Prüfungsdaten, Berufungsakten, Personalvorgänge: Besonders schützenswerte Daten im Hochschul-Tenant



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

BERATUNG
Schutzkonzept für Prüfungs-, Berufungs- und Personaldaten: Bestandsaufnahme, Labels, Gastmodell, Aufbewahrung, Copilot-Ausschluss.
› **Beratung für Hochschulen und Forschung**

SCHULUNG
Für Prüfungsamt, Berufungsreferat, Personaldezernat und Site-Besitzer: sicher teilen, richtig kennzeichnen, sauber abschließen.
› **Schulungen für Hochschulen und Forschung**

Jede Hochschule hat diese eine Geschichte. Die Notenliste, die im Verteiler der ganzen Fakultät landete, weil im Adressfeld die Autovervollständigung schneller war als der Daumen. Das Gutachten im Berufungsverfahren, das ein externer Professor netterweise „an alle“ zurückschickte. Der Ordner „Personal_alt_NICHT_LÖSCHEN“ auf einer Site, deren Besitzer vor sechs Jahren emeritiert ist. Man erzählt sich diese Geschichten im Hochschulrechenzentrum gern beim Kaffee. Weniger gern erzählt man sie der Landesdatenschutzaufsicht.

Dieser Beitrag beschäftigt sich mit den Datenbeständen, bei denen ein Fehler nicht nur peinlich ist, sondern Menschen tatsächlich schadet: Prüfungsdaten mit Attesten und Nachteilsausgleich, Berufungsakten mit Bewerbungen und vergleichenden Gutachten, Personalvorgänge, Studentenakten sowie Beschwerde- und Ordnungsverfahren. Er zeigt, wie ein Schutzkonzept in Microsoft 365 aussieht, das im Alltag tatsächlich benutzt wird: eingeschränkte Sites, Vertraulichkeitsbezeichnungen, befristeter Gastzugriff für externe Gutachter, Schluss mit Mail-Anhängen, Aufbewahrung und Löschung nach Verfahrensende und ein klarer Ausschluss aus der Reichweite von Copilot.

Er gehört zur Serie Microsoft 365 in Hochschule und Forschung und richtet sich an Leitungen von Hochschulrechenzentren, CIOs, Kanzlerinnen und Kanzler, die Dezernate der Hochschulverwaltung, Datenschutzbeauftragte und Personalräte sowie an IT- und Verwaltungsleitungen außeruniversitärer Forschungseinrichtungen. Universitätsklinika mit ihren Patientendaten folgen eigenen Regeln und bleiben hier außen vor.

FAKTEN · Das Wichtigste in Kürze

Das Fachverfahren bleibt die führende Quelle: Campus-Management, Prüfungsverwaltung und Personalsystem gehören nicht nach SharePoint. Microsoft 365 ist der Ort für die Arbeit drumherum, also Entwürfe, Abstimmungen, Gutachten und Protokolle.

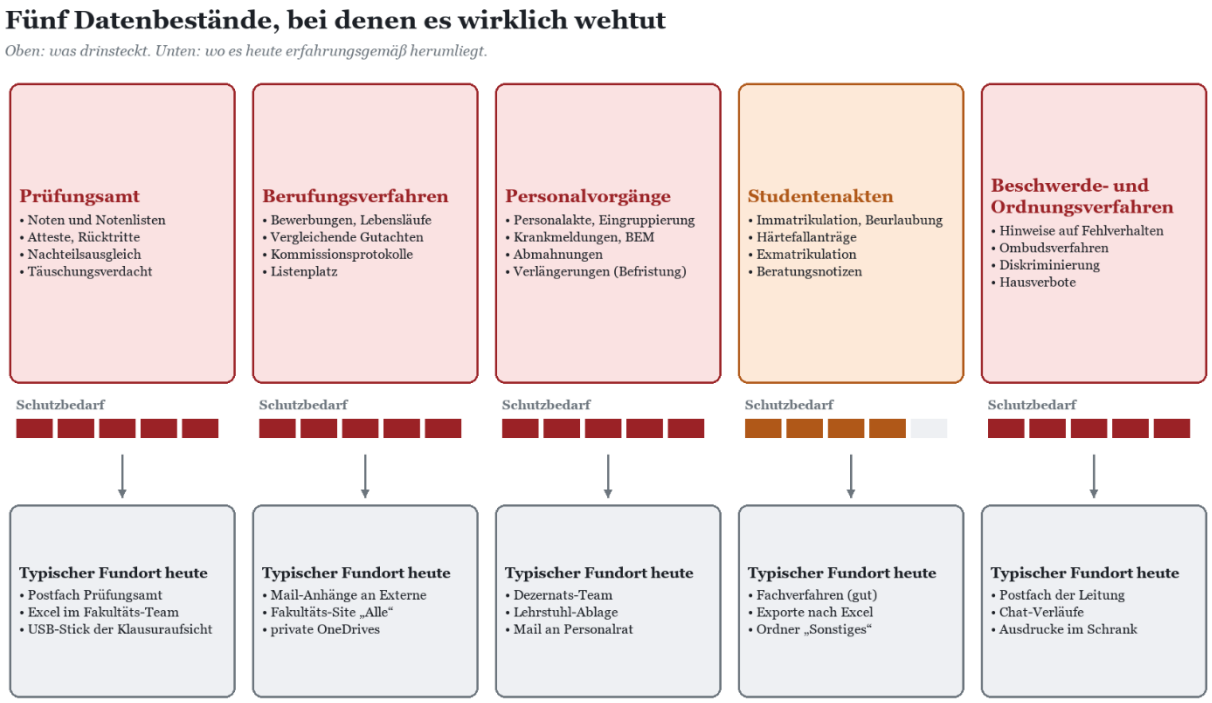
Für jeden besonders schützenswerten Bestand gibt es eine eigene, private Site oder ein eigenes Team mit Vertraulichkeitsbezeichnung. Ein Container-Label legt Privatsphäre, Gastzugriff und externe Freigabe fest; die Dateien darin erben das Label aber nicht automatisch.

Externe Gutachter kommen als namentliche Gäste mit automatischem Ablauf in genau einen Arbeitsraum, nicht als Mail-Empfänger von Anhängen.

