Factbook

KI-Weltreise – Staffel 7

Mit dem Beifahrer: Ein Roadtrip vom Valley zum Yukon

Inhalt

1) Copilot-Landkarte: Welche „Copilots“ meint Microsoft eigentlich? 2
A) Microsoft 365 Copilot (M365 Copilot) 2
B) Copilot Studio (Agenten bauen) 2
C) Security Copilot 2
D) GitHub Copilot 2
2) Preis-Snapshot DE/AT (Stand: Quellenlage, Listenpreise, ohne Rabatte) 2
2.1 Microsoft 365 Copilot (Enterprise / add-on) 2
2.2 Microsoft 365 Copilot Business (SMB bis 300 User) 2
2.3 Copilot Studio (Agenten/Custom) 3
2.4 Security Copilot 3
2.5 GitHub Copilot (Org/Enterprise) 3
3) Copilot-Services & „Derivate“: Was gehört in ein fundiertes Portfolio-Board? 3
3.1 Copilot Chat (Entra-ID, „Basis-Chat“) 3
3.2 Microsoft 365 Copilot (in Apps) 3
3.3 Copilot Studio (Agentic Layer) 4
3.4 Security Copilot 4
3.5 GitHub Copilot 4
4) DSGVO: die echten Hebel (nicht die Folklore) 4
4.1 Was Microsoft explizit zusagt (für M365 Copilot) 4
4.2 Die DSGVO-Risikostellen sind meist „hausgemacht“ 4
5) EU AI Act: Relevanz für Copilot in Unternehmen (DE/AT) 5
5.1 Timeline (für Planung) 5
6) Factbook: Buzzwords aus der Staffel 7 — klar & verwendbar erklärt 5
7) Kompakter Entscheidungsrahmen (DE/AT) 7

IDEE, TEXT, KONZEPT & LERNAUFBEREITUNG: BIRGIT POHN & ROBERT HORTSCHITZ;
OPTIMIERT UND UNTERSTÜTZT MIT DEN KI SYSTEMEN CHATGPT,COPILOT, GEMINI,
MISTRAL, NOTEBOOKLM; EINE PRODUKTION DER MOGI BUSINESS CREATION COMANY
GMBH & STRO GMBH;

1) Copilot-Landkarte: Welche „Copilots“ meint Microsoft eigentlich?

Microsoft verwendet „Copilot“ inzwischen als **Markendach** für mehrere Produktfamilien. Für Unternehmen sind diese vier Klassen entscheidend:

A) Microsoft 365 Copilot (M365 Copilot)

Der „Beifahrer im Büroauto“: Copilot **in Word/Excel/PowerPoint/Outlook/Teams** + Zugriff auf M365-Kontext über **Microsoft Graph** (Berechtigungen beachten!). Funktionsumfang variiert je Tenant/Release, aber das ist der Kern.

Wichtig: Es gibt auch **Copilot Chat** für Entra-ID-User, der (je nach Lizenz/Markt) ohne Zusatzkosten verfügbar sein kann, und ab 2025/2026 teilweise tiefer in Apps ausgerollt wird.

B) Copilot Studio (Agenten bauen)

Die „Werkbank“: Eigene **Agenten/Chatbots/Workflows** erstellen, Kanäle anbinden, Aktionen ausführen. Abrechnung über **Credits / Kapazität / Pay-as-you-go** (Azure).

C) Security Copilot

Der „Beifahrer für SOC/SecOps“: Hilfe bei Incident Response, Hunting, KQL, Zusammenfassungen — abgerechnet als **Security Compute Units (SCU) pro Stunde**.

D) GitHub Copilot

Der „Beifahrer im Code-Auto“: IDE-Autovervollständigung + Chat + (je nach Plan) Org-Features. Preise typischerweise **pro Seat/Monat**.

2) Preis-Snapshot DE/AT (Stand: Quellenlage, Listenpreise, ohne Rabatte)

Hinweis zur Seriosität: Microsoft-Preise hängen in DE/AT oft an **CSP/EA**, Laufzeit (monatlich/jährlich), Steuer, Bundle (z. B. „No Teams“), Promotions. Ich gebe daher **belegte Referenzpreise** + wo nötig **Spannen/Varianten**.

