

CHECKLISTE

# Microsoft Copilot & KI- Readiness Checkliste

KUNDE

—

DATUM

20.03.2026

VERSION

2.0

## Inhaltsverzeichnis

Phase 1: Fundament — Tenant & Lizenzen

---

Phase 2: Datensicherheit & Compliance

---

Phase 3: Governance & Richtlinien

---

Phase 4: Pilot & Rollout

---

Phase 5: Monitoring & Optimierung

---

## Dokumenthistorie

| VERSION | DATUM      | AUTOR         | ÄNDERUNGEN                                                                        |
|---------|------------|---------------|-----------------------------------------------------------------------------------|
| 1.0     | 14.03.2026 | Hofmann<br>IT | Initiale Erstellung                                                               |
| 2.0     | 20.03.2026 | Hofmann<br>IT | Komplett überarbeitet: Power Platform, DSPM for AI, EU<br>AI Act, Phasen-Struktur |

Stand: 20.03.2026 / Version 2.0 / Hofmann IT

Diese Checkliste führt IT-Verantwortliche und Entscheider im Mittelstand strukturiert durch alle Schritte, die vor und während der Einführung von Microsoft Copilot und KI-Diensten im Microsoft-Ökosystem notwendig sind. Sie deckt M365 Copilot, Power Platform, Copilot Studio und die zugehörige Governance ab.

## Phase 1: Fundament — Tenant & Lizenzen

Bevor Copilot aktiviert werden kann, muss die technische Basis stehen. Diese Phase stellt sicher, dass Lizenzen, Identitäten und Netzwerk korrekt konfiguriert sind.

### 1.1 Lizenzierung

Microsoft 365 Copilot ist ein kostenpflichtiges Add-on, das einen qualifizierenden Basisplan voraussetzt. Ohne korrekte Lizenzierung lässt sich Copilot nicht zuweisen.

☐ **BASISPLAN VORHANDEN**

Mindestens einer der folgenden Pläne ist aktiv: Microsoft 365 Business Basic/Standard/Premium, Microsoft 365 E3/E5, Microsoft 365 F1/F3, Office 365 E1/E3/E5

☐ **COPILOT-ADD-ON BESCHAFFT**

Microsoft 365 Copilot-Lizenzen in benötigter Anzahl erworben (pro User, pro Monat)

☐ **LIZENZZUWEISUNG GEPLANT**

Entschieden, welche User in der Pilotphase und welche im Rollout Copilot erhalten

☐ **POWER PLATFORM LIZENZIERUNG GEPRÜFT**

Falls Power Apps, Power Automate oder Copilot Studio genutzt werden sollen — passende Lizenzen vorhanden (Power Apps Premium, Copilot Studio User License, Copilot Credits)

☐ **AI BUILDER CREDITS GEPRÜFT**

Falls AI Builder in Power Apps/Power Automate genutzt wird — Copilot Credits verfügbar (AI Builder Seeded Credits werden November 2026 entfernt)

☐ **SHAREPOINT ADVANCED MANAGEMENT (SAM)**

In der Copilot-Lizenz enthalten — Aktivierung im SharePoint Admin Center prüfen

| PLAN                               | COPILOT-FÄHIG | ANMERKUNG                                       |
|------------------------------------|---------------|-------------------------------------------------|
| Business<br>Basic/Standard/Premium | Ja            | Add-on erforderlich                             |
| Microsoft 365 E3                   | Ja            | Add-on erforderlich                             |
| Microsoft 365 E5                   | Ja            | Add-on erforderlich, Purview-Features inklusive |
| Microsoft 365 F1/F3                | Ja            | Eingeschränkter Funktionsumfang (Frontline)     |
| Office 365 E1/E3/E5                | Ja            | Add-on erforderlich                             |

**Hinweis:** Aktuelle Preise und Lizenzdetails finden Sie unter <https://learn.microsoft.com/copilot/microsoft-365/microsoft-365-copilot-licensing>

## 1.2 Entra ID & Identity

Copilot greift auf Daten zu, für die der jeweilige User Berechtigungen hat. Saubere Identitäten sind die Grundlage für sichere KI-Nutzung.

