetite, zulässige Nutzung und Verantwortlichkeiten.
- 2 USE CASE ZUERST** Nicht das Tool, sondern Zweck, Daten, betroffene Personen und Wirkung bestimmen Risiko und Regulierung.
- 3 RECHT & FRAMEWORK** DSGVO und gegebenenfalls EU AI Act setzen den Rahmen. NIST, OECD und ISO/IEC 42001 helfen bei der Operationalisierung.
- 4 POLICY → CONTROL** Entra, M365 Permissions, Purview, Power Platform und Copilot Control System übersetzen Regeln in technische Controls und Evidenz.
- 5 LIFECYCLE STATT PROJEKT** Discover, Assess, Govern, Protect und Monitor müssen kontinuierlich betrieben und verbessert werden.

Gute Governance bremst AI nicht. Sie macht sichere Skalierung möglich.

AI kontrolliert einführen

Online (AI) Governance Service

Microsoft-365-Standards dauerhaft im Blick behalten.

Standards etablieren

- ✓ Wie KI funktioniert – und wo ihre Grenzen liegen
- ✓ Erlaubte Tools und Umgang mit sensiblen Daten
- ✓ Ergebnisse kritisch prüfen, Fehler melden

Abweichungen steuern

- ✓ Vereinbarte Konfigurationen überwachen und priorisieren
- ✓ Erkannte Schatten-KI-Nutzung einordnen
- ✓ Änderungen kontrolliert nach Freigabe umsetzen

Nachweise liefern

- ✓ Status, Änderungen und offene Massnahmen berichten
- ✓ Regelmässiges Review
- ✓ Klare nächste Schritte

Weniger manuelle Kontrollen. Klare Verantwortung. Nachvollziehbare Entscheidungen.



Microsoft
Intune



Microsoft
Defender



Microsoft
Entra ID



Microsoft
Purview



Microsoft
Teams



Microsoft
Exchange



Microsoft
SharePoint



Microsoft
OneDrive



Microsoft
Copilot

Next Webinars

Up to date im Bereich AI!

«Microsoft Ignite 2026: Die wichtigsten AI-News aus San Francisco»

 Donnerstag, 3. Dezember 2026

 11:00 Uhr

 Online & kostenlos

Klick hier...

- ✓ ...um dich für die kommenden Webinar anzumelden!
- ✓ ...um alle Aufzeichnungen der vergangenen Webinare anzuschauen!

Klick!

ONLINE GROUP × east#KI

8 TICKETS. 8 CHANCEN.

Sei am east#KI dabei!

11. November 2026 | St. Gallen

Melde dich bis 4. November für unser Dezember-Webinar an und sichere dir die Chance auf eines von 8 Tickets.

JETZT ANMELDEN & MITMACHEN

Klick!

Mehr
Infos
zum
Event!



Wert pro Ticket: CHF 25.- | Auslosung: 5. November 2026

online
macht digital.

Must-Have LinkedIn Newsletter **Shift – Das Signal im Rauschen**



NEWSLETTER

shift – Das Signal im Rauschen

Orientierung für Entscheider im Zeitalter von AI und Digitalisierung.



Von Balz Zürrer
Ich unterstütze Führungskräfte dabei, KI in

Klick!

Erscheint: 14-täglich
1.114 Abonnenten

Klick hier...

✓ ...um den Newsletter zu abonnieren – Stay up to date!





Danke für eure Aufmerksamkeit!
Q&A mit unseren Experten



Folge uns auf LinkedIn

Online macht dir Kaffee.

Du bist jederzeit herzlich willkommen.

Hauptsitz Schweiz

Online Consulting AG

Weststrasse 38

CH - 9500 Wil

+41 71 913 31 31

info@online.ch

Office Zürich

Online Consulting AG

Richtistrasse 2

CH - 8304 Wallisellen

+41 44 291 67 00

info@online.ch

Deutschland

Online P4I GmbH

Otto-Lilienthal-Strasse 5

DE - 71034 Böblingen

+49 7031 2070910

info@online.ch

Polen

Online Solutions Sp. z o.o.

Grodzka 9

PL - 50-137 Wrocław

+48 71 727 50 20

info@onlinesolutions.pl



Folge uns auf LinkedIn.