

Microsoft Purview im Oktober: Copilot Pages und Notebooks werden durchsuchbar und auf Hold setzbar

Monatelang hat dein Team fleißig Copilot Pages gebaut, Notebooks gefüttert und Loop-Workspaces vollgeschrieben. Und monatelang hat deine Rechtsabteilung geglaubt, ein Litigation Hold auf den Benutzer würde das alles mit einfrieren. Spoiler: tat er nicht. Der Oktober räumt hier auf – und bringt nebenbei Dateiarchivierung, die Copilot das Vergessen beibringt.

Executive Summary

Copilot Pages, Copilot Notebooks und Loop „My workspace“ liegen nicht in OneDrive, sondern in einem **benutzereigenen SharePoint-Embedded-Container**. Den musste eDiscovery bisher quasi mit Taschenlampe und handgeschriebener Container-URL suchen, die du per PowerShell oder beim SharePoint-Admin erbetteln durftest. Ab **Mitte Oktober 2026** taucht dieser Container direkt im Datenquellen-Picker auf, wenn du einen Benutzer zu einem Case, einer Suche oder einem Hold hinzufügst. Rollout-Ende: voraussichtlich Ende Oktober.

Parallel landet die **Archivierung auf Dateiebene** in SharePoint: Einzelne inaktive Dateien wandern ins Microsoft 365 Archive, bleiben unter Aufbewahrung und Hold, bleiben für eDiscovery auffindbar – und verschwinden aus dem Copilot-Index. Dazu kommen Network Data Security als GA, Compliance-Abdeckung für Claude Enterprise und ein paar Grenzen bei mandantenübergreifenden Teams-Chats, die du kennen solltest, bevor sie dich kennenlernen.

Warum das gerade jetzt Gewicht hat? Weil Copilot-Inhalte längst keine Spielwiese mehr sind. In Pages landen Projektentscheidungen, in Notebooks ganze Verhandlungsstrategien, in Loop die Protokolle, die früher in einer E-Mail gestanden hätten. Die E-Mail war seit Jahren sauber unter Aufbewahrung. Ihr KI-Nachfolger lebte bis eben im Compliance-Niemandland. Das ist ungefähr so, als würdest du das Firmenarchiv brandschutzsanieren und die Akten im Gartenhäuschen lagern.

1 FAKTEN: Die drei Kernaussagen in 30 Sekunden

1. Copilot Pages, Notebooks und Loop sind jetzt erstklassige eDiscovery-Quellen: suchen, halten, exportieren.
2. Deine Aufbewahrungspläne müssen diese Inhaltstypen ausdrücklich nennen – sonst existieren sie juristisch im Graubereich.
3. Archivierte Dateien sind für Copilot tot, für den Anwalt der Gegenseite aber quicklebendig.

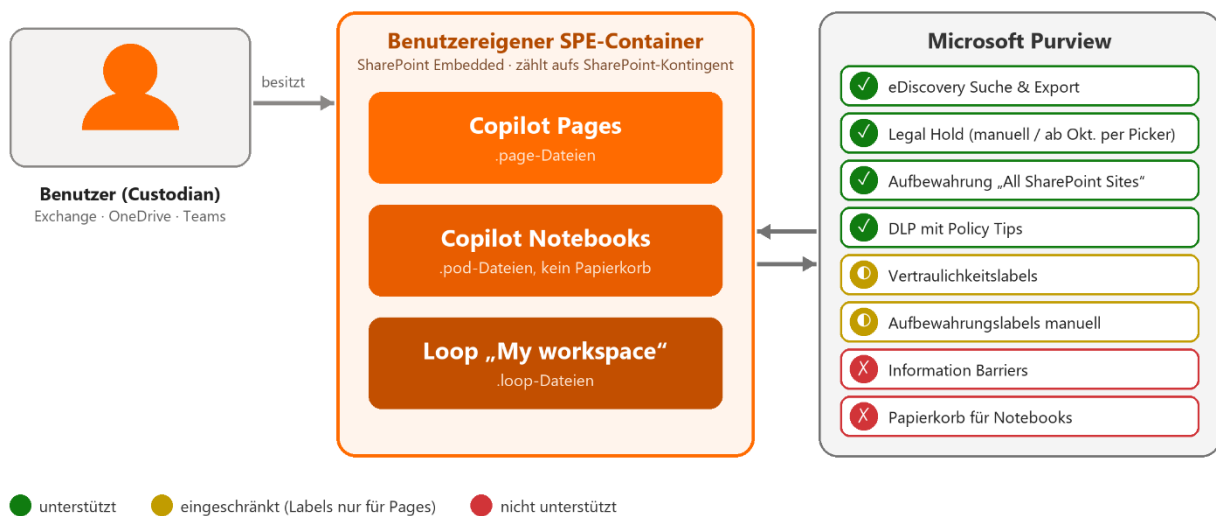
Worum geht es im Detail?

