S.H.A.R.E.

Empfohlenen Sicherheitseinstellungen im Bezug auf CoPilot

Quelle: Ausführliche KI Recherche zur nDSG Konformität von M365 Copilot, Stand 15.09.2026

Empfänger: IT-Administration / M365-Tenant-Administrator

Priorität: Hoch / Sofortmassnahme

Zweck: Unterbindung von Datenabflüssen in Drittstaaten und Schutz vor interner Datenoffenlegung («Oversharing») gemäss Schweizer Datenschutzgesetz (revDSG) bei der Nutzung von Microsoft Copilot.

Teil 1: Sofortmassnahmen (Notfall-Härtung im Admin Center)

Frist: Unverzüglich umzusetzen

Bitte führen Sie im Microsoft 365 Tenant die folgenden administrativen Konfigurationen durch und bestätigen Sie deren Umsetzung:

1. **Drittstaaten-Routing sperren (Flex Routing deaktivieren)**
   - **Microsoft 365 Admin Center:** Unter `Copilot` > `Settings` > `View all` > Menüpunkt `Flex routing during peak load periods` auf **`Do not allow flex routing`** setzen.
   - **Power Platform Admin Center** (sofern Umgebungen aktiv sind): In den Umgebungseinstellungen unter `Generative AI features` die Optionen `Move data across regions` und `Allow flex routing during periods of peak load` deaktivieren.
   - *Ziel:* Verhindert, dass Prompts und Daten bei Server-Lastspitzen in die USA, nach Kanada oder Australien weitergeleitet werden.

2. **Externe KI-Subprozessoren (Anthropic) sperren**
   - **Microsoft 365 Admin Center:** Unter `Copilot` > `Settings` > `View all` > `AI providers operating as Microsoft subprocessors` prüfen und sicherstellen, dass der Status für **Anthropic** mandantenweit auf **`Disable`** bzw. **`No users`** steht.

- Den app-spezifischen Schalter `Copilot in Microsoft 365 apps with Anthropic models` (für Word, Excel, PowerPoint) ebenfalls deaktivieren.
- *Ziel:* Verhindert Datenübermittlungen an externe Modell-Infrastrukturen ausserhalb des europäischen Raums.

3. **Web-Suchanreicherung deaktivieren (Web Search Grounding)**
   - **Cloud Policy Service (`config.office.com`):** Eine globale Richtlinie für die Organisation konfigurieren und die Einstellung **`Allow web search in Copilot`** auf **`Disabled`** setzen.
   - *Ziel:* Unterbindet die Übermittlung von Begriffen oder Prompt-Fragmenten an die Bing-Websuche.

4. **Sensible Ablagen abschirmen (Restricted Content Discovery aktivieren)**
   - **SharePoint Admin Center:** Für alle Websites mit sensiblen Inhalten (z. B. Klientenakten, HR, Spenderverzeichnisse, Finanzen) unter `Active sites` > Website auswählen > `Settings` den Schalter **`Restrict content from Microsoft Copilot`** aktivieren.
   - *Hinweis: Restricted SharePoint Search* (RSS) ist abgekündigt und darf nicht mehr neu eingerichtet werden; es ist ausschliesslich **Restricted Content Discovery (RCD)** zu verwenden.
   - *Ziel:* Schliesst diese Datenbestände sofort von organisationsweiten KI-Antworten aus, ohne den berechtigten Nutzern den direkten Dateizugriff zu entziehen.

5. **Microsoft Purview DLP für Copilot aktivieren**
   - **Purview Portal (`purview.microsoft.com`):** Eine Data Loss Prevention (DLP)-Richtlinie für den Speicherort **`Microsoft 365 Copilot and Copilot Chat`** einrichten:
     - Regel 1: Dokumente mit Sensitivitätslabels für vertrauliche/hochsensible Daten mit der Aktion **`Prevent Copilot from processing content`** belegen.
     - Regel 2: Prompts, die sensible Informationstypen (z. B. Schweizer AHV-Nummer, IBAN) enthalten, mit der Aktion **`Prevent Copilot from processing prompts`** blockieren.

Teil 2: Langfristige Governance- und Architektur-Massnahmen

Frist: Einplanung in den IT- und Compliance-Betrieb

Nach Umsetzung der Notfall-Härtung sind folgende strukturelle Massnahmen umzusetzen:

1. **Berechtigungsbereinigung und Oversharing-Audit**
    - Im SharePoint Admin Center unter `Reports` > `Data access governance` Berichte über weitreichende Freigaben erstellen.
    - Zugriffsrechte der Pseudogruppe `Everyone except external users` sowie organisationsweite Freigabelinks («Jeder im Unternehmen») auf sensiblen Dokumenten und Ordnern systematisch entfernen.
    - Zugriffsberechtigungen strikt nach dem «Need-to-Know»-Prinzip über geschlossene Entra-Sicherheitsgruppen neu strukturieren.

2. **Einführung und Durchsetzung von Sensitivity Labels**
    - Ein verbindliches Klassifizierungsschema in Microsoft Purview etablieren (z. B. *Öffentlich*, *Intern*, *Vertraulich*, *Besonders schützenswert*).
    - Automatische oder pflichtmässige Kennzeichnung für alle neuen Dokumente und E-Mails durchsetzen, damit Sicherheitsfilter verlässlich greifen.

3. **Unterstützung bei der Datenschutz-Folgenabschätzung (DSFA)**
    - Bereitstellung der technischen Systemdokumentation und Nachweise der oben genannten Härtungsmassnahmen für die Dokumentation nach Art. 22 revDSG.

4. **Verbindliche interne KI-Nutzungsrichtlinie («Acceptable Use Policy»)**
    - Statutarische Verankerung des Verbots, unverschlüsselte Klardaten von Schutzbedürftigen direkt in Prompts einzugeben.
    - Festlegung des Vier-Augen-Prinzips: Keine unkritische Übernahme von KI-Ergebnissen bei folgenschweren Entscheidungen.