Nach Verfahrensende greift eine Aufbewahrungsbezeichnung mit Ereignis. Copilot bleibt per DLP-Regel auf das Label außen vor, nicht per Hoffnung.

Wo es wirklich wehtut: fünf Datenbestände im Hochschulalltag

Eine Hochschule verarbeitet viele personenbezogene Daten, und die meisten davon sind unspektakulär. Wer im Sommersemester in welchem Seminar saß, interessiert außer dem Dozenten niemanden. Fünf Bestände fallen aber aus dem Rahmen, weil sie Gesundheitsdaten, Leistungsbewertungen oder Vorwürfe enthalten und weil sich eine Panne dort nicht mehr zurückholen lässt. Eine Note, die einmal im falschen Postfach war, ist dort. Für immer, oder zumindest bis zur nächsten Postfachbereinigung, die es nie gibt.



Skizze 1: Der Inhalt ist selten das Problem. Der Ablageort ist es.

Prüfungsamt: Noten, Atteste, Nachteilsausgleich

Im Prüfungsamt treffen drei Arten von Daten aufeinander: Leistungsdaten wie Noten und Prüfungsversuche, Gesundheitsdaten aus ärztlichen Attesten bei Rücktritt oder Krankheit und die besonders heiklen Unterlagen zum Nachteilsausgleich, die Behinderungen oder chronische Erkrankungen offenlegen. Dazu kommen Verfahren wegen Täuschungsverdacht, die für Studenten existenzielle Folgen haben können. Die Notenverwaltung selbst liegt in aller Regel im Campus-Management-System. Der Ärger entsteht drumherum: Notenlisten, die Dozenten als Excel-Datei

einreichen, Attestscans im Funktionspostfach, Abstimmungen mit dem Prüfungsausschuss per Chat.

Für Microsoft 365 heißt das: Das Prüfungsamt bekommt einen eigenen, privaten Arbeitsraum, getrennt nach Vorgangsart. Atteste und Nachteilsausgleich gehören in eine eigene Bibliothek mit eigenem Berechtigungskreis, weil dort deutlich weniger Personen hineinschauen müssen als in die Notenlisten. Die Einreichung von Noten durch Dozenten läuft idealerweise direkt im Fachverfahren; wo das nicht geht, über eine Dateianforderung oder einen Upload-Ordner, nicht über Mail.

Berufungsverfahren: Bewerbungen, Gutachten, externe Mitglieder

Kein Verfahren an der Hochschule verbindet so viel Vertraulichkeit mit so vielen Externen. Bewerbungsunterlagen enthalten Lebensläufe, Publikationslisten, oft Angaben zu Familie und Schwerbehinderung. Die vergleichenden Gutachten stammen von Professoren anderer Hochschulen, die Kommission hat häufig externe Mitglieder, und Gleichstellung, gegebenenfalls die Schwerbehindertenvertretung und das Berufungsreferat sind beteiligt. Kommissionsprotokolle und der Listenvorschlag sind über Jahre hinweg brisant, auch und gerade für die Personen, die nicht auf Platz eins gelandet sind.

Gleichzeitig sind Berufungsverfahren der Bereich, in dem die Mail-Kultur am hartnäckigsten überlebt: Bewerbungsmappen von 80 Seiten als PDF an zwölf Personen, Rückfragen per Antwort an alle, Gutachten als Anhang an den Vorsitz. Wie ein Berufungsverfahren als geschützter Arbeitsraum aussieht, zeigt Abschnitt drei.

Personalvorgänge

Die Personalakte selbst liegt im Personalsystem oder in Papierform im Dezernat. In Microsoft 365 landen die Vorgänge: Entwürfe von Arbeitsverträgen, Vermerke zu Eingruppierung und Befristung, Unterlagen zum betrieblichen Eingliederungsmanagement, Abmahnungen, Stellungnahmen an den Personalrat. Hochschultypisch kommt die dezentrale Zuständigkeit dazu: Lehrstühle und Institute bereiten Verlängerungen von wissenschaftlichen Mitarbeitern oder Einstellungen studentischer Hilfskräfte selbst vor und legen dafür gern eine Excel-Tabelle mit Vertragsenden, Stundenumfängen und Gehaltsstufen im Lehrstuhl-Team ab. Dort liest dann auch die Hilfskraft mit, deren Vertrag gerade nicht verlängert wird.

Studentenakten

Immatrikulation, Beurlaubung, Exmatrikulation und Härtefallanträge laufen im Studentensekretariat und dort im Fachverfahren. Problematisch werden Exporte für Auswertungen, Beratungsnotizen der Studienberatung und Unterlagen zu Härtefällen, die psychische Erkrankungen, finanzielle Notlagen oder familiäre Situationen beschreiben. Für psychologische Beratungsstellen gilt zusätzlich die berufliche Schweigepflicht. Solche Notizen gehören in einen sehr kleinen Kreis und ganz sicher nicht in ein Team, dem die halbe Abteilung angehört.

Beschwerde- und Ordnungsverfahren

Hinweise auf wissenschaftliches Fehlverhalten an die Ombudsperson, Beschwerden wegen Diskriminierung oder sexueller Belästigung, Ordnungsverfahren gegen Studenten, Hausverbote, Meldungen über das Hinweisgebersystem: Diese Bestände sind klein, aber hochexplosiv. Hier kommt zum Datenschutz noch der Schutz von Hinweisgebern und betroffenen Personen hinzu, und oft auch die Frage, wer von einem Vorgang überhaupt wissen darf. Ein Site-Name wie „Beschwerdeverfahren Prof. X“ ist schon ein Datenleck, wenn er in einer Suche oder einer Copilot-Antwort auftaucht. Neutrale Namen und Aktenzeichen statt Personennamen sind hier Pflicht, nicht Kür.

TYPISCHE SITUATION · Die Excel-Liste im falschen Team

Aus Projekten in einer Stadtverwaltung kennen wir folgende Lage: Die Personalabteilung führte eine Liste aller befristeten Verträge mit Enddatum und Bewertung, gespeichert in einem Team, das ursprünglich für die Organisation einer Betriebsfeier angelegt worden war. Mitglieder: rund 60 Personen, darunter Nachwuchskräfte in der Ausbildung. Aufgefallen ist es erst, als jemand nach „Verlängerung“ suchte und mehr fand als erwartet.