2.1 Microsoft 365 Copilot (Enterprise / add-on)

- In Microsofts DE-Preisseiten wird für den Copilot-Add-on u. a. ein Wert von **26,00 € pro Benutzer/Monat (jährliche Abrechnung)** angezeigt (zzgl. MwSt.).
- International wird oft die **$30/User/Monat**-Größe genannt (z. B. als Base-Preis in Analysen/News), aber für **DE/AT** ist die **€-Angabe** aus der Microsoft-DE-Seite die belastbarere Referenz.

2.2 Microsoft 365 Copilot Business (SMB bis 300 User)

- Microsoft zeigt für „Copilot Business“-Angebote im DE-Umfeld **Preispunkte im Bereich ~17–26 € pro User/Monat** je nach Bundle/Promo (Beispielseite mit „Originally … 26,20 €, now … 17,21 €“, jährliche Abrechnung; Marktverfügbarkeit kann variieren).
- Ein österreichischer Reseller/Marketplace führt **~20,69 € pro User/Monat** (zzgl. MwSt.) als Referenz.

➡️ **Praktisch:** Rechne in DE/AT realistisch mit **~20–30 € p. P./Monat** Listenpreis-Region, je nach Plan/Vertrag.

2.3 Copilot Studio (Agenten/Custom)

- Häufig zitierter Listenpreis: **$200 pro Tenant/Monat für 25.000 Messages** (klassische Message Packs) – das wird in Fachbeiträgen/Community-Dokumentation konsistent beschrieben.
- Zusätzlich/alternativ: **Pay-as-you-go** über Azure, Verbrauchseinheit „Credits", abhängig von Agent-Typ, Quellen, Komplexität.
  ➡️ Für DE/AT: kaufmännisch am besten als **OPEX-Baustein** (Grundpaket + variable Nutzung) modellieren, nicht als „fixe Userlizenz".

2.4 Security Copilot

- Microsoft listet **Provisioned 1 SCU/Hour = $4** und **Overage 1 SCU/Hour = $6**.
  ➡️ In € wird das über Azure-Billing/FX laufen; **Kostenhebel ist die 24/7-Provisionierung**, nicht der Prompt.

2.5 GitHub Copilot (Org/Enterprise)

- GitHub Docs nennen **Copilot Business: $19/Seat/Monat**, **Copilot Enterprise: $39/Seat/Monat**.
- Azure-Preisseite (DE) bestätigt die $-Größenordnung ebenfalls.
  ➡️ Für DE/AT: meist USD-Billing, je nach Einkaufskanal. Für Budgetierung: **Seat-basiert + ggf. Premium-Requests** (je nach Plan) einkalkulieren.

3) Copilot-Services & „Derivate": Was gehört in ein fundiertes Portfolio-Board?

3.1 Copilot Chat (Entra-ID, „Basis-Chat")

- Für viele Entra-ID-User ohne Zusatzkosten möglich (je nach M365-Abo), mit Option auf Agenten über Azure.
  Use Case: Richtlinienfragen, Zusammenfassen (mit Upload-Limitations), Ideation — aber ohne tiefen M365-App-Copilot-Komfort.

3.2 Microsoft 365 Copilot (in Apps)

Use Cases (harte Business-Nüsse):

- Meeting-Recaps + Action Items (Teams)
- Word: Draft → Redline → Stil
- Excel: Analyse/Erklärungen (Achtung: Review nötig)
- PowerPoint: Storylining aus vorhandenen Artefakten

Technischer Kern: Graph-Grounding + Zugriff nur innerhalb bestehender Berechtigungen.

3.3 Copilot Studio (Agentic Layer)

Use Cases:

- HR-Agent („Urlaub, Policies, Onboarding“)
- IT-Agent („Wie beantrage ich…“, „Ticket anlegen“)
- Sales-Agent (Angebotsunterlagen + CRM-Zusammenzug)

Kosten-/Risiko-Kern: Nachrichten/Credits + Datenquellen + Konnektoren + Governance.

3.4 Security Copilot

Use Cases: Incident Summaries, guided investigations, KQL-Assist, alert triage.
Kosten-/Betriebs-Kern: SCU-Kapazität + 24/7 vs. on-demand.

