

Copilot an der Hochschule: Lizenz, Oversharing und die Frage, wer ihn überhaupt bekommt

Microsoft 365 · Hochschule und Forschung · Copilot

Copilot an der Hochschule: Lizenz, Oversharing und die Frage, wer ihn überhaupt bekommt

Copilot findet alles, was Sie freigegeben haben. Auch das, was Sie vergessen haben.

Copilot Chat Add-on-Lizenz Jeder außer externen Benutzern Berufungsakten Prüfungsdaten

Oversharing-Prüfung Pilot Personalrat

boddenberg.de

WISSEN

Alle Beiträge der Serie zu Microsoft 365 in Hochschule und Forschung an einem Ort.

› [Microsoft 365 in Hochschule und Forschung](#)

BERATUNG

Copilot- und Oversharing-Überprüfung für Ihren Hochschul-Tenant: Berechtigungslage, Sofortschutz, Pilotplanung, Vorlage fürs Präsidium.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Hochschulrechenzentrum, Site-Besitzer und Pilotgruppen: Purview, SharePoint Advanced Management und Copilot im Alltag.

› [Schulungen für Hochschulen und Forschung](#)

Irgendwann in diesem Semester kommt die Mail aus dem Präsidium. Sie ist kurz, freundlich und enthält das Wort „Copilot“. Meist auch die Wörter „zeitnah“, „Pilot“ und „die anderen Hochschulen machen das doch auch“. Im Hochschulrechenzentrum weiß man in diesem Moment zwei Dinge: Erstens wird das Thema nicht wieder weggehen. Zweitens hat niemand eine Ahnung, was eigentlich alles in den rund viertausend Teams und Sites steht, die seit der Pandemie entstanden sind. Copilot wird es herausfinden. Schneller als Sie.

Das ist der eigentliche Punkt dieses Beitrags. Die Lizenzfrage ist lösbar, die Technik ist es auch. Das Risiko liegt woanders: in jahrelang zu weit geteilten Sites, Teams und Ordnern, in denen Berufungsunterlagen, Prüfungsdaten und Personalvorgänge liegen, auf die formal die halbe Hochschule zugreifen darf. Bisher hat das niemand gemerkt, weil niemand danach gesucht hat. Copilot sucht. Er ist dabei nicht böswillig, nur gründlich. Das ist schlimmer.

Dieser Beitrag gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#). Er richtet sich an Leitungen von Hochschulrechenzentren, CIOs, Kanzlerinnen und Kanzler, die Dezernate der Verwaltung, Datenschutzbeauftragte und Personalräte sowie an IT- und Verwaltungsleitungen außeruniversitärer Forschungseinrichtungen. Er klärt, was Microsoft im Education-Bereich derzeit anbietet und für wen, warum die Berechtigungslage vor jeder Lizenzbestellung kommt und in welcher Reihenfolge Sie vorgehen sollten. Universitätsklinika mit ihren eigenen Regeln für Gesundheitsdaten bleiben außen vor, Schulen ohnehin.

FAKTEN · Das Wichtigste in Kürze

Microsoft Copilot Chat steht Personal und Studenten mit Microsoft 365 A1, A3 oder A5

(einschließlich Student Use Benefit) ohne Aufpreis zur Verfügung, sofern sie sich mit dem Hochschulkonto anmelden. Für Studenten ab 13 Jahren verlangt Microsoft zusätzliche Verwaltungsschritte.

Das kostenpflichtige Add-on, das Microsoft inzwischen schlicht „Microsoft Copilot“ nennt (bisher Microsoft 365 Copilot), gibt es als akademisches Angebot für Mitarbeiterinnen und Mitarbeiter, Lehrpersonal und Studenten ab 13 Jahren, bezogen über EES oder einen CSP-Partner.

Copilot sieht nur, was die angemeldete Person ohnehin sehen darf. Genau das ist das Problem, wenn diese Rechte seit Jahren zu weit gefasst sind.

Reihenfolge: Berechtigungslage prüfen, dann pilotieren, dann ausrollen. Der Personalrat gehört von Anfang an dazu, nicht erst zum Rollout.

Was es gibt und wer es bekommt: Copilot Chat, Add-on und die Lizenzfrage

Bevor es ernst wird, eine kleine Begriffsklärung, denn Microsoft hat die Produkte mal wieder umbenannt. Was Sie als „Microsoft 365 Copilot“ kennen, heißt in der aktuellen Dokumentation „Microsoft Copilot“; aus „Microsoft 365 Copilot Chat“ wurde „Microsoft Copilot Chat“. Gemeint ist dasselbe. Wer in Gremienvorlagen trotzdem den alten Namen verwendet, liegt nicht falsch, nur ein Jahr hinterher. In der Hochschulpraxis also völlig normal.

Copilot Chat: schon da, ob Sie wollen oder nicht

Copilot Chat ist die Grundstufe. Laut Microsoft steht er ohne zusätzliche Kosten allen Personen zur Verfügung, die sich mit einem Entra-Konto anmelden und einen berechtigten Plan haben. Im Education-Bereich sind das Microsoft 365 A1, A3 und A5, ausdrücklich einschließlich der Varianten für Studenten, für Lehrpersonal und des Student Use Benefit, außerdem Office 365 A1, A1 Plus, A3 und A5. Copilot Chat arbeitet mit dem Web, mit hochgeladenen Dateien und mit dem Dokument, das gerade in Word, Excel oder PowerPoint offen ist. Er durchsucht aber nicht von sich aus Ihren Tenant. Das Postfach der Kanzlerin bleibt für ihn so verschlossen wie bisher.

Wichtig für die Planung: Copilot Chat ist standardmäßig in den Microsoft-365-Apps angeheftet. Das Lösen dieser Anheftung entfernt den Zugang nicht, Copilot Chat bleibt über die Copilot-App erreichbar. Wer ihn für bestimmte Gruppen wirklich sperren will, nutzt die Zugriffssteuerung im Microsoft 365 Admin Center, die laut Dokumentation für alle Benutzer oder gezielt für Benutzer und Gruppen greift. Für Mandanten mit Hauptstandort im EWR steuert die Anheft-Einstellung die Copilot-App seit Juli 2025 ohnehin nicht mehr. Wer also glaubt, mit einem Häkchen sei das Thema vom Tisch, darf sich auf überraschte Gesichter einstellen. Vor allem auf das eigene.