- ☐ **ALLE USER HABEN ENTRA ID-KONTEN**  
Keine lokalen Konten ohne Sync — hybride Umgebungen müssen über Entra Connect synchronisiert sein
- ☐ **MFA AKTIVIERT**  
Multi-Faktor-Authentifizierung für alle Copilot-User aktiv (Security Defaults oder Conditional Access)
- ☐ **CONDITIONAL ACCESS POLICIES GEPRÜFT**  
Bestehende CA-Policies blockieren Copilot-Zugriff nicht unbeabsichtigt
- ☐ **GASTKONTEN GEPRÜFT**  
Externe Gastkonten haben keinen ungewollten Zugriff auf interne Daten, die Copilot verarbeiten könnte
- ☐ **PRIVILEGIERTE KONTEN SEPARIERT**  
Admin-Konten nutzen Copilot nicht für reguläre Arbeit (Least Privilege)

## 1.3 Tenant-Grundkonfiguration

Die Tenant-Einstellungen bestimmen, wo Daten verarbeitet werden und welche Dienste aktiv sind.

- ☐ **DATENRESIDENZ GEPRÜFT**  
Tenant-Region ist korrekt (EU-Region für DSGVO-Compliance). Prüfen unter: [Admin Center](#) → [Settings](#) → [Org Settings](#) → [Organization profile](#) → [Data location](#)

☐ **EU DATA BOUNDARY**

Für Unternehmen in der EU — EU Data Boundary ist aktiviert (Datenverarbeitung innerhalb der EU)

☐ **MICROSOFT 365 APPS AKTUELL**

Microsoft 365 Apps (Desktop) sind auf aktuellem Current Channel oder Monthly Enterprise Channel

☐ **MICROSOFT SEARCH AKTIV**

Microsoft Search ist aktiviert und indiziert SharePoint, OneDrive, Teams und Exchange-Inhalte

☐ **COPILOT IM ADMIN CENTER SICHTBAR**

Copilot-Einstellungen sind unter **Admin Center → Copilot** verfügbar

## 1.4 Netzwerk & Endpoints

Copilot benötigt Zugriff auf spezifische Microsoft-Dienste. Geblockte Endpoints führen zu Funktionsausfällen.

☐ **NETZWERK-ENDPOINTS FREIGESCHALTET**

Alle Copilot-spezifischen Domains und WebSocket-Verbindungen (WSS) sind in Firewall/Proxy erlaubt

☐ **PROXY-AUSNAHMEN KONFIGURIERT**

SSL-Inspection für Microsoft-365-Traffic deaktiviert oder korrekt konfiguriert

☐ **BANDBREITE GEPRÜFT**

Ausreichende Bandbreite für KI-gestützte Anfragen (geringe Latenz zu Microsoft-Rechenzentren)

☐ **MOBILE GERÄTE**

iOS 16+ / Android 10+ für mobile Copilot-Nutzung sichergestellt

**Hinweis:** Die vollständige Endpoint-Liste finden Sie unter

<https://learn.microsoft.com/copilot/microsoft-365/microsoft-365-copilot-requirements>

## Phase 2: Datensicherheit & Compliance

Copilot arbeitet mit den Daten, auf die der User Zugriff hat. Ungeschützte oder zu breit geteilte Daten werden durch Copilot leichter auffindbar. Diese Phase sichert Ihre Daten ab.

### 2.1 Sensitivity Labels

Sensitivity Labels sind die wichtigste Schutzschicht für Dokumente und E-Mails. Copilot respektiert Labels und kann sie an neu erstellte Inhalte vererben.