Übertragen auf die Hochschule ist das die typische Situation am Lehrstuhl oder im Dekanat: Ein Team wird für etwas Harmloses angelegt und wächst dann zur Ablage für alles. Die Gegenmaßnahme ist nicht Verbot, sondern ein eigener, vorbereiteter Arbeitsraum, der schneller verfügbar ist als die Ausrede.

Die Übersicht: Datenbestand, Schutzbedarf, Ablage, Zugriff, Löschung

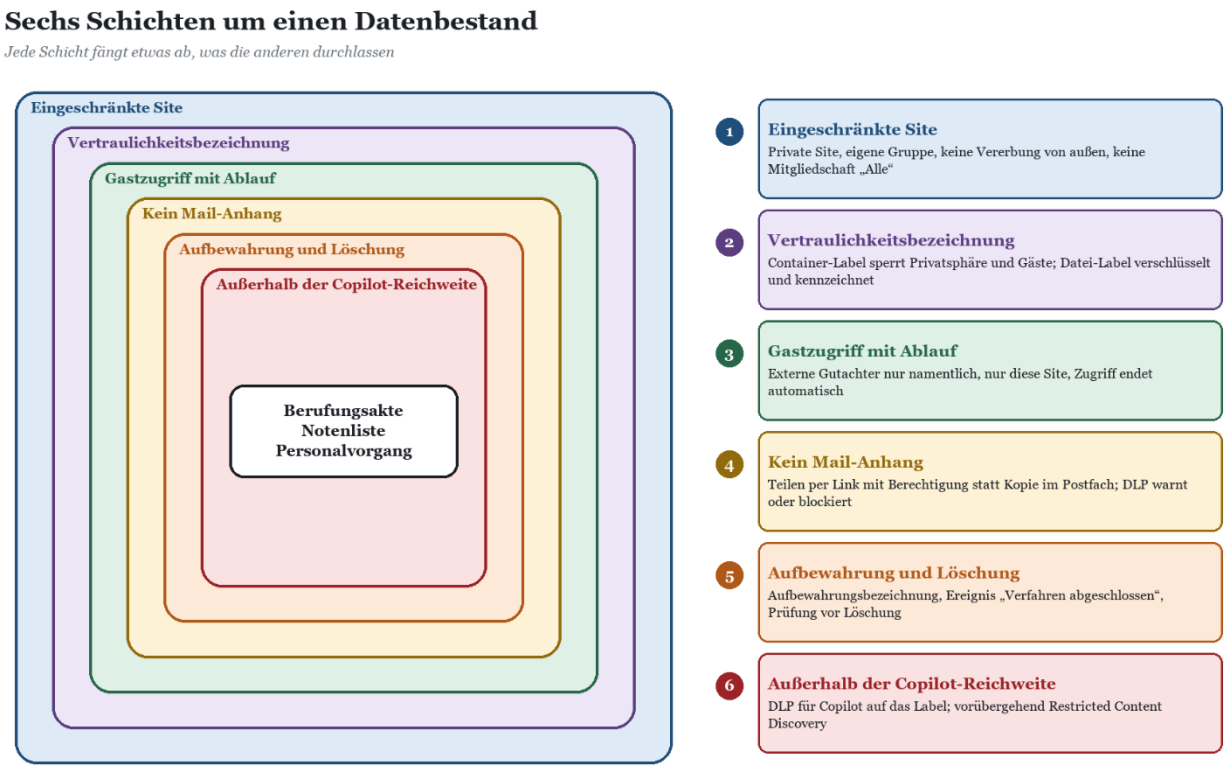
Die folgende Tabelle ist ein Ausgangspunkt für die eigene Klassifizierung, keine Vorgabe. Die konkreten Fristen ergeben sich aus Prüfungsordnungen, Landesrecht, Aktenplan und den Vorgaben des zuständigen Archivs; sie unterscheiden sich zwischen den Ländern und häufig auch zwischen Hochschulen desselben Landes.

Datenbestand	Schutzbedarf	Ablage in Microsoft 365	Zugriffsmodell	Löschung
Notenlisten, Prüfungsprotokolle	hoch	Private Site Prüfungsamt, Bibliothek je Fakultät oder Studiengang	Prüfungsamt, Prüfungsausschuss lesend; Dozenten nur Upload	Nach Übernahme ins Fachverfahren und Ablauf der Frist laut Prüfungsordnung
Atteste, Nachteilsausgleich	sehr hoch	Eigene Bibliothek mit gebrochener Vererbung oder eigene Site	Namentlich benannte Personen im Prüfungsamt, kein Ausschuss-Vollzugriff	Nach Entscheidung und Fristablauf; Ereignis „Antrag entschieden“
Berufungsakte	sehr hoch	Eine private Site je Verfahren aus Vorlage	Kommission intern als Mitglieder, Externe als befristete Gäste, Berufungsreferat als Besitzer	Ereignis „Verfahren abgeschlossen“, Frist nach Landesrecht und Hausregel
Personalvorgänge	sehr hoch	Private Site Personaldezernat, keine Lehrstuhl-Ablage	Sachbearbeitung nach Zuständigkeit; Lehrstühle nur über Formular oder Upload	Nach Abschluss des Vorgangs; Personalakte selbst im Fachsystem
Studentenakten, Härtefälle	hoch bis sehr hoch	Fachverfahren; in Microsoft 365 nur Arbeitskopien in privater Site	Studentensekretariat, Beratung getrennt	Arbeitskopien kurzfristig nach Entscheidung
Beschwerde-, Ombuds- und Ordnungsverfahren	sehr hoch	Eigene Site je Stelle, neutrale Namen, Aktenzeichen statt Namen	Sehr kleiner Kreis, keine Gäste, keine Freigabelinks	Nach Verfahrensabschluss und Frist; Prüfung vor Löschung

Das Schutzkonzept: sechs Bausteine, die zusammengehören

Ein Schutzkonzept für diese Bestände ist kein Projekt mit Hochglanzfolie, sondern eine Handvoll Regeln, die technisch durchgesetzt werden. Microsoft 365 bringt die Werkzeuge dafür mit, auch

wenn einige davon höhere Lizenzstufen oder Zusatzprodukte voraussetzen; welche Ihre Hochschule nutzen kann, hängt von den gebuchten Education-Plänen ab. Wichtiger als das einzelne Werkzeug ist die Schichtung: Jede Maßnahme fängt einen anderen Fehler ab.