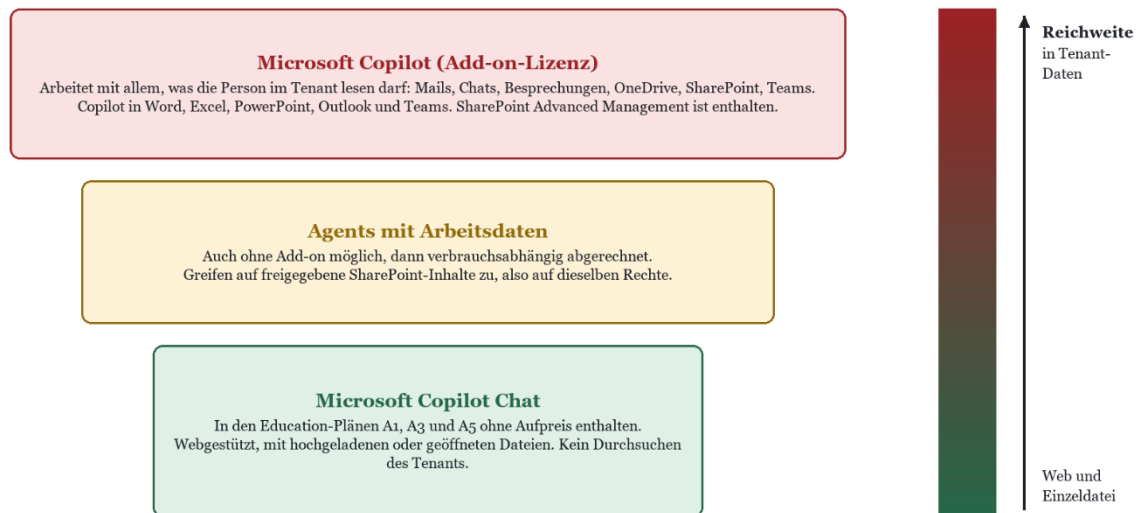
Das Add-on: Copilot mit Zugriff auf den Tenant

Die Add-on-Lizenz ist die Stufe, um die es in diesem Beitrag eigentlich geht. Erst sie erlaubt es Copilot, im Namen der Person auf Mails, Kalender, Chats, Besprechungstranskripte, OneDrive und SharePoint zuzugreifen, und bringt Copilot in Word, Excel, PowerPoint, Outlook und Teams. Microsoft bietet sie im akademischen Umfeld für Mitarbeiterinnen und Mitarbeiter, Lehrpersonal und Studenten ab 13 Jahren an. Als Voraussetzung nennt die aktuelle Dokumentation unter anderem Microsoft 365 A1, A3 und A5 sowie Office 365 A1, A3 und A5; bezogen wird über Enrollment for Education Solutions oder einen Cloud Solution Provider. Wie sich das zu Ihrem bestehenden Vertrag verhält, klären die Beiträge [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#) und [Microsoft-Bundesvertrag für Hochschulen: EES, Beitritt und was man damit wirklich bekommt](#). Preise nennen wir bewusst nicht: Sie ändern sich schneller als die Geschäftsordnung des Senats.

Dazwischen liegt eine Grauzone, die gern übersehen wird: Agents. Auch Personen ohne Add-on können Agents nutzen, die auf Arbeitsdaten im Tenant zugreifen, etwa auf eine SharePoint-Site. Microsoft rechnet das dann verbrauchsabhängig ab. Für die Berechtigungsfrage ist das egal: Ein Agent auf einer zu weit geteilten Site findet genau dasselbe wie der lizenzierte Copilot.

Drei Ebenen, ein Name: was hinter „Copilot“ an der Hochschule steckt

Je mehr Tenant-Daten Copilot erreicht, desto stärker zählt die Berechtigungslage



Skizze 1: Copilot Chat ist schon da. Das Oversharing-Problem beginnt dort, wo Copilot den Tenant durchsuchen darf.

Merkmal	Copilot Chat	Copilot (Add-on)
Kosten	in berechtigten A-Plänen ohne Aufpreis	zusätzliche Lizenz je Person
Personengruppen	Personal; Studenten ab 13 mit Zusatzschritten	Personal, Lehrpersonal, Studenten ab 13
Datengrundlage	Web, hochgeladene und geöffnete Dateien	alles, worauf die Person im Tenant Zugriff hat
In den Office-Apps	Chat-Seitenleiste, Bezug auf offenes Dokument	voll integriert in Word, Excel, PowerPoint, Outlook, Teams
Agents mit Arbeitsdaten	möglich, verbrauchsabhängig	enthalten
SharePoint Advanced Management	nicht enthalten	laut Microsoft enthalten
Oversharing-Risiko	gering, solange keine Agents auf Sites zeigen	hoch, wenn Berechtigungen nicht bereinigt sind

Studenten: dürfen, sollen, müssen?

Für Studenten ist die Lage freundlicher, als viele denken. Copilot Chat steht ihnen mit der Hochschullizenz ohne Aufpreis zur Verfügung, mit dem Datenschutz-Schild der Unternehmensanmeldung statt mit dem privaten Konto. Das ist ein echtes Argument: Studenten nutzen generative KI ohnehin. Die Frage ist nur, ob sie das mit dem Hochschulkonto unter Ihren Regeln tun oder mit irgendeinem Privatkonto unter gar keinen. Die Add-on-Lizenz für alle Studenten ist dagegen an deutschen Hochschulen vor allem eine Haushaltsfrage, und die beantwortet sich bei fünfstelligen Immatrikulationszahlen meist von selbst.

WICHTIG · Frühstudium und Juniorstudium nicht vergessen

Microsoft verlangt für Studentenkonten zusätzliche Schritte, damit die Altersgrenze eingehalten wird; dazu gehört das Attribut ageGroup in Entra ID. An Hochschulen betrifft das vor allem Frühstudienten und Schüler im Juniorstudium, die noch nicht volljährig sind. Sorgen Sie dafür, dass das Campus-Management diese Information liefert und der Identity Lifecycle sie korrekt in Entra ID schreibt. Wie das an der Hochschule funktioniert, zeigt der Beitrag:

[Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#)