Wo Copilot Pages eigentlich wohnen

SharePoint Embedded ist eine app-spezifische Speicherpartition in deinem Mandanten – SharePoint ohne die SharePoint-Oberfläche. Jeder Benutzer bekommt **genau einen Container**, den sich Copilot Pages (.page-Dateien), Copilot Notebooks (.pod-Dateien) und der Loop „My workspace“ teilen. Der Speicher zählt gegen dein SharePoint-Kontingent, Quoten pro Container kannst du nicht setzen, und standardmäßig hält jede Datei 50 Hauptversionen vor. Klingt nach Detail, ist aber der Grund, warum klassische OneDrive-Prozesse hier ins Leere laufen: Der Container gehört zwar dem Benutzer, ist aber nicht sein OneDrive.

Wo Copilot Pages und Notebooks wirklich wohnen

Ein Container pro Benutzer in SharePoint Embedded – und was Purview dort darf



Achtung Falle:

Ein Litigation Hold auf den Benutzer erfasst den Container NICHT automatisch.
App-eigene SPE-Container bleiben auch nach dem Oktober-Release außen vor.

Abbildung 1: Der benutzereigene SPE-Container und der Funktionsumfang von Purview (Stand Oktober 2026)

Neulich bei einem Maschinenbauer: Der Vertriebsleiter hatte seine komplette Angebotsstrategie für einen Großkunden in einem Copilot Notebook entwickelt – inklusive Rabattstaffeln, die man lieber nicht vor Gericht vorliest. Als ein Rechtsstreit drohte, setzte die Rechtsabteilung brav den Hold auf Postfach und OneDrive. Das Notebook? Lag fröhlich daneben, ungehalten und löschbar. Einen Papierkorb für Notebooks gibt es übrigens nicht. Weg ist weg, wie die Karriere eines Projektleiters nach dem dritten verschobenen Go-live.

Was sich im Oktober konkret ändert

Laut Message Center (MC1470884) lief die Public Preview ab Mitte September, die weltweite allgemeine Verfügbarkeit startet Mitte Oktober. Fügt du einen Benutzer als Datenquelle hinzu, siehst du künftig seine SPE-Container und kannst sie für Cases, Suchen und Holds auswählen. Es werden nur Container angezeigt, die dem Benutzer gehören, und es entstehen keine zusätzlichen Berechtigungen. Bestehende Cases und Holds werden **nicht** automatisch angepasst. Bereits seit Sommer kann eDiscovery Premium Loop- und Copilot-Pages-Dateien beim Export oder im Review Set in HTML umwandeln – vorher bekam man ein Dateiformat, mit dem kein Review-Tool etwas anfangen konnte.

