ARTAKER IT Group

IM GESPRÄCH

KI-Compliance ohne Lücken der Mostviertler Gebäudetechnik

Data Governance und KI mit Microsoft Purview

Masa Maurer, Artaker IT Group
Mathias Grimm, ALSO Austria

ALSO THE TECHNOLOGY PROVIDER

Ein Schmerz: Die Daten sind nicht geschützt

Zu viele sehen sie, oder sie verlassen das Haus. Drei Szenen aus der Mostviertler Gebäudetechnik:

ZU VIELE SEHEN ES



Die Gehaltsliste

Copilot zeigt der Assistentin die Gehälter. Die Liste lag offen im Team.

VERLÄSST DAS HAUS



Der Rahmenvertrag

Ging als Mailanhang an die Steuerberatung, ohne jeden Schutz.

VERLÄSST DAS HAUS



Die Rechnung

Samt IBAN zum Übersetzen in einen kostenlosen KI-Dienst kopiert.

Copilot verursacht kein Oversharing. Er macht es sichtbar.

Data Governance in fünf Fragen

1. **Welche Daten haben wir?**
2. **Wo liegen sie?**
3. **Wer kann darauf zugreifen?**
4. **Wie sind sie geschützt?**
5. **Was macht die KI damit?**

NEU DURCH KI

Können Sie alle fünf für Ihr Unternehmen beantworten, mit Belegen?

Alle Ebenen reden mit: Unternehmensführung, Fachbereiche, IT und Mitarbeitende.

Fragen 1 bis 4 nach Microsoft, Stand Oktober 2026.

Fragen 1 bis 4: erkennen, schützen, lenken

1

Welche Daten haben wir?

Sensitive Information Types erkennen etwa die IBAN.

2

Wo liegen sie?

Data Security Posture Management (DSPM) zeigt sie in Mail, Teams, SharePoint und OneDrive.

3

Wer kann darauf zugreifen?

DSPM findet zu offene Freigaben, Sie schließen sie gleich.

4

Wie sind sie geschützt?

Sensitivity Label verschlüsselt, **Data Loss Prevention (DLP)** warnt beim Weitergeben.

BEISPIEL BERLIN, AUGUST 2026

Was passiert ist

Dateien aus Ordnern der Verwaltung landeten im Darknet, laut Medien auch Gehaltslisten.

Was Purview daran ändert

Den Einbruch nicht. Verschlüsselte Dateien bleiben aber ohne Berechtigung unlesbar.

Am heikelsten sind oft Dateien, an die keiner denkt.

Quellen: berlin.de (29.09.2026), Spiegel, WELT; Microsoft Learn, Oktober 2026.

Die KI hält sich an Ihre Berechtigungen

Copilot im Haus

Sieht nur, was die Person öffnen darf. Aber alles davon, auch die vergessene Gehaltsliste.

Fremde KI im Browser

Was dort eingefügt wird, liegt bei einem fremden Anbieter. Ohne Überblick sieht das niemand.

Purview zieht die Leitplanken ein, für Copilot und für fremde KI.

Ihre Daten trainieren nicht die KI-Modelle von Copilot. So sagt es Microsoft.

Quelle: Microsoft Learn, Datenschutz und Sicherheit für Microsoft Copilot, Stand Oktober 2026.

Copilot einführen, Leitplanken mitziehen

Parallel zum Start, nicht als Hürde davor.

Sehen

DSPM: Welche KI wird genutzt, mit welchen sensiblen Daten?

Aufräumen

Data Risk Assessment: Zu offene Freigaben finden und schließen.

Ausnehmen

DLP for Copilot: Streng vertrauliche Dateien bleiben draußen.

Nachvollziehen

Audit: Prompts und Antworten landen im Protokoll.

Copilot nutzen, ohne die Kontrolle über Ihre Daten abzugeben.

DSPM: Data Security Posture Management · DLP: Data Loss Prevention · Microsoft Learn, Stand Oktober 2026, Umfang je nach Lizenz.

Wann greift was?

SZENE UND MOMENT		PURVIEW-FUNKTION UND WIRKUNG
Die Gehaltsliste bevor Copilot sucht	→	**DSPM und Sensitivity Label** Offenes Team fällt auf, Copilot zeigt die Gehälter nicht mehr.
Der Rahmenvertrag beim Versenden	→	**DLP Policy und Sensitivity Label** Policy Tip in Outlook, draußen nur für Berechtigte lesbar.
Die Rechnung beim Einfügen in ChatGPT	→	**Endpoint DLP** Warnung oder Sperre direkt am Gerät, je nach Einstellung.

Im Hintergrund: Audit protokolliert, der Compliance Manager zeigt den Fortschritt.

Business Premium: Manual Labeling, DLP für Mail und Ablagen. Purview Suite bzw. E5: Auto-Labeling, Endpoint DLP, DLP for Copilot für Dateien.
DSPM: Data Security Posture Management · DLP: Data Loss Prevention · laut Microsoft, Stand Oktober 2026.