☐ **SENSITIVITY LABELS AKTIVIERT**

Information Protection ist im Microsoft Purview Portal aktiviert

☐ **LABEL-TAXONOMIE DEFINIERT**

Mindestens 3-4 Stufen festgelegt (z.B. Öffentlich, Intern, Vertraulich, Streng Vertraulich)

☐ **LABELS FÜR SHAREPOINT/ONEDRIVE AKTIVIERT**

Sensitivity Labels funktionieren in SharePoint und OneDrive (nicht nur in Office-Apps). Prüfen unter: [Purview Portal → Information Protection → Labels](#)

☐ **AUTO-LABELING KONFIGURIERT**

Automatische Label-Zuweisung für sensible Inhalte (z.B. Bankverbindungen, Personalakten) eingerichtet

☐ **LABEL-VERERBUNG VERSTANDEN**

Wenn Copilot in Word/PowerPoint Inhalte aus gelabelten Dateien verwendet, wird das höchste Label automatisch übernommen

☐ **EXTRACT-RECHT GEPRÜFT**

Labels mit Verschlüsselung müssen das EXTRACT-Recht für Copilot-User erlauben, sonst können diese Inhalte nicht verarbeitet werden

## 2.2 DLP-Policies für Copilot

Data Loss Prevention verhindert, dass sensible Informationen über Copilot abfließen oder in Antworten auftauchen.

☐ **DLP-POLICY FÜR COPILOT ERSTELLT**

Im Purview Portal eine DLP-Policy mit dem Standort "Microsoft 365 Copilot and Copilot Chat" angelegt

☐ **SENSITIVITY-LABEL-BEDINGUNG**

DLP-Regel mit Bedingung "Content contains → Sensitivity labels" für hochsensible Labels erstellt (verhindert, dass Copilot diese Inhalte verarbeitet)

☐ **SENSITIVE-INFO-TYPES-BEDINGUNG**

Separate DLP-Regel für sensible Informationstypen (Kreditkartennummern, Personalausweisnummern etc.)

☐ **ENDPOINT DLP GEPRÜFT**

Falls Windows-Geräte genutzt werden — Endpoint DLP konfiguriert, um das Einfügen sensibler Daten in KI-Dienste Dritter (z.B. ChatGPT) zu blockieren oder zu warnen

☐ **DLP-ALERTS KONFIGURIERT**

Benachrichtigungen bei DLP-Verstößen an IT-Verantwortliche aktiviert

**Hinweis:** Sensitivity Labels und Sensitive Info Types können nicht in derselben DLP-Regel kombiniert werden. Erstellen Sie separate Regeln in derselben Policy.

## 2.3 SharePoint & OneDrive — Oversharing verhindern

Copilot greift auf alle SharePoint- und OneDrive-Inhalte zu, für die der User berechtigt ist. Zu breite Berechtigungen sind das grösste Risiko.

- ☐ **OVERSHARING-ASSESSMENT DURCHGEFÜHRT**  
SharePoint Advanced Management (SAM) nutzen, um Sites mit zu breitem Zugriff zu identifizieren

---

- ☐ **SHARING-DEFAULTS VERSCHÄRFT**  
Organisation-weite Sharing-Einstellung von "Anyone" auf "Specific People" geändert. Pfad: [SharePoint Admin Center](#) → [Policies](#) → [Sharing](#)

---

- ☐ **SITE ACCESS REVIEWS GESTARTET**  
Regelmässige Überprüfung der Berechtigungen für kritische SharePoint-Sites aktiviert (SAM Feature)

---

- ☐ **"EVERYONE EXCEPT EXTERNAL USERS"-BERECHTIGUNGEN ENTFERNT**  
Sicherstellen, dass keine Sites oder Bibliotheken für "Jeder ausser externe Benutzer" freigegeben sind

---

- ☐ **VERALTETE SITES IDENTIFIZIERT**  
Inaktive Sites mit sensiblen Daten einschränken oder archivieren

---

- ☐ **ONEDRIVE-SHARING GEPRÜFT**  
Standard-Freigabelinks auf "Bestimmte Personen" gesetzt (nicht "Personen in Ihrer Organisation")

---

- ☐ **RESTRICTED SHAREPOINT SEARCH**  
Falls nötig — SearchByURL aktivieren, um Copilot nur auf genehmigte Sites zugreifen zu lassen

---

## 2.4 Power Platform — DLP & Environment-Strategie

Die Power Platform (Power Apps, Power Automate, Copilot Studio) nutzt dasselbe Tenant-Ökosystem. Ohne DLP-Policies können Daten unkontrolliert zwischen Konnektoren fliessen.