Purview-Funktion	Status für Pages / Notebooks	Was das in der Praxis heißt
eDiscovery Suche & Export	unterstützt	Review und HTML-Export erfordern eDiscovery Premium (E5)
Legal Hold	unterstützt	Container muss explizit gewählt werden, ab Oktober per Picker
Aufbewahrungsrichtlinien	über „All SharePoint Sites“	Gilt für alle Containertypen – auch für Gruppen und Mandant
Aufbewahrungslabels	eingeschränkt	Manuell nur über die Loop-App, keine Record-Labels von Hand
Vertraulichkeitslabels	nur Copilot Pages	Notebooks haben kein Container-Label
DLP	unterstützt	Inklusive Policy Tips für den Benutzer
Information Barriers	nicht unterstützt	Bei IB-Pflicht: Pages und Notebooks per Cloud Policy abschalten
Papierkorb (Notebooks)	nicht vorhanden	Gelöschte Notebooks sind nicht wiederherstellbar

⚠ **WARNUNG: Der Hold, der keiner war**

Ein Litigation Hold auf den Benutzer erfasst den Copilot-Container nicht automatisch – anders als OneDrive. Und alte Holds werden durch das Oktober-Update auch nicht nachträglich erweitert. Wenn du jetzt laufende Verfahren hast, geh sie durch. Heute. Nicht nach der Weihnachtsfeier.

Archivierung auf Dateiebene: Copilot lernt vergessen

Bisher konntest du in SharePoint nur ganze Sites archivieren. Jetzt geht es pro Datei. Archivierte Dateien bleiben unter Aufbewahrung und Legal Hold, bleiben in eDiscovery auffindbar und behalten alle Versionen – fallen aber aus dem Microsoft-365-Copilot-Index, bis jemand sie reaktiviert. Lesen geht erst nach der Reaktivierung, die selbst keine Gebühr kostet. Der Hintergrund ist doppelt: Speicherkosten senken und Copilot vom Datenfriedhof fernhalten. Wer schon einmal erlebt hat, wie Copilot eine Preisliste von 2019 als „aktuelles Angebot“ zusammenfasst, versteht den Charme.

Der Haken steckt im Kleingedruckten: Sobald SharePoint Archive aktiv ist, ist die Dateiarchivierung für **alle Sites** eingeschaltet, und jeder Benutzer mit Bearbeitungsrechten darf archivieren. Abschalten kannst du sie pro Mandant oder pro Site per PowerShell. Archivspeicher wird gemessen und ist günstiger als Standardspeicher, die Site-Speichernutzung sinkt aber nicht. Zusätzlich bekommt Data Lifecycle Management eine Archive-Aktion in Aufbewahrungsrichtlinien – die ist standardmäßig aus und muss bewusst konfiguriert werden.

Zum Hintergrund der Kosten: Microsoft 365 Archive ist ein verbrauchsbasierter Dienst. Die Archivierung ganzer Sites setzt ein Azure-Pay-as-you-go-Abonnement voraus, abgerechnet wird der Archivspeicher separat. Das ist günstiger als zusätzliches SharePoint-Kontingent, aber eben eine zweite Rechnung, die irgendwer lesen muss. Erfahrungsgemäß liest sie niemand, bis der Controller mit der Frage vor der Tür steht, wer eigentlich „M365 Archive“ ist und warum der so viel Hunger hat.