Der eigentliche Risikofaktor: zehn Jahre „Jeder außer externen Benutzern“

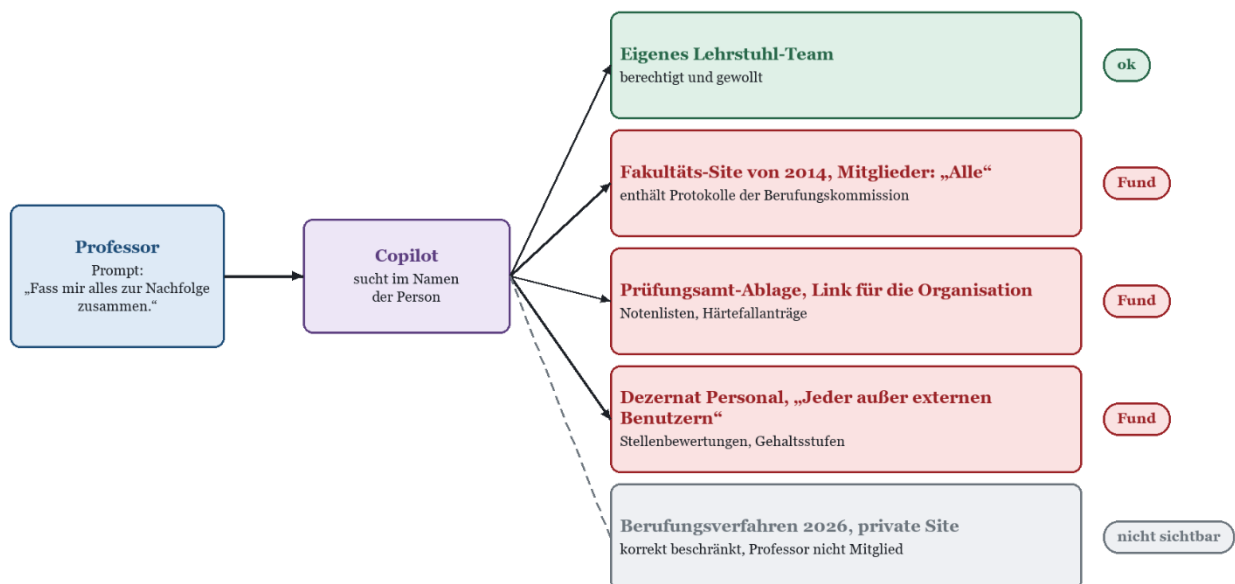
Microsoft wird nicht müde zu betonen, dass Copilot nur auf Daten zugreift, die die jeweilige Person ohnehin sehen darf. Das stimmt. Es ist auch genau der Satz, bei dem erfahrene Rechenzentrumsleute anfangen, nervös mit dem Kugelschreiber zu klicken. Denn „sehen darf“ heißt in einem gewachsenen Hochschul-Tenant: alles, was irgendwann irgendwer mit zu weiten Rechten versehen hat. Und das ist erfahrungsgemäß eine Menge.

Copilot erweitert keine Rechte, er macht sie benutzbar

Bisher schützte die Hochschule vor allem eines: Unauffindbarkeit. Wer die Fakultäts-Site von 2014 nicht kannte, fand die Protokolle der Berufungskommission darin auch nicht. Die Suche in SharePoint hätte sie zwar geliefert, aber wer sucht schon in SharePoint. Copilot ändert genau das. Er beantwortet eine harmlose Frage nach „allem zum Thema Nachfolge am Institut“ mit einer ordentlich gegliederten Zusammenfassung, gespeist aus Quellen, von deren Existenz die fragende Person bis dahin nichts wusste. Mit Quellenangabe. Hilfsbereit bis zur Selbstanzeige.

Copilot sieht, was die Person sehen darf. Nicht was sie sehen sollte.

Beispiel: ein Professor fragt nach „allem zum Thema Nachfolge am Institut“



Skizze 2: Copilot erweitert keine Rechte. Er macht vorhandene, zu weite Rechte nur endlich bequem benutzbar.

Wo es an Hochschulen typischerweise brennt

Die folgenden Fundorte sind keine Theorie. Sie tauchen in praktisch jedem gewachsenen Tenant auf, der eine öffentliche Verwaltung mit dezentralen Einheiten abbildet. An Hochschulen kommen die Gremienstruktur und die hohe Fluktuation noch obendrauf.

Fundort	Typischer Inhalt	Warum es zu weit offen ist
Kommissions-Teams im Berufungsverfahren	Bewerbungen, Gutachten, Listenplätze, Protokolle	Team als „öffentlich“ angelegt, Mitglieder nach Verfahrensende nie entfernt
Ablagen des Prüfungsamts	Notenlisten, Rücktritte, Atteste, Härtefallanträge	Ordner per Link „Personen in Ihrer Organisation“ geteilt, damit Prüfer schnell Zugriff haben
Dezernat Personal und Dekanatsverwaltung	Stellenbewertungen, Vertragsentwürfe, Verlängerungen nach WissZeitVG	Gruppe „Jeder außer externen Benutzern“ beim Einrichten als Abkürzung genutzt
Gremien-Sites (Senat, Fakultätsrat, Ausschüsse)	nichtöffentliche Beratungsunterlagen, Personalangelegenheiten	Unterlagen öffentlicher und nichtöffentlicher Sitzungen in derselben Bibliothek
Lehrstuhl-Sites nach Wechsel oder Emeritierung	Gutachten, Korrespondenz, Prüfungsunterlagen	Besitzer weg, Rechte bleiben, niemand fühlt sich zuständig
Pandemie-Teams	alles Mögliche, einschließlich Gesundheitsdaten	schnell angelegt, nie aufgeräumt, oft öffentlich
OneDrive-Freigaben	Entwürfe von Gutachten, Exceltabellen mit Studentendaten	Organisationsweite Links als bequeme Standardeinstellung

WARNUNG · Was Copilot findet, kann Copilot zitieren

Ein Copilot-Ergebnis ist eine neue Datei, eine Mail oder eine Chatnachricht. Wer eine Zusammenfassung aus einem offen herumliegenden Berufsprotokoll in ein Teams-Gespräch kopiert, hat aus einem passiven Berechtigungsfehler eine aktive Weitergabe gemacht. Für die betroffenen Bewerberinnen und Bewerber ist der Unterschied gleichgültig, für Ihre Datenschutzbeauftragte nicht.

Warum Hochschulen besonders betroffen sind

Hochschulen sind keine Unternehmen mit sauberer Linienorganisation. Sie sind ein Verbund aus Fakultäten, Instituten, Lehrstühlen, Zentralen Einrichtungen und Gremien, jeweils mit eigener IT-Kultur, gelegentlich mit eigenen Admins. Dazu kommt eine Fluktuation, die jedes Personalamt in der Wirtschaft in den Wahnsinn treiben würde: befristete wissenschaftliche Mitarbeiter, studentische Hilfskräfte im Semesterrhythmus, Gastwissenschaftler, Lehrbeauftragte und Emeriti, die alle irgendwann irgendwo Mitglied wurden und selten wieder entfernt. Wie das in der Organisation zusammenhängt, beschreibt der Beitrag [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#).