- ☐ **ENVIRONMENT-STRATEGIE DEFINIERT**  
Mindestens getrennte Environments für Produktion und Entwicklung. Managed Environments für Governance-Features aktiviert

---

- ☐ **POWER PLATFORM DLP-POLICIES ERSTELLT**  
Connector-Klassifizierung in Business/Non-Business/Blocked durchgeführt. Mindestens eine Tenant-weite DLP-Policy aktiv

---

- ☐ **KRITISCHE KONNEKTOREN BLOCKIERT**  
Konnektoren mit externem Datenabfluss-Risiko (z.B. HTTP, SMTP, Twitter) in der "Blocked"-Gruppe

---

- ☐ **COPILOT STUDIO DLP-ENFORCEMENT AKTIV**  
Seit 2025 Pflicht für alle Tenants — prüfen, dass alle Copilot Studio Agents den DLP-Policies entsprechen

---

- ☐ **MAKER-BERECHTIGUNGEN EINGESCHRÄNKT**  
Nicht jeder User sollte Power Apps oder Flows erstellen können — Environment-Zugriff beschränken

---

☐ **DEFAULT-ENVIRONMENT GESICHERT**

Die Default-Umgebung ist die risikoreichste — zusätzliche Einschränkungen prüfen

| ENVIRONMENT | ZWECK                         | DLP-POLICY           |
|-------------|-------------------------------|----------------------|
| Default     | Standard-Umgebung (alle User) | Restriktiv           |
| Development | Entwicklung & Test            | Moderat              |
| Production  | Live-Apps und Flows           | Restriktiv           |
| Sandbox     | Experimentieren               | Permissiv (isoliert) |

## 2.5 Microsoft Purview — DSPM for AI

Data Security Posture Management for AI ist die zentrale Steuerung für KI-Sicherheit in Ihrem Tenant.

☐ **PURVIEW AUDIT AKTIVIERT**

Auditing im Purview Portal eingeschaltet (Voraussetzung für alle weiteren Features)

☐ **DSPM FOR AI AUFGERUFEN**

Im Purview Portal unter "Solutions → DSPM for AI" die Übersicht geprüft

☐ **DATA RISK ASSESSMENT DURCHGEFÜHRT**

Wöchentliches Assessment "Protect your data from potential oversharing risks" ist aktiv

☐ **ONE-CLICK POLICIES AKTIVIERT**

Mindestens die folgenden DSPM-Empfehlungen umgesetzt:

☐ **REPORTS-ANSICHT GEPRÜFT**

DSPM-Reports zeigen Copilot-Interaktionen, genutzte Sensitivity Labels und Risiko-Indikatoren (mind. 24h nach Aktivierung)

## 2.6 DSGVO & EU AI Act

KI-Einführung hat regulatorische Implikationen. Diese Punkte stellen die grundlegende Compliance sicher.

☐ **MICROSOFT DPA GEPRÜFT**

Das Data Processing Agreement von Microsoft deckt Copilot ab — auf aktuellem Stand prüfen

☐ **VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN AKTUALISIERT**

Copilot und Power Platform als neue Verarbeitungstätigkeit aufnehmen

☐ **DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA)**

Prüfen, ob eine DSFA für den Copilot-Einsatz erforderlich ist (insbesondere bei Verarbeitung personenbezogener Daten)

☐ **MITARBEITERINFORMATION**

Beschäftigte über die KI-Nutzung informiert (Betriebsvereinbarung, Information gem. Art. 13/14 DSGVO)

☐ **EU AI ACT ANFORDERUNGEN GEPRÜFT**

Copilot fällt als KI-System unter den AI Act — Dokumentationspflichten, Transparenzanforderungen und Risikobewertung durchgeführt

☐ **COMPLIANCE MANAGER TEMPLATES**

Im Purview Compliance Manager die AI-Regulations-Templates aktiviert und Massnahmen nachverfolgen

## Phase 3: Governance & Richtlinien

Technische Massnahmen allein reichen nicht. Klare Regeln und Verantwortlichkeiten sorgen für nachhaltigen und sicheren KI-Einsatz.