Skizze 2: Keine Schicht ist allein dicht. Zusammen ergeben sie ein Schutzkonzept, das auch einen Fehlklick verzeiht.

Baustein 1: Eingeschränkte Sites statt Ordner in großen Teams

Die Grundregel ist einfach und wird trotzdem ständig gebrochen: Besonders schützenswerte Daten bekommen einen eigenen Container. Ein Ordner mit abweichenden Berechtigungen in einem großen Fakultäts-Team ist kein Schutzkonzept, sondern eine Wette darauf, dass nie jemand die Vererbung wiederherstellt. Eine private Site oder ein privates Team mit kleinem Mitgliederkreis ist übersichtlicher, lässt sich mit einem Label versehen und am Ende als Ganzes abschließen.

Dazu gehören ein paar Selbstverständlichkeiten, die in gewachsenen Tenants selten selbstverständlich sind: keine Gruppe „Jeder außer externen Benutzern“ in den Berechtigungen, mindestens zwei benannte Besitzer aus der Fachabteilung, Teilen nur durch Besitzer und ein Standard-Freigabelink, der auf bestimmte Personen zeigt statt auf die ganze Organisation. Microsoft dokumentiert diese Einstellungen auch als Teil der Vertraulichkeitsbezeichnung, sodass sie nicht für jede Site einzeln gepflegt werden müssen. Für die organisatorische Seite rund um Speicher, Lehrstuhlwechsel und Besitzerwechsel empfiehlt sich der Beitrag SharePoint und OneDrive an der Hochschule: Speicherpool, Lehrstuhlwechsel und Exmatrikulation.

TIPP · Vorlage statt Einzelanfertigung

Legen Sie für Berufungsverfahren, Prüfungsausschüsse und Beschwerdestellen je eine Site-Vorlage an: Bibliotheken, Berechtigungsgruppen, Label, Aufbewahrungsbezeichnung und eine kurze Startseite mit den Spielregeln. Das Berufungsreferat beantragt eine neue Site, das Rechenzentrum oder ein Automatismus stellt sie in Minuten bereit. Wenn die sichere Variante schneller da ist als der Workaround, gewinnt sie.

Baustein 2: Vertraulichkeitsbezeichnungen auf zwei Ebenen

Vertraulichkeitsbezeichnungen aus Microsoft Purview wirken auf zwei Ebenen, und die Unterscheidung ist wichtig. Als Container-Label auf einer Site, einem Team oder einer Microsoft-365-Gruppe legt eine Bezeichnung die Privatsphäre fest, steuert, ob Besitzer Gäste aufnehmen dürfen, wie weit externe Freigaben gehen und ob der Zugriff von nicht verwalteten Geräten blockiert oder auf den Browser beschränkt wird. Über einen Authentifizierungskontext lässt sich zusätzlich eine strengere Richtlinie für bedingten Zugriff erzwingen, etwa eine erneute Mehrstufenauthentifizierung beim Betreten der Site.

Was ein Container-Label nicht tut: Es vererbt sich nicht auf die Dateien. Eine Notenliste in einer als streng vertraulich gekennzeichneten Site ist für sich genommen unbezeichnet, sobald sie heruntergeladen oder weitergeleitet wird. Dafür braucht es Datei-Labels, die Inhalte kennzeichnen und auf Wunsch verschlüsseln, sodass auch eine Kopie außerhalb der Site nur für berechtigte Personen lesbar bleibt. Eine Standardbezeichnung für Dokumentbibliotheken oder automatische Bezeichnung nach erkannten Inhalten schließt die Lücke zwischen Container und Datei, setzt aber je nach Variante höhere Lizenzstufen voraus.

Ein hilfreiches Detail: Lädt jemand ein Dokument mit höher priorisiertem Label in eine niedriger gekennzeichnete Site, blockiert SharePoint das nicht, protokolliert aber den Fall und benachrichtigt die Person, die hochgeladen hat, sowie Besitzer und Site-Administratoren. Wer seine Label-Reihenfolge sauber pflegt, bekommt damit ein kostenloses Frühwarnsystem für die Berufungsakte im Lehrstuhl-Team.

Label (Beispiel)	Container-Einstellungen	Datei-Einstellungen	Typische Bestände
Intern	Privat oder öffentlich, Gäste nach Bedarf	Kennzeichnung, keine Verschlüsselung	Lehre, Gremien allgemein
Vertraulich · Personal und Prüfung	Privat, keine Gäste, nur interne Freigabe, Browser-Zugriff von privaten Geräten	Kennzeichnung, Verschlüsselung für die Organisation	Notenlisten, Personalvorgänge
Streng vertraulich · Berufung	Privat, Gäste nur namentlich, Authentifizierungskontext mit MFA	Verschlüsselung mit festgelegten Rechten, kein Weiterleiten	Berufungsakten, Gutachten
Streng vertraulich · Verfahren	Privat, keine Gäste, nicht auffindbar, kein Download auf privaten Geräten	Verschlüsselung für benannte Gruppe	Atteste, Nachteilsausgleich, Beschwerden, Ombudsverfahren

Für Forschungsprojekte mit Exportkontrolle oder Vertraulichkeitsvereinbarungen greift dieselbe Mechanik, nur mit anderen Bestandsarten. Wie man Labels und DLP dort zuschneidet, beschreibt der Beitrag Exportkontrolle und vertrauliche Drittmittelprojekte: Sensitivity Labels und DLP in der Forschung.