Die Freiheit von Forschung und Lehre verstärkt das. Kein Präsidium schreibt einem Lehrstuhl vor, wie er seine Team-Ablage zu organisieren hat, und das ist auch gut so. Es führt aber dazu, dass zentrale Vorgaben zu Freigaben oft als Empfehlung verstanden werden. Als sehr unverbindliche Empfehlung. Speicherpool, Lehrstuhlwechsel und die Frage, was mit Sites passiert, deren Besitzer längst an einer anderen Universität forscht, behandelt der Beitrag [SharePoint und OneDrive an der Hochschule: Speicherpool, Lehrstuhlwechsel und Exmatrikulation](#).

TYPISCHE SITUATION · Aus der Verwaltung auf die Hochschule übertragen

Bei einer Berechtigungsprüfung in einer Stadtverwaltung fand sich in der ersten Stunde eine Bibliothek des Personalamts mit Beurteilungen und Gehaltsunterlagen, freigegeben für die gesamte Organisation. Angelegt hatte sie ein inzwischen pensionierter Sachbearbeiter, damit „die Kollegen aus

der Außenstelle auch drankommen“. In einem kommunalen Verband war es ein Gremien-Team, in dem öffentliche und nichtöffentliche Vorlagen nebeneinander lagen, sichtbar für alle Mitglieder sämtlicher Ausschüsse. Übertragen auf die Hochschule ist das die typische Situation: das Personaldezernat mit dem Außenstandort, der Fakultätsrat mit seinen Kommissionen. Niemand hat dabei etwas Böses gewollt. Es hat nur niemand mehr hingeschaut.

Erst prüfen, dann pilotieren, dann ausrollen

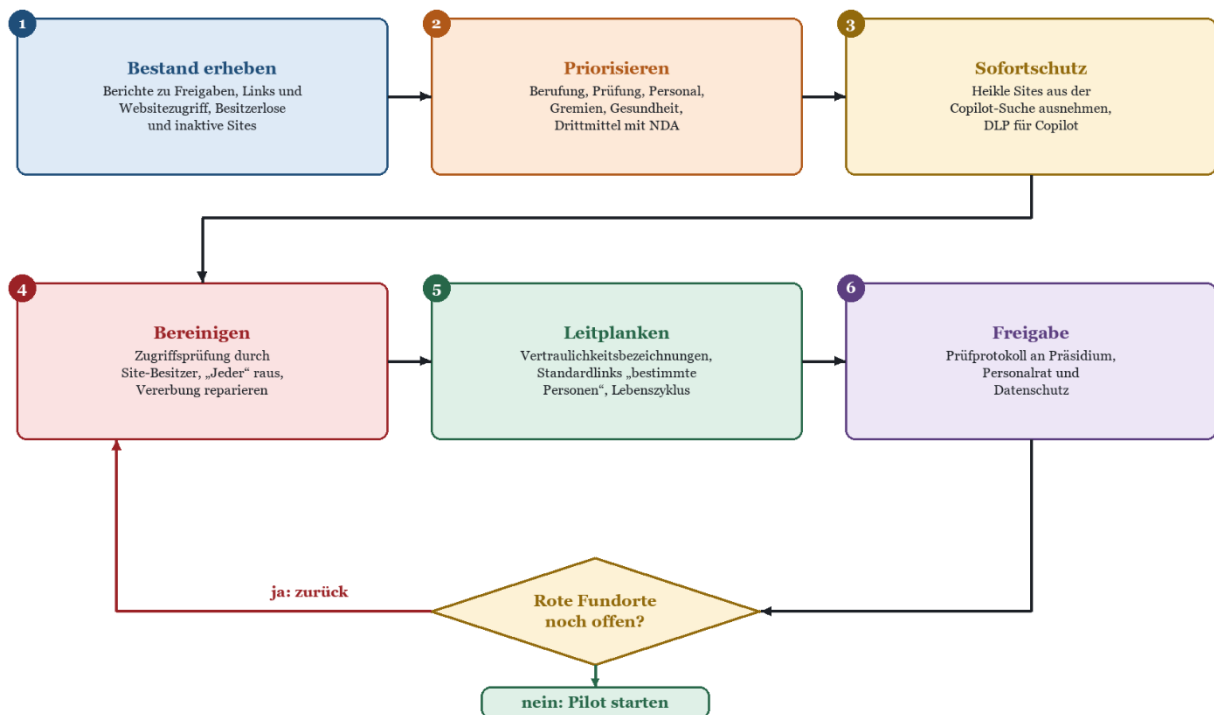
Die Reihenfolge ist nicht verhandelbar, auch wenn das Präsidium gern eine andere hätte. Ein Pilot auf einem unbereinigten Tenant ist kein Pilot, sondern ein Feldversuch mit echten Personaldaten. Microsoft empfiehlt in seinem eigenen Bereitstellungsleitfaden für eine sichere Datengrundlage dieselbe Abfolge: zuerst Oversharing beheben, dann Leitplanken setzen, dann regulatorische Anforderungen erfüllen. Selten sind sich Hersteller und skeptisches Rechenzentrum so einig.

Die Oversharing-Prüfung vor dem Piloten

Die Prüfung folgt sechs Schritten. Sie beginnt mit Zahlen statt mit Bauchgefühl, priorisiert nach Schutzbedarf und endet mit einem Tor, durch das der Pilot erst gehen darf, wenn die roten Fundorte geschlossen sind.

Oversharing-Prüfung vor dem Piloten

Sechs Schritte, ein Tor: kein Pilot, solange rote Fundorte offen sind



Skizze 3: Die Prüfung ist kein Projektabschnitt, der einmal abgehakt wird. Schritt 5 läuft danach dauerhaft weiter.

- **Bestand erheben.** Berichte zu Freigabelinks, zu Inhalten, die mit „Jeder“ oder „Jeder außer externen Benutzern“ geteilt sind, zu unterbrochener Vererbung sowie zu besitzerlosen und inaktiven Sites. Microsoft liefert dafür Datenrisikobewertungen in Purview und das Content Management Assessment in SharePoint Advanced Management.
- **Priorisieren.** Nicht jede offene Site ist ein Problem. Die Vorlesungsfolien der Einführungsveranstaltung dürfen gern auffindbar sein. Rot sind Berufungs-, Prüfungs- und Personalvorgänge, nichtöffentliche Gremienunterlagen, Gesundheitsdaten und Drittmittelprojekte mit Geheimhaltungsvereinbarung.