### 3.1 Interne KI-Nutzungsrichtlinie

Eine Nutzungsrichtlinie definiert, wie Mitarbeitende KI-Tools verwenden dürfen und sollen. Ohne Richtlinie fehlt der verbindliche Rahmen.

☐ **KI-NUTZUNGSRICHTLINIE ERSTELLT**

Schriftliche Richtlinie, die Dos und Don'ts für den KI-Einsatz definiert

☐ **ERLAUBTE KI-TOOLS FESTGELEGT**

Nur Microsoft Copilot und freigegebene Tools — Nutzung nicht genehmigter KI-Dienste (ChatGPT, Claude etc.) geregelt

☐ **VERTRAULICHKEITSREGELN DEFINIERT**

Welche Informationen dürfen in Copilot-Prompts eingegeben werden, welche nicht (z.B. keine Kundendaten in externen KI-Tools)

☐ **VERANTWORTLICHKEITEN FESTGELEGT**

Wer ist Ansprechpartner für KI-Themen im Unternehmen (KI-Verantwortlicher, IT, Datenschutz)

☐ **QUALITÄTSPRÜFUNG GEREGLT**

Copilot-generierte Inhalte müssen vor externer Verwendung geprüft werden (kein blindes Vertrauen in KI-Ausgaben)

☐ **RICHTLINIE KOMMUNIZIERT UND UNTERSCHRIEBEN**

Alle Mitarbeitenden haben die Richtlinie erhalten und bestätigt

### 3.2 Copilot Studio & Agents Governance

Copilot Studio ermöglicht die Erstellung eigener KI-Agents. Ohne Governance kann jeder User unkontrolliert Agents erstellen und teilen.

- ☐ **AGENT-ERSTELLUNGSRECHTE EINGESCHRÄNKT**  
Festgelegt, wer Copilot Studio Agents erstellen darf (nicht jeder User)

---

- ☐ **AGENT-SHARING-REGELN DEFINIERT**  
Agents dürfen nur innerhalb definierter Grenzen geteilt werden (kein anonymer Zugang)

---

- ☐ **AUTHENTIFIZIERUNGS-PROVIDER FEST GELEGT**  
Agents nutzen ausschliesslich genehmigte Auth-Provider (z.B. Entra ID)

---

- ☐ **AGENT-LIFECYCLE DEFINIERT**  
Prozess für Erstellung, Prüfung, Freigabe und Deaktivierung von Agents

---

- ☐ **TEAMS-AGENTS-INTEGRATION GEPRÜFT**  
Agents in Microsoft Teams folgen denselben Governance-Regeln wie Copilot Studio Agents

---

- ☐ **CONNECTOR-NUTZUNG IN AGENTS EINGESCHRÄNKT**  
Agents dürfen nur freigegebene Konnektoren verwenden (DLP-Policies greifen)

---

### 3.3 Retention & Data Lifecycle

Copilot-Interaktionen (Prompts und Antworten) werden gespeichert und unterliegen denselben Aufbewahrungsregeln wie andere M365-Daten.

- ☐ **RETENTION POLICY FÜR COPILOT ERSTELLT**  
Im Purview Portal eine Retention Policy mit dem Standort "Microsoft Copilot Experiences" angelegt

---

- ☐ **AUFBEWAHRUNGSFRISTEN DEFINIERT**  
Entschieden, wie lange Copilot-Interaktionen aufbewahrt werden (regulatorische Anforderungen, interne Vorgaben)

---

- ☐ **CLOUD ATTACHMENTS RETENTION**  
Auto-Apply Retention Label für "Cloud attachments shared in Copilot" konfiguriert — sichert die Dateiversion zum Zeitpunkt der Copilot-Referenzierung

---

- ☐ **EDISCOVERY-BEREITSCHAFT**  
Copilot-Interaktionen sind über eDiscovery durchsuchbar (Bedingung: Type → "Copilot activity").  
Sicherstellen, dass dies bei Bedarf funktioniert

---

## Phase 4: Pilot & Rollout

Ein phasenweiser Rollout minimiert Risiken und ermöglicht Lernen aus der Praxis. Beginnen Sie klein, skalieren Sie schnell.