WARNUNG · Verschlüsselung hat Nebenwirkungen

Verschlüsselte Dateien lassen sich nur von berechtigten Personen öffnen, das ist der Sinn. Es bedeutet aber auch: Gäste brauchen ein Konto, das die Berechtigung einlösen kann, ältere Programme und manche Viewer scheitern, und Suchfunktionen sehen weniger. Testen Sie das Label mit einem externen Gutachter aus einer befreundeten Hochschule, bevor Sie es im ersten echten Berufungsverfahren einsetzen. Und legen Sie fest, wer im Notfall Superuser-Zugriff hat, sonst ist eine Akte am Ende sicherer, als Ihnen lieb ist.

Baustein 3: Gastzugriff für externe Gutachter, mit Ablaufdatum

Externe Gutachter und externe Kommissionsmitglieder sind an jeder Hochschule Alltag. Der sichere Weg führt über namentliche Gastkonten in Entra ID, die genau auf den Arbeitsraum des Verfahrens berechtigt werden. Keine Freigabelinks für Jedermann, keine Gastkonten auf Vorrat, keine Gäste, die nach dem Verfahren noch jahrelang im Verzeichnis stehen.

SharePoint kann den Gastzugriff auf eine Site automatisch nach einer festgelegten Zahl von Tagen auslaufen lassen; Site-Besitzer können den Zugriff verlängern oder vorzeitig beenden. Wer mehr Steuerung braucht, nutzt in Entra ID Zugriffspakete mit Ablaufdatum oder Zugriffsüberprüfungen, die Besitzer regelmäßig fragen, ob ein Gast noch gebraucht wird. Diese Governance-Funktionen setzen zusätzliche Entra-Lizenzen voraus; prüfen Sie, was in Ihrem Vertragsumfang enthalten ist. Mehrstufenauthentifizierung für Gäste gehört in jedem Fall dazu, sei es über die Heimatorganisation des Gutachters mit vertrauenswürdigen MFA-Ansprüchen oder über die eigene Richtlinie.

Variante	Wie es funktioniert	Stärke	Schwäche
Freigabelink für bestimmte Personen	Gutachter erhält Link auf eine Datei oder einen Ordner	Schnell, ohne Vorarbeit	Unübersichtlich bei vielen Dateien, Ablauf leicht vergessen
Gast in der Site mit SharePoint-Ablauf	Gast wird Mitglied der Verfahrens-Site, Zugriff endet automatisch	Übersichtlich, Ablauf erzwungen	Ablauf gilt pauschal, nicht je Verfahren fein steuerbar
Zugriffspaket in Entra ID	Paket je Verfahren mit Genehmigung, Laufzeit und Überprüfung	Sauberer Lebenszyklus, nachvollziehbar	Lizenz- und Einrichtungsaufwand
Mandantenübergreifender Zugriff	Vertrauen zur Heimatorganisation des Gutachters, deren MFA zählt	Bessere Anmeldung, weniger Helpdesk	Lohnt nur bei häufigen Partnern

Wie Gäste, Lehrbeauftragte und andere Sonderrollen in Entra ID insgesamt sauber abgebildet werden, behandelt der Beitrag Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden. Für regelmäßige Partnerhochschulen lohnt der Blick in Hochschulübergreifend zusammenarbeiten: B2B, mandantenübergreifender Zugriff und Verbundprojekte.

Baustein 4: Kein Versand per Mail-Anhang

Der Mail-Anhang ist der natürliche Feind jedes Schutzkonzepts. Er erzeugt eine Kopie, die außerhalb jeder Berechtigung, jeder Aufbewahrungsregel und jeder Löschfrist liegt, und zwar in so vielen Postfächern, wie Empfänger im Adressfeld stehen, plus Weiterleitungen, plus die Postfächer externer Gutachter an anderen Hochschulen, über deren Löschpraxis Sie nichts wissen. Wer nach Verfahrensende löschen will, kann bei Anhängen nur noch hoffen.

Die Alternative ist der Link auf die Datei in der Verfahrens-Site. Der Inhalt bleibt an einem Ort, Berechtigungen gelten weiter, der Zugriff endet mit dem Gastzugriff. Technisch unterstützen DLP-Regeln das: Sie erkennen Mails mit Anhängen, die ein bestimmtes Label tragen oder bestimmte Inhalte enthalten, und warnen, verlangen eine Begründung oder blockieren den Versand nach außen. Beginnen Sie mit Warnungen und Richtlinientipps, nicht mit Blockaden, sonst hat das Prüfungsamt am Semesterende ein sehr schlechtes Verhältnis zum Rechenzentrum.

WICHTIG · Wenn es doch Mail sein muss

Manche Vorgänge laufen zwingend per Mail, etwa Schreiben an Personen ohne Gastkonto. Dann gilt:

Label mit Verschlüsselung auf die Mail, nicht nur auf den Anhang, oder Ende-zu-Ende-Verschlüsselung per S/MIME, wenn beide Seiten Zertifikate haben. Funktionspostfächer für Prüfungsamt und Berufungsreferat bekommen eigene Aufbewahrungsregeln, damit nicht jedes Postfach zum Archiv wird.

Mehr dazu: S/MIME an Hochschulen: Nutzerzertifikate aus GÉANT TCS in Outlook und Exchange Online.

Baustein 5: Aufbewahrung und Löschung nach Verfahrensende

Daten, die nicht mehr da sind, können nicht mehr abfließen. Diese schwarzhumorige Grundwahrheit des Datenschutzes wird an Hochschulen gern übersehen, weil niemand für das Löschen zuständig ist und alle Angst haben, etwas zu löschen, was noch gebraucht wird. Das Ergebnis sind Berufungs-Sites aus dem Jahr 2017 mit vollständigen Bewerbungsmappen aller Kandidatinnen und Kandidaten, inklusive derer, die damals abgesagt haben.

Microsoft Purview bietet dafür Aufbewahrungsbezeichnungen, deren Frist nicht ab Erstellung, sondern ab einem Ereignis läuft. Für ein Berufungsverfahren ist das Ereignis zum Beispiel „Verfahren abgeschlossen“. Die Inhalte erhalten eine Bezeichnung mit diesem Ereignistyp und eine Kennung, etwa das Aktenzeichen des Verfahrens. Tritt das Ereignis ein, wird es in Purview oder per Schnittstelle angelegt, und die Frist beginnt für alle Inhalte mit dieser Kennung. Bis dahin sind die Inhalte geschützt; am Ende der Frist löscht Purview automatisch oder legt die Inhalte einer berechtigten Person zur Prüfung vor.