- **Sofortschutz.** Was nicht schnell bereinigt werden kann, wird vorübergehend aus der Copilot-Suche genommen. Microsoft nennt das Restricted Content Discovery; ergänzend kann eine DLP-Richtlinie für Copilot verhindern, dass Inhalte mit bestimmten Vertraulichkeitsbezeichnungen in Antworten einfließen. Beides ist Pflaster, keine Heilung.
- **Bereinigen.** Site-Besitzer prüfen ihre Zugriffe selbst, unterstützt durch Zugriffsüberprüfungen aus SharePoint Advanced Management. Organisationsweite Links und die Gruppe „Jeder außer externen Benutzern“ fliegen raus, unterbrochene Vererbung wird repariert, jede Site bekommt mindestens zwei verantwortliche Besitzer.
- **Leitplanken.** Standard-Freigabelink auf „bestimmte Personen“, Vertraulichkeitsbezeichnungen für Teams und Sites, Restricted Access Control für besonders schutzbedürftige Sites, Richtlinien für inaktive und besitzerlose Sites. Dieser Schritt hört nie auf.
- **Freigabe.** Ein kurzes Prüfprotokoll an Präsidium, Personalrat und Datenschutzbeauftragte: was gefunden, was behoben, was bewusst offen gelassen wurde und warum.

TIPP · Die Fundorte kennt meist nicht die IT, sondern die Verwaltung

Die Berichte zeigen, wo Rechte zu weit sind. Ob dort etwas Heikles liegt, wissen das Prüfungsamt, das Personaldezernat und die Geschäftsstelle des Senats besser als jedes Werkzeug. Holen Sie diese Stellen in Schritt 2 an den Tisch und fragen Sie konkret: Wo liegen bei Ihnen Unterlagen, die Sie keinem Kollegen aus einer anderen Fakultät zeigen würden? Die Antworten sind lehrreich und gelegentlich beunruhigend.

Werkzeuge: was Microsoft mitliefert und was es voraussetzt

Die gute Nachricht für skeptische Rechenzentren: Für die Prüfung brauchen Sie keine Drittanbieter-Suite, und vieles lässt sich auch mit PowerShell und eigenen Auswertungen abdecken, wenn Ihnen die Microsoft-Oberflächen zu bunt sind. Die weniger gute: Einige Komfortfunktionen hängen an Lizenzen, die nicht jede Hochschule flächendeckend hat. SharePoint Advanced Management ist laut Microsoft in der Copilot-Lizenz enthalten; für tenantweite Funktionen lohnt der Blick in die aktuelle Dokumentation, wie viele Copilot-Lizenzen dafür vorhanden sein müssen.

Werkzeug	Zweck in der Prüfung	Voraussetzung (Stand der Recherche)
Berichte zur Datenzugriffs-Governance (SAM)	offene Links, Freigaben an „Jeder“, sensible Inhalte nach Site	SharePoint Advanced Management
Content Management Assessment (SAM)	zu große Zielgruppen, unterbrochene Vererbung, inaktive und besitzerlose Sites	SharePoint Advanced Management
Site-Zugriffsüberprüfung (SAM)	Besitzer prüfen und bereinigen Zugriffe bis auf Dateiebene	SharePoint Advanced Management
Restricted Content Discovery	heikle Sites vorübergehend aus der Copilot-Suche nehmen	SharePoint Advanced Management
Restricted Access Control	Zugriff auf eine Site an eine Gruppe binden, unabhängig von Einzelfreigaben	SharePoint Advanced Management
Purview-Datenrisikobewertung (DSPM)	überteilte Sites mit sensiblen Inhalten erkennen	Purview; Umfang abhängig von A3 oder A5
DLP für Copilot	gelabelte Inhalte von Copilot-Antworten ausschließen	Purview DLP, Vertraulichkeitsbezeichnungen

Vertraulichkeitsbezeichnungen für Teams und Sites	Datenschutzeinstellung und Freigaben je Schutzklasse erzwingen	Purview Information Protection
--	--	--------------------------------

WEITERLESEN · Copilot- und Oversharing-Überprüfung für Ihren Tenant

Sie wollen wissen, was Copilot in Ihrem Tenant finden würde, bevor es die erste Pilotperson herausfindet? Wir prüfen die Berechtigungslage Ihres Hochschul- oder Institutstenants, priorisieren die Fundorte gemeinsam mit Verwaltung und Datenschutz, setzen den Sofortschutz und liefern Pilotplan und Entscheidungsvorlage für das Präsidium. Ohne Marketingfolien, mit Protokoll.

› [Microsoft-365-Beratung für Hochschulen und Forschung](#)

Der Pilot: klein, gemischt, ehrlich

Ein guter Pilot ist nicht die Liste der Personen, die am lautesten gefragt haben. Er ist eine bewusst gemischte Gruppe: einige Personen aus den Dezernaten, die täglich mit Vorlagen und Mails ringen, einige wissenschaftliche Mitarbeiter und Professoren aus unterschiedlichen Fakultäten, ein Dekanat, das Hochschulrechenzentrum selbst und mindestens eine Person, die Copilot kritisch sieht. Letztere ist kein Störfaktor, sondern Ihr bestes Messinstrument.

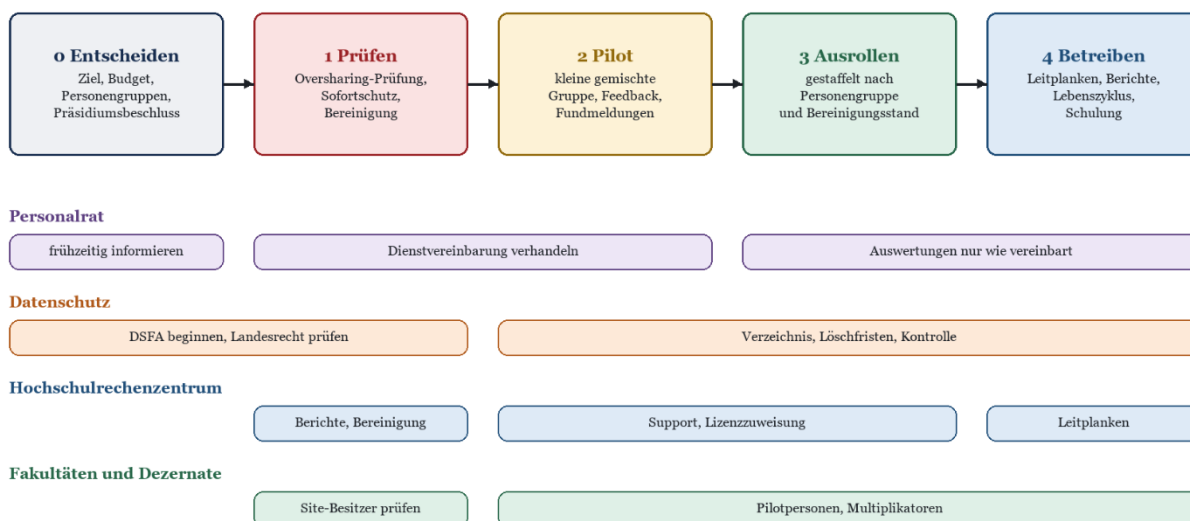
Zum Pilot gehört ein klarer Meldeweg: Wer in einer Copilot-Antwort Inhalte sieht, die er nicht sehen sollte, meldet das, ohne dass daraus ein Vorwurf wird. Jede solche Meldung ist ein gefundener Berechtigungsfehler, den sonst später jemand mit weniger guten Absichten gefunden hätte. Sammeln Sie außerdem, wofür Copilot tatsächlich genutzt wird. Die ehrliche Antwort lautet oft: Besprechungen zusammenfassen, Mails entschärfen, Vorlagen umformulieren. Das ist nicht spektakulär, aber es ist die Grundlage für die Frage, wer die Lizenz wirklich braucht.