## 4.1 Pilotgruppe definieren

- ☐ **PILOT GRUPPE ZUSAMMENGESTELLT**  
5-15 User aus verschiedenen Abteilungen (idealerweise technikaffin, aber auch "normale" Anwender)

---

- ☐ **ABTEILUNGSÜBERGREIFEND BESETZT**  
Mindestens Vertreter aus Vertrieb, Verwaltung und einer Fachabteilung

---

- ☐ **ERFOLGSKRITERIEN DEFINIERT**  
Messbare Kriterien festgelegt (z.B. Zeitersparnis bei E-Mails, Qualität von Zusammenfassungen, User-Zufriedenheit)

---

- ☐ **PILOT-ZEITRAUM FEST GELEGT**  
Mindestens 4 Wochen, idealerweise 6-8 Wochen für aussagekräftige Ergebnisse

---

- ☐ **FEEDBACK-KANAL EINGERICHTET**  
Dedizierter Teams-Kanal, Kurzumfrage oder regelmässiges Feedback-Meeting

---

## 4.2 Training & Enablement

Copilot ohne Training verschenkt Potenzial. Geschulte User erzielen deutlich bessere Ergebnisse.

- ☐ **GRUNDLAGEN-SCHULUNG ERSTELLT**  
Einführung in Copilot (Was kann es? Wo finde ich es? Wie starte ich?)

---

- ☐ **PROMPT-TRAINING DURCHGEFÜHRT**  
Best Practices für effektive Prompts (spezifisch, kontextreich, iterativ)

---

- ☐ **ABTEILUNGSSPEZIFISCHE USE CASES**  
Pro Abteilung 3-5 konkrete Anwendungsfälle identifiziert und geschult

---

- ☐ **CHAMPIONS IDENTIFIZIERT**  
Pro Abteilung 1-2 Power-User als Multiplikatoren und erste Anlaufstelle

---

- ☐ **SCHULUNGSMATERIAL BEREITGESTELLT**  
Kurzanleitungen, Prompt-Bibliothek und FAQ-Dokument verfügbar

---

- ☐ **COPILOT LAB VERWIESEN**  
Microsoft Copilot Lab (<https://copilot.cloud.microsoft/prompts>) als Ressource für Prompt-Inspiration kommuniziert

---

## 4.3 Kommunikation & Change Management

Technologie allein ändert nichts. Mitarbeitende brauchen Verständnis, warum KI eingeführt wird und was sich für sie ändert.

- ☐ **KOMMUNIKATIONSPLAN ERSTELLT**  
Wer wird wann über was informiert (Management, Pilotgruppe, alle Mitarbeitende)

---

☐ **MANAGEMENT-BUY-IN SICHERGESTELLT**

Geschäftsführung steht hinter der KI-Einführung und kommuniziert dies aktiv

☐ **ÄNGSTE ADRESSIERT**

Offene Kommunikation darüber, dass Copilot unterstützt (nicht ersetzt) — Fragen und Bedenken ernst nehmen

☐ **QUICK WINS KOMMUNIZIERT**

Erste Erfolge aus der Pilotphase sichtbar machen und teilen

☐ **ROLLOUT-PLAN ERSTELLT**

Nach erfolgreichem Pilot — gestaffelter Rollout mit definierten Wellen und Zeitplan

## Phase 5: Monitoring & Optimierung

Nach dem Rollout beginnt die kontinuierliche Optimierung. Monitoring-Daten zeigen, wo Copilot Mehrwert liefert und wo nachgesteuert werden muss.