Lebenszyklus einer SharePoint-Datei mit Dateiarchivierung

Was Copilot sieht, was eDiscovery sieht – und wer zahlt

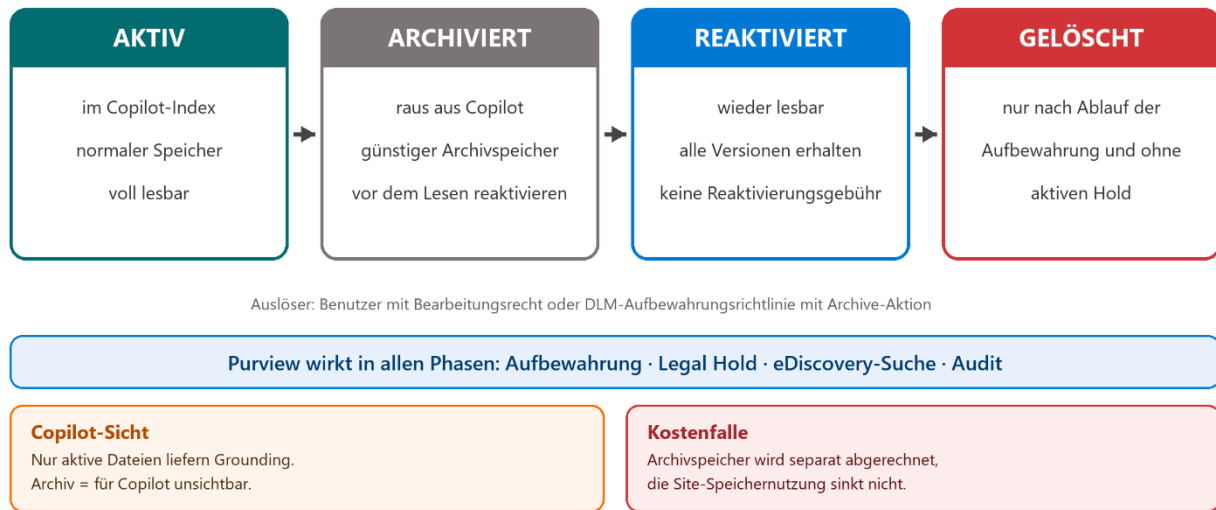


Abbildung 2: Lebenszyklus einer Datei mit Dateiarchivierung – Copilot-Sicht und Compliance-Sicht

Der Rest des Oktober-Pakets

Neben dem Copilot-Thema schiebt Microsoft eine ganze Reihe von Neuerungen in die allgemeine Verfügbarkeit. Die spannendste ist Network Data Security: Über Entra Global Secure Access prüft Purview Texte, Dateien und KI-Interaktionen direkt auf Netzwerkebene – also auch dort, wo kein Microsoft-Client mitspielt. Der Rest ist eher Kleingedrucktes, das aber genau in dem Moment wichtig wird, in dem ein Auditor danach fragt.

Neuerung	Kernfakten	Pferdefuß
Network Data Security (GA)	DLP und Insider Risk auf Netzwerkebene, über 35.000 Apps inkl. ChatGPT, Gemini, Claude	Nur Audit oder Block; 4 MB Text / 3 MB Datei; gilt nicht für B2B-Gäste; E5/E7 plus Entra Internet Access
Claude Enterprise	eDiscovery, Lifecycle, Insider Risk, Communication Compliance, Audit	Keine Labels, keine DLP – Erkennung statt Prävention; Pay-as-you-go nötig
Teams-Chats über Mandanten	DLP greift beim Mandanten, der die Unterhaltung initiiert	Deine Richtlinien schweigen, wenn der Partner hostet
Auto-Labeling	Simulation für bis zu 20 Mio. Elemente und 50.000 Sites	Simulation ist noch kein Rollout
eDiscovery-PowerShell	Keine App-only-Authentifizierung	Automatisierung auf Microsoft Graph umbauen
Endpoint DLP macOS 27	Preview, Client ab 101.26072	Ohne Gerätekontrolle- und Datenzugriffsrecht stiller Schutzverlust

Was sind Chancen? Was sind Risiken?

Die gute Nachricht: Copilot-Inhalte werden endlich so behandelt wie alles andere, was ein Unternehmen vor Gericht bringen oder retten kann. Die schlechte: Bis der Prozess sitzt, hast du

eine Lücke, die nicht im Dashboard blinkt. Purview meldet dir nämlich nicht, dass ein Hold unvollständig ist. Es lässt dich in dem Glauben – wie ein höflicher Bestatter.