Der Rollout: gestaffelt nach Personengruppen

Nach dem Pilot wird nicht „ausgerollt“, sondern erweitert: Personengruppe für Personengruppe, jeweils dann, wenn deren Bereiche bereinigt sind. Das Dezernat, dessen Ablage noch auf der roten Liste steht, wartet. Das ist unpopulär, aber einfacher zu erklären als eine Datenpanne im Berufungsverfahren.

Erst prüfen, dann pilotieren, dann ausrollen

Phasen mit festen Toren, daneben die Beteiligten, die nicht erst am Ende gefragt werden



Skizze 4: Wer erst in Phase 3 mit dem Personalrat spricht, plant Phase 3 zweimal.

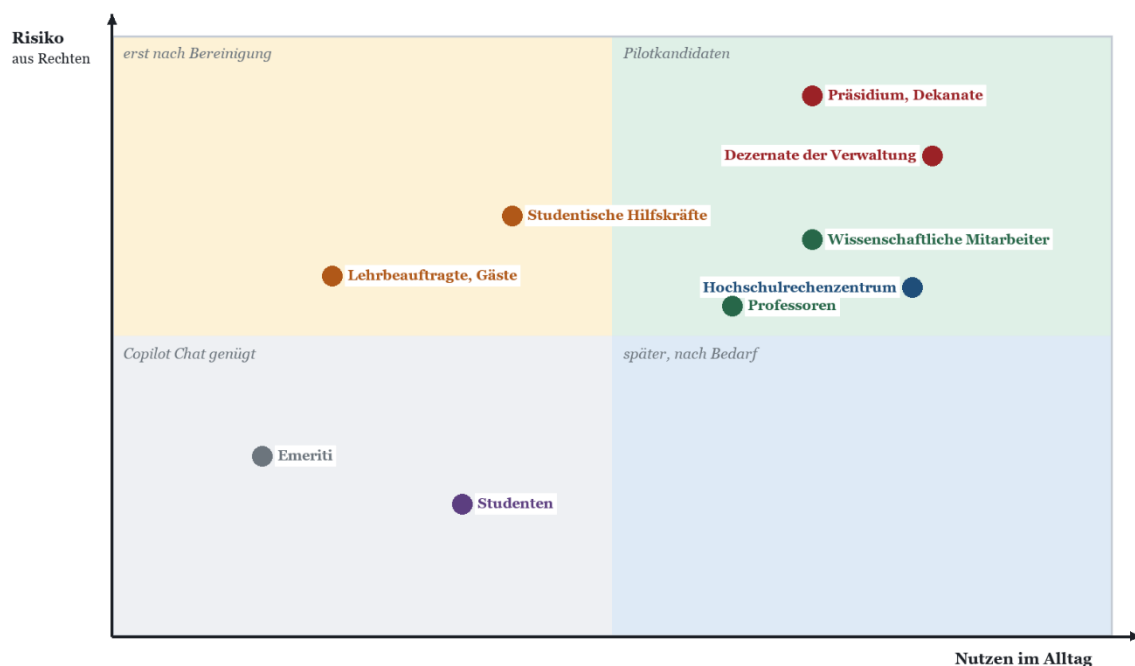
Wer ihn überhaupt bekommt: Personengruppen im Vergleich

Die Lizenzfrage ist an Hochschulen keine Frage der Hierarchie, auch wenn sie gern so behandelt wird. Nicht jede Person mit Lehrstuhl braucht Copilot, und nicht jede Sachbearbeiterin ohne ihn kommt gut zurecht. Entscheidend sind drei Fragen: Wie viel Routine-Text, Mail und Besprechung fällt an? Auf welche Datenbestände hat die Gruppe Zugriff? Und wie stabil sind diese Zugriffe über die Zeit?

Personengruppe	Nutzen	Risiko	Empfehlung
Präsidium, Rektorat, Kanzler	hoch: Vorlagen, Gremienunterlagen, Korrespondenz	sehr hoch: Zugriff auf Personal-, Berufungs- und Gremienvorgänge	nach Bereinigung früh, mit gezielt geschützten Bereichen
Dezernate der Verwaltung	sehr hoch: Mails, Vorlagen, Besprechungen, Auswertungen	hoch: Personal, Haushalt, Prüfungsamt	Pilotkern, aber erst nach Bereinigung der eigenen Ablagen
Dekanate, Fakultätsverwaltung	hoch: Berufungen, Studienorganisation	hoch: Berufungs- und Prüfungsvorgänge	mit Dezernaten gemeinsam, gleiche Voraussetzungen
Hochschulrechenzentrum	hoch: Dokumentation, Skripte, Tickets	mittel bis hoch: Admin-Konten nie mit Copilot	in den Pilot, nur mit Standardkonten
Professoren	mittel bis hoch: Gutachten, Anträge, Korrespondenz	mittel: Gremien- und Kommissionsmitgliedschaften	nach Bedarf und Bereinigungsstand, nicht pauschal
Wissenschaftliche Mitarbeiter	hoch: Anträge, Literatur, Projektverwaltung	mittel: Projektdaten, eventuell NDA	gute Pilotgruppe, Drittmittel mit Geheimhaltung beachten
Studentische Hilfskräfte	mittel	hoch: oft Zugriff auf Verwaltungsablagen ohne passende Rollen	zunächst Copilot Chat; Zugriffe vorher prüfen
Lehrbeauftragte, Gastwissenschaftler	gering bis mittel	hoch: Konten selten sauber befristet	Copilot Chat; Add-on nur im Einzelfall
Emeriti	gering	mittel: Altzugriffe aus aktiver Zeit	Copilot Chat genügt
Studenten	mittel, vor allem beim Lernen und Schreiben	gering bis mittel, abhängig von Kursteams und Freigaben	Copilot Chat mit Hochschulkonto, Add-on nur in Sonderfällen

Wer bekommt die Add-on-Lizenz zuerst?

