Ist deine Datenablage ready für Copilot?

Copilot Checkliste:

Copilot sieht alles, was eine Person in M365 öffnen darf. Ist die Ablage unstrukturiert, veraltet oder zu breit berechtigt, liefert Copilot schlechte Antworten oder zeigt Inhalte, die niemand sehen sollte.

1. Struktur & Ablage

- ☐ Dokumentierte Ablagelogik: Was gehört in OneDrive, was in Teams, was in SharePoint?
- ☐ Persönliche Arbeitsdokumente liegen in OneDrive, Teamdokumente in Teams oder SharePoint.
- ☐ Teams und SharePoint-Sites sind nach Organisationseinheiten, Projekten, Themen aufgebaut.
- ☐ Namenskonvention für Teams, Sites, Kanäle und Dateien vorhanden.
- ☐ Ordnerstrukturen flach (maximal 3 - 4 Ebenen).
- ☐ Dokumente aussagekräftig benannt (kein «Entwurf_final_v3_neu.docx»).
- ☐ Pro Thema eine massgebende Version. Duplikate und Kopien bereinigt.
- ☐ Wichtige Dokumente via Metadaten / Spalten auffindbar (z. B. Dokumenttyp, Status, Gültigkeit).
- ☐ Daten aus alten Fileservern migriert oder klar als Archiv gekennzeichnet.

2. Berechtigung & Oversharing

- ☐ Berichte Datenzugriffs-Governance im SharePoint Admin Center ausgeführt und ausgewertet.
- ☐ Freigaben «Jeder ausser externen Benutzern» und «Jeder» geprüft und aufs Nötigste reduziert.
- ☐ Organisationsweite Freigabelinks und anonyme Links geprüft und wo nötig entfernt.
- ☐ Öffentliche Teams und Sites bewusst öffentlich. Alle anderen auf privat gestellt.
- ☐ Standardeinstellung Freigabelinks «Bestimmte Personen» statt «Personen in der Organisation».
- ☐ Berechtigungen über Gruppen vergeben, nicht Einzelpersonen.
- ☐ Unterbrochene Vererbung Ordner- und Dateiebene bekannt und auf Ausnahmen beschränkt.
- ☐ Gastzugriffe geprüft. Gäste ohne aktuelles Projekt entfernt.
- ☐ Ehemalige Mitarbeitende und Rollenwechsel in Berechtigungen nachgeführt.
- ☐ Heikle Sites (noch nicht bereinigt) Restricted Content Discovery als Übergangslösung aktiviert.

Vorgehen für diese Checkliste

- Jeden Punkt abhaken der vollständig erfüllt ist
- Teilweise erfüllt zählt als offen
- Auswertung

3. Aktualität & Lebenszyklus

- ☐ Inaktive Sites und Teams identifiziert (z. B. über Richtlinie für inaktive Sites in SharePoint Advanced Management).
- ☐ Abgeschlossene Projekte archiviert, z. B. mit Microsoft 365 Archive. Archivierte Inhalte fliessen nicht in Copilot-Antworten ein.
- ☐ Veraltete Versionen von Richtlinien, Prozessen und Vorlagen gelöscht oder ungültig gekennzeichnet.
- ☐ Aufbewahrungsrichtlinien, die festlegen, wie lange welche Daten aufbewahrt und wann sie gelöscht werden.
- ☐ Ablauf- oder Überprüfungsprozess Teams und Gruppen (z. B. Ablaufrichtlinie für M365-Gruppen).
- ☐ Wichtige Dokumente haben Überprüfungsdatum oder Gültigkeitsangabe.
- ☐ Fester Rhythmus für Aufräumen (z. B. einmal pro Jahr pro Bereich).

Dein Kontakt

Beetroot AG
+41 41 700 30 40
info@beetroot.ag

beetroot

4. Sensible Daten schützen

- Es ist bekannt, wo sensible Daten liegen (HR, Finanzen, Verträge, Gesundheits- oder Kundendaten).
- Sensible Daten in eigenen, eng berechtigten Sites oder Teams, nicht in allgemeinen Ablagen.
- Vertraulichkeitsbezeichnungen (Sensitivity Labels) sind definiert und auf heikle Daten angewendet.
- Datenschutzverantwortliche sind in die Copilot-Einführung einbezogen.
- Anforderungen aus Datenschutzgesetz (DSG) und allfälligen Branchenvorgaben geprüft.

5. Verantwortung & Rollen

- Jedes Team und jede Site hat mindestens zwei aktive Besitzende.
- Sites und Teams ohne Besitzende sind identifiziert und neu zugewiesen oder archiviert.
- Besitzende wissen, dass sie für Inhalte, Berechtigungen und Aktualität ihres Bereichs verantwortlich sind.
- Pro Bereich gibt es eine datenverantwortliche Person, die über Struktur und Aufbewahrung entscheidet.
- Zuständigkeiten zwischen IT, Fachbereichen und Datenschutz sind geklärt.
- Spielregeln für die Ablage, die allen Mitarbeitenden bekannt sind.

6. Testen vor dem Rollout

- Pilotgruppe aus verschiedenen Abteilungen und Hierarchiestufen ist bestimmt.
- Pilotgruppe testet gezielt heikle Fragen (z. B. «Zeig mir Lohninformationen»).
- Quellenangaben in den Copilot-Antworten werden geprüft: Stammen sie aus aktuellen und massgebenden Dokumenten?
- Gefundene Probleme werden dokumentiert und vor dem breiten Rollout behoben.
- Meldeweg ist definiert, falls Mitarbeitende nach dem Rollout Inhalte sehen, die sie nicht sehen sollten.

7. Mitarbeitende befähigen

- Mitarbeitende wissen, wo welche Daten abgelegt werden.
- Mitarbeitende wissen, wie sie Dokumente richtig teilen (Personen statt Organisation, Link statt Anhang).
- Mitarbeitende verstehen, dass Copilot alles findet, worauf sie Zugriff haben.
- Key User oder Champions pro Bereich sind bestimmt und geschult.
- Es gibt eine kurze Anleitung oder ein Lernangebot zur Ablage in M365.

Ergebnis	Einschätzung	Nächster Schritt
Blöcke 2 und 4 vollständig, übrige mehrheitlich erfüllt	**Bereit für den Rollout**	Pilot durchführen, dann schrittweise ausrollen
Blöcke 2 und 4 vollständig, übrige grösstenteils offen	**Bedingt bereit**	Pilot starten, Struktur und Aktualität parallel verbessern
Offene Punkte in Block 2 oder 4	**Noch nicht bereit**	Berechtigungen bereinigen und sensible Daten schützen, erst dann pilotieren

beetroot