

# Copilot-Rollout ohne böse Überraschungen

Welche 7 Entscheidungen Sie dringend treffen müssen

## Executive Decision Paper

Für Geschäftsleitung, CIO, CISO, CFO und  
Datenschutzverantwortliche

Jetzt lesen

CONSULTICS

Partner für Microsoft Dynamics 365 · Odoo · Power Platform

Kunden u. a.:



# Executive Summary

Microsoft 365 Copilot wird häufig als Produktivitätswerkzeug vermarktet. In vielen Unternehmen beginnt die Diskussion deshalb bei der Lizenz und endet bei der Frage, wie viele Mitarbeitende Zugriff erhalten sollen. Diese Sichtweise greift jedoch zu kurz.

Tatsächlich verändert Copilot die Art und Weise, wie Unternehmenswissen gefunden, verknüpft und genutzt wird. Gleichzeitig entstehen neue Anforderungen an Berechtigungen, Datenqualität, Governance, Budgetplanung und Datenschutz. Die Einführung von Copilot ist deshalb keine einfache Softwarebeschaffung, sondern ein strategisches Transformationsprojekt.

Für Schweizer Unternehmen kommen zusätzliche regulatorische Fragestellungen hinzu. Das neue Datenschutzgesetz, Dokumentationspflichten, Datenschutz-Folgenabschätzungen und Transfer-Impact-Assessments müssen ebenso berücksichtigt werden wie technische Sicherheitskonzepte und organisatorische Governance-Massnahmen.

Dieses Whitepaper zeigt sieben Entscheidungsfragen, die vor einem produktiven Rollout beantwortet werden sollten. Ziel ist nicht, eine vollständige Implementierungsanleitung zu ersetzen, sondern eine belastbare Entscheidungsgrundlage für Management, IT, Security, Datenschutz und Fachbereiche zu schaffen.

## Kernthese

Copilot ist kein reines Lizenzthema. Copilot ist ein Governance-, Compliance- und Betriebsmodell für Unternehmenswissen und KI-gestützte Prozesse.

# Inhalt

01

Verstehen wir überhaupt, welchen Copilot wir einsetzen?

02

Was kostet Copilot wirklich?

03

Ist unser Unternehmen auf die Agent Economy vorbereitet?

04

Haben wir ein Copilot-Problem – oder ein Berechtigungsproblem?

05

Sind wir datenschutzrechtlich vorbereitet?

06

Welche Daten sollen Copilot überhaupt sehen dürfen?

07

Wie sieht ein realistischer Einführungsfahrplan aus?

08

Executive Readiness Check

09

Fazit und nächster Schritt

## ENTSCHEIDUNGSFRAGE 1

# Verstehen wir überhaupt, welchen Copilot wir einsetzen?

Die erste Fehleinschätzung vieler Unternehmen besteht darin, alle Copilot-Produkte als identisch zu betrachten. In der Praxis unterscheiden sich die Einsatzszenarien deutlich: persönliche Assistenz, abgesicherter Chat, Agentenautomatisierung und tiefere Integration in Geschäftsprozesse folgen jeweils anderen Kosten-, Sicherheits- und Governance-Regeln.



Microsoft 365 Copilot ist in erster Linie der persönliche KI-Assistent in den Microsoft-365-Anwendungen. Er wird dort relevant, wo Mitarbeitende vorhandene Informationen aus Outlook, Teams, Word, Excel, PowerPoint, SharePoint und anderen Microsoft-365-Diensten produktiver nutzen sollen. Copilot Chat dagegen adressiert abgesicherte KI-Nutzung ohne denselben Bezug zu Unternehmensdaten. Copilot Studio und Agenten erweitern das Modell um Prozessautomatisierung und teilweise eigenständig arbeitende Workflows.

Die strategische Frage lautet deshalb nicht: Kaufen wir Copilot? Die bessere Frage lautet: Welche Art von KI-Fähigkeit wollen wir organisatorisch zulassen und operativ beherrschen?

## Management-Implikation

Wer Copilot als ein einzelnes Produkt betrachtet, unterschätzt die Governance-Auswirkungen. Entscheidend ist die klare Trennung zwischen persönlicher Assistenz, Unternehmensdaten-Grounding und autonomen Agentenprozessen.