Nutzen gegen Risiko aus der Berechtigungslage, typische Einschätzung vor der Bereinigung



Skizze 5: Die Verwaltung profitiert am meisten und sitzt zugleich auf den heikelsten Daten. Genau deshalb kommt die Prüfung zuerst.

Verwaltung und Präsidium

Die Verwaltung ist der Bereich mit dem größten messbaren Nutzen: viel Text, viele Besprechungen, viele Vorlagen, die immer wieder ähnlich aussehen. Sie ist zugleich der Bereich, der auf den heikelsten Daten sitzt. Das ist kein Grund, sie auszuschließen, sondern einer, gerade hier mit der Bereinigung anzufangen. Ein Personaldezernat, dessen Ablagen sauber sind, ist der beste Beweis, dass Copilot an Ihrer Hochschule funktioniert.

Wissenschaft

In Lehrstühlen und Instituten ist der Nutzen sehr unterschiedlich verteilt. Manche Professoren werden Copilot nach einer Woche nicht mehr hergeben, andere nach einer Woche zurückgeben. Lizenzen hier nach Bedarf zu vergeben, ist wirtschaftlich sinnvoll und organisatorisch anstrengend. Ein einfaches Antragsverfahren über das Dekanat, kombiniert mit einer Rückgabe bei Nichtnutzung, hat sich in der öffentlichen Verwaltung bewährt. Besondere Vorsicht gilt bei Drittmittelprojekten mit Geheimhaltungsvereinbarung oder exportkontrollrelevanten Inhalten; wie man die schützt, steht im Beitrag [Exportkontrolle und vertrauliche Drittmittelprojekte: Sensitivity Labels und DLP in der Forschung](#).

Studenten, Hilfskräfte und Gäste

Studentische Hilfskräfte sind der unterschätzte Risikofaktor: Sie arbeiten häufig in Verwaltungsbereichen, werden schnell in Teams aufgenommen und selten wieder entfernt. Gäste, Lehrbeauftragte und Emeriti haben oft Konten, deren Befristung niemand pflegt. Für alle diese Gruppen gilt: Erst die Konten und Mitgliedschaften sauber führen, dann über mehr als Copilot Chat nachdenken. Wie Sonderrollen in Entra ID abgebildet werden, beschreibt der Beitrag [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#); was sich in einem Tenant nach Jahren an verwaisten Konten findet, zeigt [Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet](#).

Ein Wort zu Prüfungsrecht und KI in der Lehre, weil die Frage im Senat garantiert kommt: Ob und wie Studenten KI in Hausarbeiten und Prüfungen nutzen dürfen, regeln Prüfungsordnungen, Fakultäten und die Hochschuldidaktik, nicht das Rechenzentrum. Die Bereitstellung von Copilot

Chat verändert diese Frage nicht grundsätzlich, denn generative KI ist für Studenten ohnehin frei verfügbar. Sie verschiebt nur, unter welchen Datenschutzbedingungen die Nutzung stattfindet. Dieser Beitrag lässt das Thema bewusst bei denen, die dafür zuständig sind.

Personalrat, Datenschutz und das Kleingedruckte

Personalrat früh einbinden

Copilot ist aus Sicht der Personalvertretung kein neutrales Schreibwerkzeug. Die Werkzeuge rund um Copilot können Nutzung auswerten: Berichte im Admin Center zeigen aktive Nutzer und Prompt-Zahlen, der Aktivitäts-Explorer in Purview kann Copilot-Interaktionen einschließlich Prompts und Antworten sichtbar machen, Besprechungstranskripte halten fest, wer was gesagt hat. Damit ist der Bereich der technischen Einrichtungen berührt, die geeignet sind, Verhalten oder Leistung zu überwachen, und damit in allen Ländern die Mitbestimmung, wenn auch mit unterschiedlicher Reichweite.

Die Landespersonalvertretungsgesetze unterscheiden sich hier spürbar. Das gilt besonders für das wissenschaftliche Personal: Ob und wie weit der Personalrat für Professoren, wissenschaftliche Mitarbeiter oder studentische Hilfskräfte zuständig ist, regelt jedes Land anders, teils mit Antragserfordernis, teils mit eigenen Vertretungen. Klären Sie das am Anfang, nicht nach dem Pilot. Was in eine Dienstvereinbarung zu Microsoft 365 gehört und wie man mit der Verhaltenskontrolle umgeht, behandelt ausführlich der Beitrag [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#).

TIPP · Regelungspunkte für die Dienstvereinbarung zu Copilot

Zweck und Personengruppen der Einführung; Freiwilligkeit oder Verpflichtung der Nutzung.

Ausschluss von Leistungs- und Verhaltenskontrolle auf Basis von Copilot-Prompts, Nutzungsberichten und Transkripten; Zugriff auf Purview-Auswertungen nur im Vier-Augen-Prinzip und für festgelegte Anlässe.

Regeln für Transkription und Zusammenfassung in Besprechungen, insbesondere in Gremien und Personalgesprächen.

Aufbewahrung und Löschung von Copilot-Interaktionen.

Schulungsanspruch und Ansprechpartner; Verfahren bei gemeldeten Fehlzugriffen.

Datenschutz und Landesrecht

Für den Datenschutz ändert Copilot weniger an der Grundsatzfrage zu Microsoft 365 als an der Praxis. Neu sind die Copilot-Interaktionen selbst, die Microsoft als Inhalte im Tenant speichert, und die Frage, welche Daten in Antworten einfließen dürfen. Eine Datenschutz-Folgenabschätzung ist bei einem hochschulweiten Einsatz naheliegend; welche Anforderungen dabei gelten, hängt vom jeweiligen Landesdatenschutzgesetz und von der Haltung Ihrer Landesaufsicht ab, die sich zwischen den Ländern unterscheiden kann. Die übergeordnete Debatte zu DSK, Landesaufsicht und Hochschulalltag führt der Beitrag [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#).