3.5 GitHub Copilot

Use Cases: Code-Completion, Test-Generierung, Refactoring-Assist, Repo-Q&A (je nach Plan).
Governance: Seat-Zuweisung, Policy (z. B. bestimmte Repos/Dateitypen), Logging.

4) DSGVO: die echten Hebel (nicht die Folklore)

4.1 Was Microsoft explizit zusagt (für M365 Copilot)

- **Prompts/Responses und Graph-Daten werden nicht zum Training von Foundation Models genutzt.**
- **EU Data Boundary:** Für EU-Kunden wird M365 Copilot als EU-Data-Boundary-Service beschrieben.
- Microsoft kündigt zudem **in-country processing** für Copilot-Interaktionen für mehr Länder an (Sovereignty-Ausbau).

4.2 Die DSGVO-Risikostellen sind meist „hausgemacht“

Die häufigsten realen Probleme sind nicht „KI böse“, sondern:

1. **Oversharing durch Berechtigungswildwuchs** (SharePoint/Teams „jeder sieht alles“) → Copilot findet’s schneller.
2. **DPIA/Datenschutz-Folgenabschätzung** nicht aktualisiert (M365-DPIA ohne Copilot-Szenarien).
3. **Aufbewahrung/Retention/eDiscovery** nicht sauber → Prompts/Outputs werden zu „neuen Datenobjekten“.
4. **Sensitive Data** ohne Purview-Labels/DLP → Copilot kann’s trotzdem verarbeiten, wenn Zugriff da ist.

Eine gute, praxisnahe juristische Einschätzung betont genau diese Punkte (Berechtigungen feinjustieren, DPIA prüfen/ergänzen, Schulung).

Kurzformel: *Copilot ist ein Verstärker. Er verstärkt Ordnung — oder Chaos.*

5) EU AI Act: Relevanz für Copilot in Unternehmen (DE/AT)

5.1 Timeline (für Planung)

Die EU-Parlamentsdarstellung fasst das Prinzip gut: **voll anwendbar 24 Monate nach Inkrafttreten**, mit früheren Stufen (z. B. Verbote früher).
Das Inkrafttreten wird breit mit **1. August 2024** angegeben.

5.2 Was ist für euch als „Deployer“ typisch relevant?

Copilot selbst ist ein Tool — AI-Act-Pflichten entstehen je nach **Einsatzkontext**:

- **Transparenzpflichten**: Wenn Inhalte KI-generiert sind und im Außenkontakt stehen → Kennzeichnung/Policy.
- **High-Risk-Nähe**: Wenn ihr Copilot/Agenten in HR-Selektion, Kreditwürdigkeit, sicherheitskritischen Prozessen etc. nutzt, seid ihr schnell in „hohem Risiko“ (dann: Dokumentation, Risiko-Mgmt, Human Oversight, Logging).
- **GPAI/General-Purpose-AI**: Anbieterpflichten liegen primär bei Microsoft/Modellanbietern, aber ihr braucht **Governance**, damit Nutzung nicht in verbotene/risikoreiche Bereiche kippt.

Pragmatische AI-Act-Checkliste für Copilot-Rollouts

1. Use-Case-Katalog + Risikoklassierung (low/medium/high)
2. Human-in-the-loop Regeln (wo Review Pflicht ist)
3. Nachvollziehbarkeit: Logging, Versions-/Prompt-Guidelines, Output-Archivierung wo nötig
4. Schulung: „Hände am Lenkrad“ (Halluzinationen, Quellenpflicht, Datenklassifikation)

6) Factbook: Buzzwords aus der Staffel 7 — klar & verwendbar erklärt

Kernbegriffe (Roadtrip-Kapitel-fähig)

Microsoft Graph
API-/Datenebene, die M365-Signale (Mail, Kalender, Files, Chats) verbindet. Copilot nutzt Graph-Kontext für „arbeitsplatznahe“ Antworten.

Grounding
„Erdung“ der Antwort durch Unternehmensdaten (z. B. SharePoint-Dokumente) statt rein generativ.

Semantic Index / Kontextindex
Index, der Inhalte so aufbereitet, dass Copilot sie schneller/treffsicherer referenzieren kann (praktisch: Relevanzranking).