## Orientierungsmodell

| Baustein                 | Typischer Nutzen                                  | Governance-Frage                                                           |
|--------------------------|---------------------------------------------------|----------------------------------------------------------------------------|
| Microsoft 365 Copilot    | Produktivität in M365-Apps und Wissensarbeit      | Welche Unternehmensdaten darf Copilot auf Basis vorhandener Rechte nutzen? |
| Copilot Chat             | Abgesicherter KI-Chat für allgemeine Aufgaben     | Welche Daten dürfen Mitarbeitende in Prompts einbringen?                   |
| Copilot Studio & Agenten | Automatisierte Workflows und Prozessunterstützung | Wer genehmigt, überwacht und budgetiert Agenten?                           |

## ENTSCHEIDUNGSFRAGE 2

# Was kostet Copilot wirklich?

Eine der häufigsten Überraschungen in Copilot-Projekten betrifft die tatsächlichen Kosten. Viele Business Cases berücksichtigen lediglich die Benutzerlizenz. Dadurch entsteht ein verzerrtes Bild der späteren Gesamtinvestition.

Die betriebswirtschaftliche Betrachtung muss breiter erfolgen. Ein belastbarer Business Case berücksichtigt mindestens vier Kostenblöcke: Benutzerlizenzen, verbrauchsabhängige Agentenkosten, Data Readiness und Governance sowie Change Management und Adoption.

Gerade die indirekten Kosten sind entscheidend. Bereinigungen von SharePoint-Strukturen, Rechte- und Rollenüberprüfungen, Sensitivity Labels, Purview-Konfigurationen, Governance Frameworks und Nutzerschulungen entstehen unabhängig von der eigentlichen Lizenz. Werden diese Aufwände nicht eingeplant, wirkt der Business Case im Vorfeld attraktiver, als er im Betrieb tatsächlich ist.

## Budgetfrage für den CFO

Nicht: Was kostet die Lizenz pro Nutzer? Sondern: Was kostet ein produktiver, sicherer und prüfbarer Copilot-Betrieb inklusive Governance, Adoption und möglicher Agentenverbräuche?

## True-Cost-Perspektive

- Base License
- PAYG Autonomous Credits
- Data Readiness & Governance
- Change Management & Adoption

## ENTSCHEIDUNGSFRAGE 3

# Ist unser Unternehmen auf die Agent Economy vorbereitet?

Die nächste Evolutionsstufe von Copilot sind autonome oder teilautonome Agenten. Während Mitarbeitende heute KI aktiv in einer Anwendung nutzen, können Agenten künftig Aufgaben im Hintergrund vorbereiten, anstossen oder ausführen.



Typische Szenarien sind Lead-Qualifizierung, CRM-Aktualisierungen, automatische Antwortentwürfe, Dokumentengenerierung, Datenabgleiche oder Prozessauslösungen. Damit verschiebt sich das Betriebsmodell: Nicht mehr nur die Anzahl lizenzierter Nutzer bestimmt die Kosten, sondern auch die Anzahl und Art der Agenteninteraktionen.

Für Entscheider ist dieser Punkt besonders relevant, weil Agenten Kosten verursachen können, ohne dass ein Mensch jede einzelne Aktion bewusst auslöst. Unternehmen brauchen daher klare Regeln für Agentendesign, Freigabe, Monitoring, Budgetierung und Lifecycle Management.

## Governance-Frage für CIO und CFO

Wer darf Agenten erstellen, veröffentlichen und mit produktiven Daten verbinden? Und wer überwacht deren Verbrauch, Nutzen und Risiken im laufenden Betrieb?

### ENTSCHEIDUNGSFRAGE 4

# Haben wir ein Copilot-Problem – oder ein Berechtigungsproblem?

Eine der wichtigsten Erkenntnisse aus erfolgreichen Copilot-Projekten lautet: Copilot macht in der Regel keine Daten sichtbar, die nicht bereits sichtbar sind. Das Risiko liegt häufig darin, dass bestehende Berechtigungen historisch zu breit vergeben wurden.



Viele Unternehmen verfügen über gewachsene SharePoint-Strukturen, offene Team Sites, alte Projektbereiche, unkontrollierte Gastzugriffe, vererbte Berechtigungen und Gruppen, die nie konsequent bereinigt wurden. Vor Copilot waren diese Informationen zwar technisch zugänglich, praktisch jedoch schwer auffindbar.

Mit Microsoft Graph und KI-gestützter Zusammenfassung verändert sich diese Situation. Informationen, die bisher nur mit hohem Suchaufwand auffindbar waren, können nun schneller gefunden, kombiniert und in einen verständlichen Kontext gebracht werden. Das ist produktivitätssteigernd – aber nur dann sicher, wenn das Berechtigungskonzept sauber ist.