Praktisch hilft eine einfache Regel: Alles, was Sie nicht in einer Copilot-Antwort sehen wollen, braucht eine Vertraulichkeitsbezeichnung und eine passende DLP-Regel, oder es gehört gar nicht in den regulären Tenant. Ebenso gilt: Websuche lässt sich per Richtlinie für Gruppen steuern, wenn Sie verhindern wollen, dass Suchanfragen aus heiklen Bereichen den Tenant verlassen.

HINWEIS · Keine Rechtsberatung

Hochschulgesetze, Landesdatenschutzgesetze und Personalvertretungsgesetze unterscheiden sich je Bundesland, ebenso die Positionen der Aufsichtsbehörden. Dieser Beitrag beschreibt technische und organisatorische Zusammenhänge. Für die rechtliche Bewertung Ihres Vorhabens wenden Sie sich an Ihr Justitiariat, Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten und gegebenenfalls an die zuständige Aufsichtsbehörde.

Häufige Fragen

Ist Copilot Chat an unserer Hochschule schon aktiv?

Sehr wahrscheinlich ja, sofern Ihre Personen A1-, A3- oder A5-Lizenzen haben. Copilot Chat ist für berechnete Pläne standardmäßig verfügbar. Für Studenten verlangt Microsoft zusätzliche Schritte. Prüfen Sie im Microsoft 365 Admin Center unter Copilot, welche Einstellungen gelten.

Kann Copilot Chat ohne Add-on unsere SharePoint-Sites durchsuchen?

Nicht von sich aus. Copilot Chat arbeitet mit dem Web und mit Dateien, die hochgeladen oder gerade geöffnet sind. Anders sieht es bei Agents aus, die auf SharePoint-Inhalte zugreifen; die sind auch ohne Add-on möglich und dann verbrauchsabhängig. Hier gelten dieselben Berechtigungsregeln wie beim Add-on.

Reicht es, Copilot Chat in den Apps zu lösen, wenn wir noch nicht so weit sind?

Nein. Das Lösen der Anheftung entfernt den Zugang nicht. Wer Copilot Chat für Gruppen sperren will, nutzt die Zugriffssteuerung im Admin Center und hinterlegt idealerweise einen Link zu einer internen Erläuterung.

Bekommen Studenten das Add-on?

Microsoft bietet das akademische Add-on auch für Studenten ab 13 Jahren an. Ob das sinnvoll ist, ist an deutschen Hochschulen vor allem eine Haushaltsfrage. Für die allermeisten Studenten ist Copilot Chat mit dem Hochschulkonto der realistische und datenschutzfreundlichere Weg.

Wie lange dauert eine Oversharing-Prüfung?

Das hängt von Größe und Zustand des Tenants ab, vor allem davon, wie gut Site-Besitzer erreichbar sind. Die Erhebung selbst ist schnell erledigt. Zeit kostet die Bereinigung in den Fachbereichen. Planen Sie die Prüfung deshalb so, dass die roten Fundorte vor dem Pilot geschlossen sind und der Rest parallel zum Pilot weiterläuft.

Können wir einzelne Sites einfach vor Copilot verstecken?

Vorübergehend ja, mit Restricted Content Discovery. Die Site bleibt für berechnete Personen erreichbar, taucht aber nicht mehr in Copilot-Antworten und der organisationsweiten Suche auf. Das ist ein Sofortschutz, kein Ersatz für korrekte Berechtigungen. Wer die Site kennt, kommt weiterhin hinein.

Muss der Personalrat zustimmen?

In aller Regel ist die Personalvertretung zu beteiligen, weil Copilot und seine Auswertungsmöglichkeiten zur Überwachung von Verhalten oder Leistung geeignet sind. Umfang und Form der Beteiligung regelt das jeweilige Landespersonalvertretungsgesetz, und für das wissenschaftliche Personal gelten je nach Land Besonderheiten. Binden Sie den Personalrat vor dem Pilot ein.

Gilt das alles auch für außeruniversitäre Forschungseinrichtungen?

Ja, im Kern sogar verschärft: Institute mit Industriekooperationen und vertraulichen Projekten haben besonders viele Inhalte, die nicht in Copilot-Antworten auftauchen dürfen. Statt Personalrat ist dort je nach Rechtsform ein Betriebsrat zuständig; die Logik der Beteiligung bleibt ähnlich.

Brauchen wir für die Prüfung zusätzliche Lizenzen?

Nicht zwingend. Viele Erkenntnisse lassen sich mit Bordmitteln und Skripten gewinnen. Komfortfunktionen wie Zugriffsüberprüfungen durch Site-Besitzer und Restricted Content Discovery gehören zu SharePoint Advanced Management, das Microsoft mit der Copilot-Lizenz bündelt. Prüfen Sie die aktuellen Voraussetzungen vor der Planung.

Fazit: Copilot ist der ehrlichste Berechtigungsprüfer, den Sie je hatten

Die Lizenzlage im Education-Bereich ist übersichtlicher geworden: Copilot Chat ist in den A-Plänen für Personal und Studenten enthalten, das Add-on gibt es als akademisches Angebot für alle Personengruppen. Die eigentliche Arbeit liegt nicht im Lizenzportal, sondern in zehn Jahren gewachsener Freigaben. Copilot macht sichtbar, was dort liegt, und er tut das ohne Rücksicht auf Gremienkultur und Zuständigkeitsgrenzen.

Wer erst die Berechtigungslage prüft, dann mit einer gemischten Gruppe pilotiert und erst danach gestaffelt erweitert, bekommt beides: einen Copilot, der im Alltag hilft, und einen Tenant, der endlich so geordnet ist, wie man es immer vorhatte. Der Personalrat sitzt dabei von Anfang an am Tisch, der Datenschutz ebenso. Wenn Sie die Copilot- und Oversharing-Überprüfung nicht nebenbei im Semesterbetrieb stemmen wollen, unterstützen wir Sie mit der [Microsoft-365-Beratung für Hochschulen und Forschung](#); für Site-Besitzer und Pilotgruppen gibt es die [Microsoft-365-Schulung für Hochschulen und Forschung](#). Und die Mail aus dem Präsidium? Die beantworten Sie dann mit einem Plan statt mit einem Seufzer.

WEITERLESEN · Weiterlesen

Für diesen Beitrag besonders passend aus der Serie:

- › [SharePoint und OneDrive an der Hochschule: Speicherpool, Lehrstuhlwechsel und Exmatrikulation](#)
- › [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#)
- › [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#)
- › [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)
- › [Microsoft-Bundesvertrag für Hochschulen: EES, Beitritt und was man damit wirklich bekommt](#)
- › [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#)
- › [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#)
- › [Exportkontrolle und vertrauliche Drittmittelprojekte: Sensitivity Labels und DLP in der Forschung](#)