Halluzination
Modell liefert plausibel klingenden, aber falschen Output. Gegenmittel: Review-Pflichten, Quellen/Artefakte anfordern, Aufgaben so formulieren, dass Copilot *prüfbar* arbeitet.

Human Oversight (Hände am Lenkrad)
Organisatorische/technische Maßnahmen, die sicherstellen, dass Menschen kritische Entscheidungen prüfen/steuern.

Oversharing
Berechtigungen zu breit → Copilot präsentiert Informationen legal aus Sicht der ACLs, aber illegal aus Sicht von „Need-to-know". Klassiker bei SharePoint/Teams.

DLP (Data Loss Prevention)
Regeln, die verhindern, dass sensible Daten geteilt/ausgeleitet werden (z. B. Kreditkartennummern, Personalakten).

Sensitivity Labels / Purview
Klassifikation + Schutz (Verschlüsselung, Wasserzeichen, Zugriff). Zentral, weil Copilot mit „was du sehen darfst" arbeitet.

DPIA (Datenschutz-Folgenabschätzung)
Für Copilot/Agenten oft nötig oder zumindest DPIA-Update sinnvoll, weil neue Verarbeitungsszenarien entstehen.

EU Data Boundary
Microsoft-Programm/Service-Zusage, Datenverarbeitung stärker in der EU zu halten; für M365 Copilot explizit erwähnt.

Commercial / Enterprise Data Protection
„Deine Daten trainieren nicht das Modell" + Compliance-Kontrollen (je nach Angebot).

Agentic & Automatisierung

Agent / KI-Agent
System, das nicht nur antwortet, sondern Aktionen ausführt (Tickets anlegen, Workflows starten) — typischerweise über Copilot Studio.

Tool Use / Actions
Der Agent ruft definierte Tools/APIs auf (z. B. CRM, ITSM). Governance-Pflicht: welche Tools, welche Rechte.

Orchestrierung
Steuerung mehrerer Schritte/Tools in einer Aufgabe („Plan → Execute → Verify").

RAG (Retrieval-Augmented Generation)
Abruf passender Dokumente + Generierung einer Antwort daraus (Grounding-Methode).

Security & Betrieb

SCU (Security Compute Unit)
Abrechnungseinheit für Security Copilot (provisioned/overage pro Stunde).

SOC (Security Operations Center)
Team/Prozess für Security-Monitoring & Incident Handling; Security Copilot zielt darauf.

KQL
Kusto Query Language (Microsoft-Ökosystem) für Log-/Security-Abfragen (Sentinel/Defender-Umfeld).

Wirtschaftlichkeit

ROI (Return on Investment)
Bei Copilot selten „E-Mail 2 Minuten schneller", eher: **komplexe Wissensarbeit** (Analyse, Konsolidierung, Angebots-/Projektarbeit). (Das ist genau eure Yukon-Goldnugget-Logik.)

TCO (Total Cost of Ownership)
Lizenz + Einführung (Change/Training) + Security/Compliance-Nacharbeit + Support.

Adoption
Ob Mitarbeitende Copilot sinnvoll nutzen *können* (Prompting, Review, Policies). Ohne Adoption wird Copilot in der Praxis teuer und unerquicklich.

7) Kompakter Entscheidungsrahmen (DE/AT)

Wenn du das Factbook als „Roadtrip-Checkliste" nutzen willst, funktioniert diese Reihenfolge extrem gut:

1. **Berechtigungen & Datenhygiene** (SharePoint/Teams) → Oversharing-Risiko runter
2. **Use-Cases auswählen** (5–10 mit messbaren Outputs)
3. **Pilotgruppe + Schulung** (Adoption)
4. **DPIA/Policies** (DSGVO) + Transparenzregeln (AI-Act readiness)
5. **Skalieren** (Lizenzen breit) erst wenn 1–4 stabil laufen

ALLE PREISANGABEN UND FUNKTIONSBESCHREIBUNGEN ZU DEN SERVICES WURDEN GEWISSENHAFT ONLINE BEIM HERSTELLER RECHERCHIERT UND ENTSPRECHEN DEM STAND FÜR ÖSTERREICH UND DEUTSCHLAND VOM JÄNNER 2026, ABWEICHUNGEN SIND UNBEABSICHTIGT UND MÜSSEN VOM LESER EVALUIERT WERDEN.