FAKTEN · Ereignisbasierte Aufbewahrung: was Sie wissen sollten

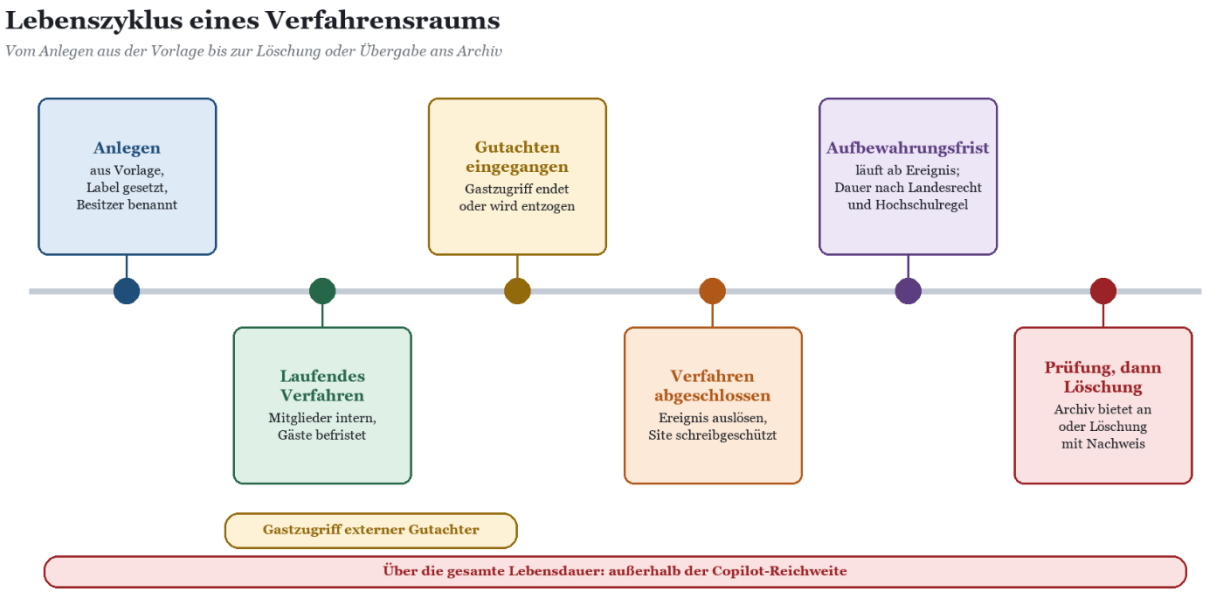
Ohne Kennung im Ereignis beginnt die Frist für alle Inhalte mit Bezeichnungen dieses Ereignistyps. Ein falsch angelegtes Ereignis startet also die Uhr für sämtliche Berufungsverfahren der Hochschule.

Die Synchronisierung eines Ereignisses auf die betroffenen Inhalte kann laut Microsoft bis zu sieben Tage dauern.

Ereignisse lassen sich nach dem Auslösen nicht zurücknehmen. Das Löschen eines Ereignisses hebt die bereits wirksamen Aufbewahrungseinstellungen nicht auf.

Die Prüfung vor Löschung ist der richtige Ort für die Anbietung an das zuständige Archiv, sofern das Landesarchivrecht das verlangt.

Welche Fristen gelten, entscheidet nicht die IT. Prüfungsordnungen, Hochschul- und Archivgesetze der Länder, Verwaltungsvorschriften und der Aktenplan der Hochschule geben den Rahmen vor, und der unterscheidet sich je Bundesland. Die IT liefert das Werkzeug und sorgt dafür, dass die Fristen auch tatsächlich durchgesetzt werden.



Skizze 4: Ein Verfahrensraum hat einen Anfang und ein Ende. Das Ende ist der wichtigere Teil.

Baustein 6: Raus aus der Copilot-Reichweite

Copilot sieht nur, was die angemeldete Person sehen darf. Das klingt beruhigend und ist es auch, solange die Rechte stimmen. Für die hier beschriebenen Bestände reicht das trotzdem nicht. Ein Kommissionsmitglied, das berechtigt in der Berufungs-Site arbeitet, soll keine Copilot-Zusammenfassung „aller Unterlagen zu Bewerberin X“ erzeugen, die dann in einem anderen Chat weiterlebt. Und eine Dekanin, die zufällig Mitglied in einer alten Prüfungsausschuss-Site ist, soll ihre Notenlisten nicht im Wochenrückblick wiederfinden.

Das wirksamste Werkzeug ist eine DLP-Richtlinie für den Speicherort Microsoft 365 Copilot und Copilot Chat mit der Bedingung „Inhalt enthält Vertraulichkeitsbezeichnung“. Dateien und Mails mit dem gewählten Label verarbeitet Copilot dann nicht mehr für Antworten; das Element kann in den Quellenangaben erscheinen, der Inhalt fließt aber nicht in die Antwort ein. In Word, Excel und PowerPoint sind die Copilot-Funktionen für eine so gekennzeichnete Datei deaktiviert. Änderungen an solchen Richtlinien können einige Stunden brauchen, bis sie wirken.