### Security-Kernaussage

Copilot erzeugt selten das Berechtigungsproblem. Copilot macht vorhandene Berechtigungsprobleme sichtbar, skalierbar und geschäftskritisch.



## ENTSCHEIDUNGSFRAGE 5

# Sind wir datenschutzrechtlich vorbereitet?

Für Schweizer Unternehmen ist die Einführung von Microsoft 365 Copilot auch eine Datenschutz- und Nachweisfrage. Relevante Stichworte sind nDSG, DSGVO-Bezugspunkte, Data Protection Addendum, Standardvertragsklauseln, Swiss Addendum, EU Data Boundary, Datenschutz-Folgenabschätzung und Transfer Impact Assessment.



Die entscheidende Managementfrage lautet nicht allein, ob Microsoft die notwendigen vertraglichen und technischen Grundlagen bereitstellt. Entscheidend ist, ob das eigene Unternehmen die rechtmässige Nutzung nachweisen, dokumentieren und organisatorisch kontrollieren kann.

Dazu gehören ein aktuelles Verzeichnis der Verarbeitungstätigkeiten, eine Bewertung der Datenflüsse, eine dokumentierte Risikobetrachtung, technische und organisatorische Massnahmen sowie klare Zuständigkeiten innerhalb von IT, Legal, Datenschutz und Fachbereich.

## DPO-Perspektive

Die Compliance-Verantwortung verbleibt beim Unternehmen. Copilot-Readiness bedeutet deshalb auch: Nachweisdokumentation, Risikobetrachtung und Verantwortlichkeiten müssen vor dem Rollout geklärt sein.

## ENTSCHEIDUNGSFRAGE 6

# Welche Daten sollen Copilot überhaupt sehen dürfen?

Sobald Unternehmen produktive KI einsetzen, wird Datenklassifikation zur strategischen Kernaufgabe. Nicht alle Informationen sollen gleich behandelt werden. Öffentliche Marketinginhalte, interne Projektdaten, vertrauliche HR-Informationen und streng vertrauliche Geschäftsleitungsunterlagen benötigen unterschiedliche Schutz- und Nutzungskonzepte.

Ein praxistaugliches Modell arbeitet mit klaren Sensitivity Labels wie Öffentlich, Intern, Vertraulich und Streng vertraulich. Diese Labels bilden die Grundlage für Verschlüsselung, Data Loss Prevention, Zugriffskontrolle, Auditierbarkeit und automatisierte Richtlinien.

Besonders wichtig ist das Spannungsverhältnis zwischen Schutz und Nutzbarkeit. Sehr starke Schutzmechanismen wie Double Key Encryption können sinnvoll sein, können aber bestimmte Cloud-Funktionen und damit auch KI-Nutzung einschränken. Unternehmen müssen deshalb bewusst entscheiden, welche Daten für Copilot nutzbar sein sollen und welche nicht.

## Architekturentscheidung

Maximaler Datenschutz und maximale KI-Nutzbarkeit sind nicht in jedem Fall gleichzeitig erreichbar. Die saubere Datenklassifikation entscheidet über beide Ziele.

## ENTSCHEIDUNGSFRAGE 7

# Wie sieht ein realistischer Einführungsfahrplan aus?

Die erfolgreichsten Copilot-Projekte starten nicht mit einem flächendeckenden Rollout, sondern mit einer Governance-Strategie und einem kontrollierten Pilotbetrieb. Ziel ist es, Risiken sichtbar zu machen, Nutzenszenarien zu validieren und ein wiederholbares Betriebsmodell aufzubauen.

Ein realistischer Einführungsfahrplan besteht aus fünf Phasen: Strategie und Data Readiness, gezielter Pilot, technische Härtung, Adoption und Qualifizierung sowie Skalierung mit kontinuierlichem PAYG- und Governance-Monitoring.

Die Phasen sollten nicht als theoretisches Projektmodell verstanden werden, sondern als Risikoreduktion. Jede Phase klärt eine zentrale Voraussetzung, bevor die nächste Ausbaustufe beginnt.