Chancen	Risiken
Vollständige Holds ohne URL-Basterei und Admin-Tickets	Bestehende Holds bleiben lückenhaft, bis sie jemand anfasst
HTML-Export macht Pages und Loop endlich prüfbar	Review und HTML-Export nur mit eDiscovery Premium
Archiv entlastet Copilot von Altlasten, Antworten werden relevanter	Jeder mit Bearbeitungsrecht archiviert – auch das, was Copilot braucht
Günstigerer Speicher für Inaktives	Verbrauchskosten ohne Budgetalarm laufen still davon
DSGVO-Auskünfte decken KI-Inhalte mit ab	Keine Information Barriers, kein Notebook-Papierkorb

Praxisbeispiel Nummer zwei, eine Kanzlei mit Chinese-Wall-Pflicht: Information Barriers sauber konfiguriert, Copilot Pages munter im Einsatz. Dass SharePoint Embedded keine Information Barriers kennt, fiel erst auf, als ein Associate eine Page der „anderen Seite“ in der Freigabeliste fand. Die Lösung war unspektakulär: Pages und Notebooks per Cloud Policy für die betroffenen Teams abschalten. Der Schreck war spektakulärer.

Und dann ist da noch der mandantenübergreifende Teams-Chat. DLP setzt der Mandant durch, der die Unterhaltung gestartet hat. Lädt dich also der Generalunternehmer in seinen Chat ein, gelten seine Regeln, nicht deine. Ein Bauzulieferer hat so erlebt, wie sein Projektteam fröhlich Kalkulationen in einen fremden Mandanten postete, während die eigene DLP-Richtlinie danebensaß wie ein Türsteher vor der falschen Disco. Das ist kein Fehler, sondern dokumentiertes Verhalten – aber eines, das du in Schulungen und Richtlinien ausdrücklich erwähnen solltest.

! WICHTIG: Claude ist kein Purview-Mitglied zweiter Klasse – sondern dritter

Für Claude Enterprise bekommst du Erkennung und Untersuchung, aber keine Labels und keine DLP. Wer Claude freigibt, dokumentiert die Risikoakzeptanz schriftlich. Sonst schreibt sie später jemand anderes für dich – im Auditbericht.

Was müssen wir jetzt schon vorbereiten?

Der Rollout passiert ohne dein Zutun – Microsoft verlangt ausdrücklich keine Admin-Aktion. Genau das ist das Problem: Neue Möglichkeiten nützen nichts, wenn alte Verfahren und Prozessbeschreibungen sie ignorieren. Die eigentliche Arbeit liegt deshalb nicht im Purview-Portal, sondern bei Rechtsabteilung, Datenschutz und Records Management.