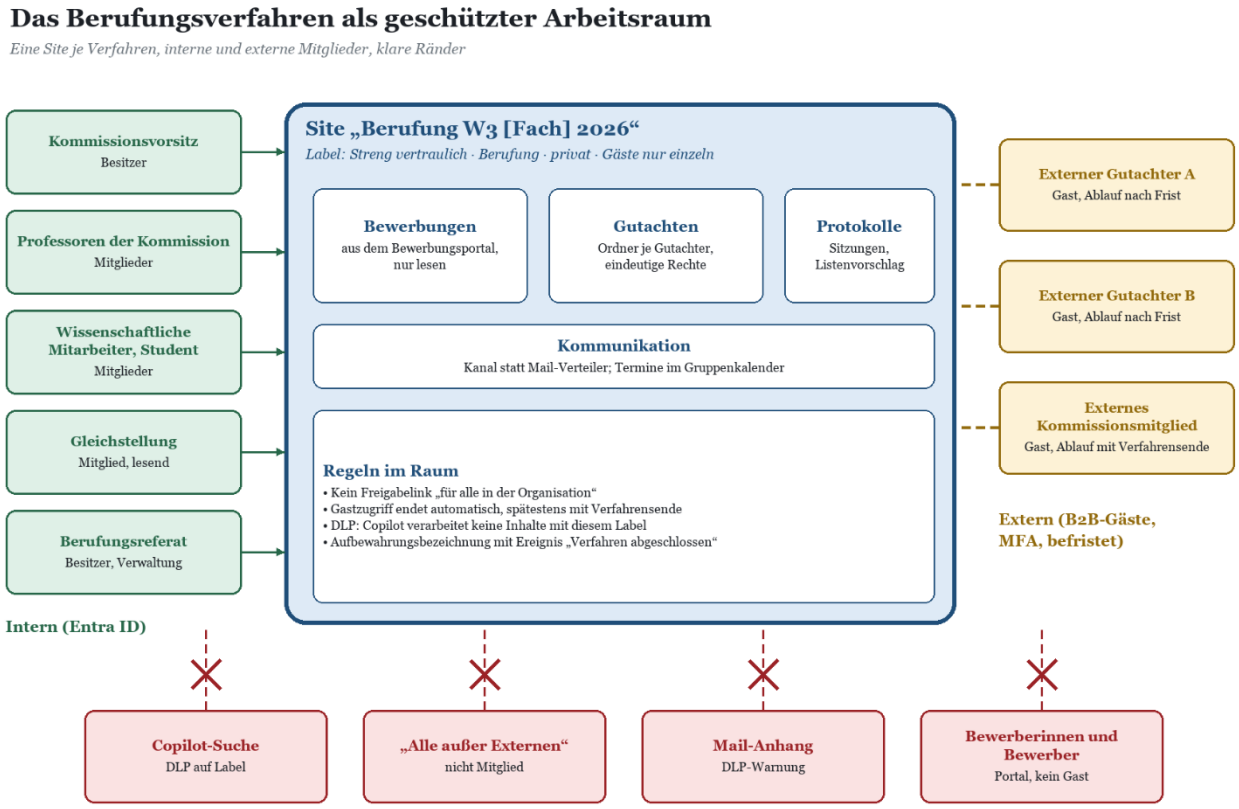
Für den Übergang, solange Labels noch nicht flächendeckend gesetzt sind, gibt es Restricted Content Discovery aus SharePoint Advanced Management. Damit tauchen Inhalte einer Site nicht mehr in der organisationsweiten Suche und in Copilot-Antworten auf. Microsoft beschreibt die Funktion ausdrücklich als vorübergehende Maßnahme: Berechtigungen ändern sich nicht, wer Zugriff hat, behält ihn, und Personen finden weiterhin Inhalte, die sie selbst besitzen oder kürzlich bearbeitet haben. Sie setzt eine Copilot-Lizenz im Tenant voraus. Wie die Oversharing-Prüfung vor einem Copilot-Piloten insgesamt abläuft, beschreibt der Beitrag Copilot an der Hochschule: Lizenz, Oversharing und die Frage, wer ihn überhaupt bekommt.

WARNUNG · Copilot ist nicht das Problem, aber der Beschleuniger

Die Berufungsakte in der Site mit Mitgliedschaft „Alle“ war schon vor Copilot ein Datenschutzvorfall, nur hat ihn niemand gefunden. Copilot findet ihn, höflich, vollständig und mit Quellenangabe. Wer die Bausteine eins bis fünf sauber umsetzt, muss Baustein sechs nur noch als Gürtel zu den Hosenträgern betrachten.

Praxisfall Berufungsverfahren: der geschützte Arbeitsraum

Am Berufungsverfahren lässt sich das gesamte Schutzkonzept durchspielen, weil hier alles zusammenkommt: interne und externe Mitglieder, besonders schützenswerte Unterlagen, ein klarer Anfang, ein klares Ende und die Pflicht, danach wieder aufzuräumen. Die folgende Skizze zeigt einen Arbeitsraum je Verfahren.



Skizze 3: Wer drin ist, arbeitet bequem. Wer draußen ist, findet nicht einmal den Namen der Site.

Anlegen: eine Site je Verfahren, aus der Vorlage

Das Berufungsreferat beantragt mit der Freigabe der Ausschreibung eine Site. Sie entsteht aus der Vorlage mit Label „Streng vertraulich · Berufung“, privaten Einstellungen, Bibliotheken für Bewerbungen, Gutachten und Protokolle und einer Aufbewahrungsbezeichnung mit dem Aktenzeichen als Kennung. Besitzer sind das Berufungsreferat und der Kommissionsvorsitz, Mitglieder die internen Kommissionsmitglieder einschließlich der Vertretungen der wissenschaftlichen Mitarbeiter und der Studenten. Die Gleichstellung erhält die Rechte, die das jeweilige Landesrecht und die Berufungsordnung vorsehen.

Bewerberinnen und Bewerber selbst werden nicht zu Gästen. Ihre Unterlagen kommen über ein Bewerbungsportal oder ein Formular in die Site, idealerweise automatisiert und mit gesetztem Label. Wer Bewerber als Gäste einlädt, damit sie hochladen können, hat sehr schnell sehr viele Gastkonten mit sehr unklarer Lebensdauer.

Arbeiten: interne Kommission und externe Gutachter

Externe Gutachter und externe Kommissionsmitglieder werden namentlich als Gäste eingeladen, jeweils mit Ablaufdatum. Gutachter sehen ihre Bewerbungsunterlagen und ihren eigenen Gutachtenordner, nicht die Gutachten der anderen und nicht die Protokolle. Externe Kommissionsmitglieder sehen, was auch die internen sehen, jedoch befristet bis zum

Verfahrensende. Kommunikation läuft im Kanal oder in Besprechungen der Gruppe, nicht über private Verteiler.