## Fünf Phasen bis zur kontrollierten Skalierung

| Phase | Fokus                      | Ergebnis                                                 |
|-------|----------------------------|----------------------------------------------------------|
| 1     | Strategie & Data Readiness | Zielbild, Governance, Daten- und Berechtigungsanalyse    |
| 2     | Gezielter Pilot            | Validierte Use Cases mit ausgewählten Key Usern          |
| 3     | Technische Härtung         | MFA, Conditional Access, Audit, Purview und Labels       |
| 4     | Adoption & Qualifizierung  | Schulung, Prompt-Kompetenz und Nutzungsrichtlinien       |
| 5     | Skalierung & Monitoring    | Kontrollierter Ausbau mit Kosten- und Agentenüberwachung |

# Executive Readiness Check

Bevor Microsoft 365 Copilot produktiv eingeführt wird, sollten die folgenden Fragen mit Ja beantwortet oder zumindest mit einer klaren Massnahmenplanung hinterlegt sein.

| Bereich     | Prüffrage                                                                                                 |
|-------------|-----------------------------------------------------------------------------------------------------------|
| Governance  | Ist eine klare KI-Strategie mit Verantwortlichkeiten, Entscheidungswegen und Eskalationsmodell vorhanden? |
| Governance  | Gibt es ein Gremium oder Board, das Copilot- und Agentenentscheidungen steuert?                           |
| Security    | Wurde ein Berechtigungs-Audit für SharePoint, Teams, OneDrive und Gruppen durchgeführt?                   |
| Security    | Sind Gastzugriffe, vererbte Rechte und alte Projektbereiche überprüft?                                    |
| Security    | Sind MFA, Conditional Access und Privileged Identity Management eingerichtet?                             |
| Datenschutz | Wurde eine Datenschutz-Folgenabschätzung für Copilot durchgeführt oder geplant?                           |
| Datenschutz | Ist ein Transfer Impact Assessment dokumentiert?                                                          |
| Datenschutz | Ist das Verzeichnis der Verarbeitungstätigkeiten für relevante Dienste aktualisiert?                      |
| Daten       | Sind Datenbestände bereinigt, archiviert oder klassifiziert?                                              |
| Daten       | Sind Sensitivity Labels und DLP-Richtlinien definiert?                                                    |
| Betrieb     | Gibt es ein Budgetmodell für Lizenzen, Agentenverbrauch, Governance und Adoption?                         |
| Betrieb     | Sind Monitoring, Nutzungsanalyse und regelmässige Governance Reviews geplant?                             |

# Fazit

Microsoft 365 Copilot ist keine reine Produktivitätslösung. Es handelt sich um eine neue Betriebsplattform für Wissen, Entscheidungen und Prozesse.

Unternehmen, die sich ausschliesslich auf Lizenzen konzentrieren, unterschätzen häufig die Bedeutung von Datenqualität, Berechtigungen, Governance und Compliance. Organisationen, die dagegen frühzeitig in Data Readiness, Datenschutz, Sicherheitsarchitektur und Adoption investieren, schaffen die Grundlage für nachhaltigen Nutzen.

Der richtige Einstieg ist daher nicht der maximale Rollout, sondern ein kontrolliertes Readiness Assessment. Es schafft Transparenz über Risiken, Kosten, Voraussetzungen und priorisierte Umsetzungsschritte.

## Nächster Schritt

Consultics unterstützt Schweizer Unternehmen bei der strategischen Einführung von Microsoft 365 Copilot, Copilot Studio und AI-Agenten – von Compliance- und Governance-Bewertung über technische Vorbereitung bis hin zu Adoption und Skalierung.



**Martin Jäger, Co-CEO**

✉ [martin.jaeger@consultics.ch](mailto:martin.jaeger@consultics.ch)

☎ +41 71 560 56 10

🌐 [consultics.ch](https://consultics.ch)

**Kostenloses Kennenlernen vereinbaren →**

# Redaktioneller Hinweis

Preis- und Lizenzinformationen zu Microsoft 365 Copilot, Copilot Studio und Copilot Credits können sich ändern. Für finale kommerzielle Aussagen sollten vor Veröffentlichung die aktuellen Microsoft-Preis- und Lizenzierungsseiten geprüft werden.

Das Dokument ersetzt keine Rechtsberatung. Datenschutz- und Compliance-Bewertungen sollten durch die zuständigen Datenschutz-, Rechts- und Sicherheitsverantwortlichen geprüft und dokumentiert werden.



Elggerstrasse 4 · 8356 Ettenhausen

+41 71 560 56 10 · [info@consultics.ch](mailto:info@consultics.ch) · [consultics.ch](https://consultics.ch)

Wir. Schaffen. Partnerschaft.