Fahrplan 2026: vom Kellerfund zur Standardquelle

Purview-Meilensteine rund um Copilot Pages, Notebooks und Archivierung

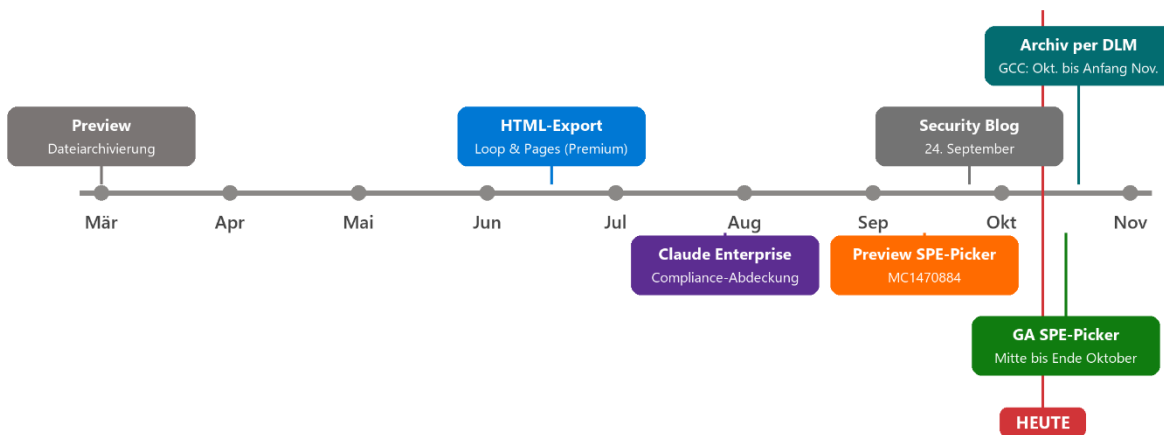


Abbildung 3: Fahrplan 2026 – Meilensteine und der heutige Stand

1. **Laufende Holds prüfen:** Für jeden Custodian den SPE-Container ergänzen. Bis der Picker in deinem Mandanten da ist, die Container-URL per PowerShell oder SharePoint Admin Center holen.
2. **Aufbewahrungsplan erweitern:** Copilot Pages, Notebooks und Loop ausdrücklich benennen, inklusive der Frage, wie Holds auf Versionen wirken. „Steckt ja in All SharePoint Sites“ ist keine Dokumentation, sondern eine Ausrede.
3. **Archivierung vor dem Einschalten regeln:** Festlegen, welche Sites Dateiarchivierung nutzen dürfen, bevor die Benutzer es selbst herausfinden. Den Rest per PowerShell sperren.
4. **Kosten unter Aufsicht stellen:** Archive, Claude, On-Demand-Klassifizierung und Network Data Security brauchen Budgets, Alarme und einen namentlich Verantwortlichen.
5. **Austrittsprozess anpassen:** Verlässt jemand das Unternehmen, folgt der Container dem OneDrive-Löschzyklus – mit einem manuellen Übergabeschritt. Vorher exportieren oder in eine Aufbewahrungsrichtlinie nehmen.
6. **Automatisierung umbauen:** eDiscovery-Skripte mit App-only-Anmeldung auf Microsoft Graph migrieren.

✓ TIPP: Der Zehn-Minuten-Test

Leg dir eine Testperson an, lass sie eine Copilot Page und ein Notebook anlegen, setz einen Hold und lösche dann beides. Findet eDiscovery die Inhalte in der Preservation Hold Library? Glückwunsch. Wenn nicht, hast du gerade das teuerste Learning des Jahres für zehn Minuten Arbeit bekommen.

Unterm Strich: Der Oktober macht Copilot-Inhalte compliance-fähig, aber nicht von allein compliant. Wer jetzt Holds nachzieht, Aufbewahrungspläne ergänzt und die Archivierung bewusst steuert, hat im nächsten Verfahren eine langweilige Woche. Und langweilige Wochen sind in der Compliance das Höchste, was man erreichen kann.

Häufig gestellte Fragen

Erfasst ein Litigation Hold automatisch Copilot Pages und Copilot Notebooks eines Benutzers?

Nein. Anders als OneDrive muss der benutzereigene SharePoint-Embedded-Container ausdrücklich als Datenquelle zum Hold hinzugefügt werden. Ab Mitte Oktober 2026 geht das direkt im eDiscovery-Datenquellen-Picker, vorher nur über die manuell ermittelte Container-URL.

Welche Lizenz brauche ich, um Copilot Pages in Purview eDiscovery zu prüfen und zu exportieren?

Suche und Sammlung funktionieren mit den Standardfunktionen von eDiscovery. Für Review Sets und den HTML-Export von Loop- und Copilot-Pages-Dateien ist eDiscovery Premium nötig, also typischerweise Microsoft 365 E5.

Findet Microsoft 365 Copilot noch archivierte SharePoint-Dateien?

Nein. Archivierte Dateien werden aus dem Copilot-Index entfernt und fließen nicht mehr in Antworten ein. Für eDiscovery, Aufbewahrung und Legal Hold bleiben sie dagegen vollständig erhalten und auffindbar.

Kann man gelöschte Copilot Notebooks wiederherstellen?

Endbenutzer und Administratoren können einzeln gelöschte Notebooks derzeit nicht wiederherstellen, weil es keinen Papierkorb für Notebooks gibt. Schutz bieten nur eine Aufbewahrungsrichtlinie oder ein Hold, der vor dem Löschen greift.

Gelten Aufbewahrungsrichtlinien automatisch für Copilot Pages und Loop?

Ja, sofern die Richtlinie für „All SharePoint Sites“ konfiguriert ist; dieser Bereich umfasst alle SharePoint-Embedded-Container von Copilot Pages, Notebooks und Loop. Richtlinien, die nur ausgewählte Sites abdecken, greifen dort nicht.