### 5.1 Copilot Usage Dashboard & Adoption

☐ **COPILOT DASHBOARD AKTIVIERT**

Im Microsoft 365 Admin Center unter "Reports → Copilot" das Usage-Dashboard aufrufen

☐ **ADOPTION SCORE BASELINE**

Microsoft Adoption Score als Baseline vor dem Rollout festgehalten (vorher/nachher-Vergleich)

☐ **AKTIVE NUTZUNG TRACKEN**

Regelmässig prüfen, welche User Copilot aktiv nutzen und welche nicht (Nachschulung für Nicht-Nutzer)

☐ **FEATURE-NUTZUNG ANALYSIEREN**

Welche Copilot-Features werden genutzt (Zusammenfassungen, Entwürfe, Datenanalyse)? Wo liegt ungenutztes Potenzial?

### 5.2 Purview Reports & DSPM-Reviews

☐ **DSPM FOR AI REPORTS REGELMÄSSIG PRÜFEN**

Wöchentlich die Copilot-spezifischen Reports in Purview DSPM aufrufen

☐ **SENSITIVITY-LABEL-NUTZUNG ÜBERWACHEN**

Prüfen, welche Labels in Copilot-Interaktionen am häufigsten referenziert werden

☐ **RISIKANTE INTERAKTIONEN PRÜFEN**

Alerts für unethische oder riskante KI-Nutzung im Insider Risk Management überprüfen

☐ **DLP-VERSTÖSSE AUSWERTEN**

Regelmässig DLP-Alerts analysieren und Policies bei Bedarf nachschärfen

### 5.3 Review-Termine & kontinuierliche Verbesserung

- ☐ **MONATLICHES REVIEW (ERSTE 3 MONATE)**  
Nutzungsdaten, Feedback, Probleme und Verbesserungsvorschläge besprechen

---

- ☐ **QUARTALS-REVIEW (DANACH)**  
Nutzungsentwicklung, ROI-Bewertung, neue Use Cases identifizieren

---

- ☐ **GOVERNANCE-REVIEW HALBJÄHRlich**  
DLP-Policies, Sensitivity Labels, Berechtigungen und Richtlinien auf Aktualität prüfen

---

- ☐ **NEUE FEATURES EVALUIEREN**  
Microsoft aktualisiert Copilot regelmässig — neue Features bewerten und ggf. aktivieren

---

- ☐ **ESKALATIONSPFAD DEFINIERT**  
Klarer Prozess, wenn Copilot sensible Daten in Antworten liefert oder Sicherheitsvorfälle auftreten

---

## Bereit für den nächsten Schritt?

Hofmann IT begleitet Sie von der Planung bis zum Go-live — KI-Strategie, Tenant-Konfiguration und Rollout aus einer Hand.

[Jetzt anfragen →](#)

## Quellen

1. [Minimum Requirements](#)
2. [License Options](#)
3. [Secure & Govern Blueprint](#)
4. [Purview for Copilot](#)
5. [DLP for Copilot](#)
6. [SharePoint SAM](#)
7. [Power Platform DLP](#)
8. [Copilot Studio Security](#)
9. [Copilot Studio Licensing](#)
10. [Managed Environments](#)

|                |            |
|----------------|------------|
| STAND          | 20.03.2026 |
| VERSION        | 2.0        |
| ERSTELLT DURCH | Hofmann IT |
| DOKUMENT TYP   | CHECKLISTE |

## Glossar

### Copilot

KI-Assistent von Microsoft, integriert in M365-Apps

### Sensitivity Labels

Klassifizierungs- und Schutzlabels in Purview

### DLP

Data Loss Prevention

### SAM

SharePoint Advanced Management

### DSPM for AI

Data Security Posture Management for AI

### Managed Environments

Governance-Feature der Power Platform

### Entra ID

Microsofts Identity-Plattform (ehem. Azure AD)

### Copilot Credits

Abrechnungseinheit für Copilot Studio/AI Builder

### EU AI Act

EU-Verordnung über Künstliche Intelligenz

### Retention Policy

Aufbewahrungsrichtlinie in Purview