Copilot und fremde KI: die häufigsten Fragen

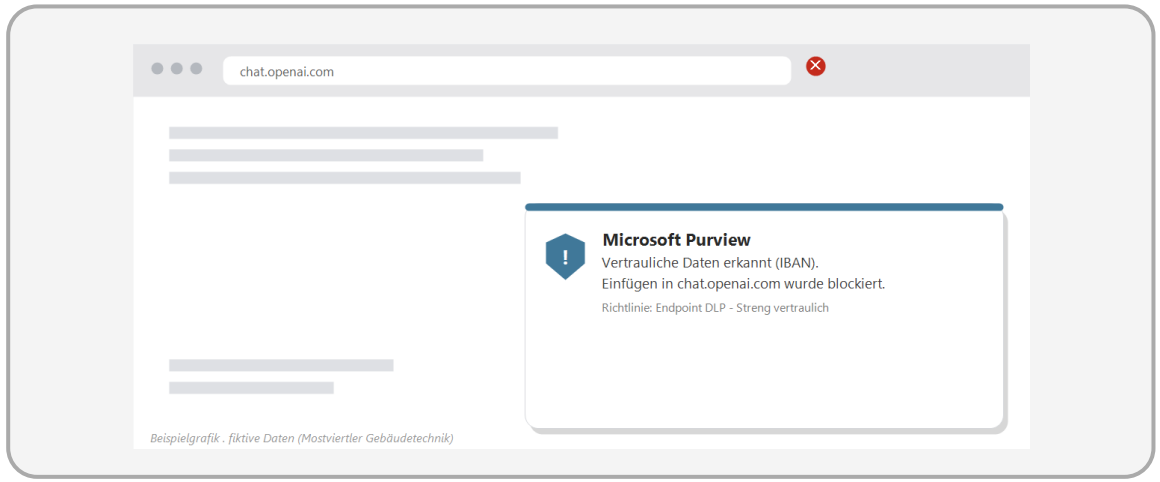
HÄUFIGE FRAGE ODER STOLPERSTEIN		KURZANTWORT
Verursacht Copilot das Oversharing?	Nein →	Er macht nur offene Freigaben sichtbar.
Wer merkt den Versand von IBAN oder SV-Nummer?	DLP →	DLP warnt und meldet es. Verschlüsselt bleibt die Datei trotzdem geschützt.
Sieht man KI-Prompts im Nachhinein?	E5 →	Ja: Prompt und Antwort landen im Audit-Log.
Schützt das auch vor ChatGPT & Co.?	Gerät →	Nur mit Endpoint DLP am eingebundenen Gerät.
Braucht das volles Geräte-Management?	Edge →	Oft reicht eine Regel in Edge for Business.

Erkennen, warnen, verschlüsseln: drei Ebenen, die sich ergänzen.

DLP: Data Loss Prevention.

Woran Sie sehen, dass es wirkt

IM ALLTAG: DIE MITARBEITENDEN SEHEN ES



Endpoint DLP warnt beim Einfügen in ChatGPT. In Outlook erscheint ein **Policy Tip** vor dem Versand.

IM ÜBERBLICK: DIE UNTERNEHMENSFÜHRUNG SIEHT ES



Compliance Manager: Ihren Startwert haben Sie schon, die **Data Protection Baseline**.

Fortschrittsmaß, kein Compliance-Zertifikat. So sagt es auch Microsoft.

DLP: Data Loss Prevention, Endpoint DLP direkt am Gerät · Microsoft Learn, Stand Oktober 2026, Umfang je nach Lizenz.

ARTAKER IT Group

Womit Sie selbst anfangen können

Die Bestandsaufnahme im Microsoft Purview Portal

1 Startwert ansehen

Compliance Manager: Ihr Wert ist schon da

2 Freigaben prüfen

DSPM zeigt, was zu offen ist, nach ein paar Tagen

3 Daten benennen

Was ist kritisch? Mit den Fachbereichen klären

Gemeinsam mit Artaker: office@artaker.it · +43 1 588 52 0 · artaker.it

Und Microsoft Defender? Der Bruder von Purview, gern im persönlichen Gespräch.

Danke! Masa Maurer, Artaker IT Group · Mathias Grimm, ALSO Austria

Vieles steckt schon in Microsoft 365 Business Premium. Auto-Labeling, Endpoint DLP und DLP for Copilot für Dateien: Purview Suite bzw. E5.
DSPM: Data Security Posture Management · laut Microsoft, Stand Oktober 2026, Änderungen vorbehalten. Keine Rechtsberatung.

ARTAKER
IT Group

NEU IM MANAGED SERVICE

Zertifikate, die sich selbst erneuern

Wir stellen Ihre SSL/TLS-Zertifikate aus, erneuern sie rechtzeitig und binden sie vollautomatisch in Ihre Systeme ein.

100 Tage

Laufzeit ab 15. März 2027

47 Tage

Laufzeit ab März 2029

Get IT done.

Ihr Nutzen auf einen Blick

Vollständig automatisiert und von unserem Managed-Service-Team betreut.

Keine Ausfälle

Erneuerung rund 30 Tage vor Ablauf

Kein Aufwand

Einmal eingerichtet, läuft alles von selbst

Sicher umgesetzt

Keine offenen Ports, kein DNS-Zugriff

Volle Transparenz

Statusbericht jeden Monat

Abgedeckt: IIS, Apache, nginx · Exchange inkl. Hybrid · Entra App Proxy · FortiGate · Sophos

Jetzt ansprechen und vor März 2027 umstellen



Raphael Kury

raphael.kury@artaker.it