TYPISCHE SITUATION · Der externe Gutachter mit drei Konten

In einem Krankenhausverbund haben wir erlebt, wie ein externer Facharzt für ein Gutachten über die Jahre drei Gastkonten mit drei verschiedenen Adressen angesammelt hatte, alle aktiv, zwei davon mit Zugriff auf längst abgeschlossene Vorgänge. Niemand hatte etwas falsch gemacht; es hatte nur niemand je aufgeräumt.

An der Hochschule ist das die typische Situation bei Professoren, die regelmäßig begutachten: einmal mit der Dienstadresse, einmal mit der Adresse einer früheren Hochschule, einmal privat. Gastzugriff mit Ablauf und regelmäßige Zugriffsüberprüfungen lösen das Problem nicht nachträglich, verhindern aber, dass es wächst. Für die Altlasten:

› Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet

Abschließen: Ereignis, Schreibschutz, Gäste raus

Mit dem Ruf, der Annahme oder dem Abbruch des Verfahrens setzt das Berufungsreferat das Ereignis „Verfahren abgeschlossen“ mit dem Aktenzeichen. Danach wird die Site schreibgeschützt, verbliebene Gäste werden entfernt, und die Aufbewahrungsfrist läuft. Am Ende der Frist erhält eine benannte Person die Inhalte zur Prüfung vor Löschung und entscheidet, ob Teile dem Archiv angeboten werden. Danach ist die Site leer und kann gelöscht werden. Ein Verfahren, das so endet, kann in fünf Jahren nicht mehr in einer Copilot-Antwort auftauchen. Das ist der Punkt.

TIPP · Checkliste für das Berufungsreferat

Site beantragt und aus der Vorlage angelegt, Label und Aufbewahrung gesetzt.

Mindestens zwei Besitzer benannt, Mitglieder entsprechen der Kommission.

Externe als Gäste mit Ablauf eingeladen, MFA geprüft, Ordnerrechte für Gutachter gesetzt.

Keine Freigabelinks für die Organisation, keine Anhänge in Mails.

Bei Abschluss: Ereignis setzen, Gäste entfernen, Site schreibschützen.

Organisation, Mitbestimmung und Recht

Wer entscheidet was

Technik ist der kleinere Teil. Der größere ist die Frage, wer für welchen Bestand verantwortlich ist. Das Hochschulrechenzentrum stellt Plattform, Vorlagen und Labels bereit. Die Fachabteilungen, also Prüfungsamt, Berufungsreferat, Personaldezernat, Studentensekretariat und Beschwerdestellen, entscheiden über Inhalte, Mitglieder und Fristen. Das Präsidium oder Rektorat legt die Klassifizierung verbindlich fest, idealerweise als Teil einer Richtlinie zur Informationssicherheit, die auch der Senat kennt. An Hochschulen mit starker dezentraler IT kommt hinzu, dass Fakultäts-Admins und Lehrstuhl-Admins in diese Bereiche nicht hineinschauen dürfen; Admin-Rollen gehören entsprechend zugeschnitten.

Rolle	Verantwortung im Schutzkonzept
Präsidium bzw. Rektorat, Kanzler	Klassifizierung und Richtlinie verbindlich machen; Ressourcen bereitstellen
Hochschulrechenzentrum	Labels, Vorlagen, DLP, Aufbewahrung technisch umsetzen; Überwachung
Fachabteilungen und	Besitz der Arbeitsräume, Mitgliedschaften, Ereignisse bei Verfahrensende

Dekanate	
Datenschutzbeauftragte	Verzeichnis der Verarbeitungstätigkeiten, Folgenabschätzung, Beratung
Personalrat	Beteiligung bei Auswertungs- und Überwachungsfunktionen, Dienstvereinbarung
Archiv der Hochschule bzw. zuständiges Landesarchiv	Bewertung vor Löschung, Übernahme archivwürdiger Unterlagen

Personalrat und Protokollierung

Schutz bedeutet auch Protokollierung: Wer hat die Berufungsakte geöffnet, wer hat die Notenliste heruntergeladen, wer hat ein Label entfernt? Diese Daten sind für die Aufklärung eines Vorfalls unverzichtbar, lassen sich aber auch zur Verhaltens- und Leistungskontrolle nutzen. Damit ist die Mitbestimmung berührt, deren Reichweite die Personalvertretungsgesetze der Länder unterschiedlich regeln, gerade für das wissenschaftliche Personal. Regeln Sie Zweck, Zugriff und Auswertung der Protokolle in der Dienstvereinbarung. Hintergründe liefert der Beitrag Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle.

Datenschutz und Landesrecht

Für Gesundheitsdaten aus Attesten und Nachteilsausgleich gelten die besonderen Kategorien personenbezogener Daten nach der Datenschutz-Grundverordnung, für den Rest der Bestände die Landesdatenschutzgesetze und die Hochschulgesetze der Länder, die sich in Details wie Aufbewahrungsfristen, Zuständigkeiten und Beteiligungsrechten unterscheiden. Eine Datenschutz-Folgenabschätzung für die Verarbeitung solcher Bestände in Microsoft 365 ist naheliegend; welche Anforderungen dabei gelten und wie Ihre Landesaufsicht den Einsatz bewertet, sollten Sie früh klären. Die übergeordnete Diskussion führt der Beitrag Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität.

HINWEIS · Keine Rechtsberatung

Dieser Beitrag beschreibt technische und organisatorische Maßnahmen. Er ersetzt keine rechtliche Prüfung. Hochschulgesetze, Landesdatenschutzgesetze, Personalvertretungsgesetze, Archivgesetze und Prüfungsordnungen unterscheiden sich je Bundesland und Hochschule. Für die rechtliche Bewertung von Fristen, Zugriffsrechten und Beteiligungspflichten wenden Sie sich an Ihr Justitiariat, Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten und gegebenenfalls an die zuständige Aufsichtsbehörde.

Schulung statt Strafpredigt

Die beste Konfiguration hilft wenig, wenn die Sachbearbeitung im Prüfungsamt nicht weiß, wie man einen Link statt eines Anhangs verschickt, oder wenn der Kommissionsvorsitz den Gastzugriff für unnötige Bürokratie hält. Kurze, rollenbezogene Schulungen für Prüfungsamt, Berufungsreferat, Personaldezernat und Site-Besitzer bringen mehr als jede Rundmail. Unterstützung dafür bieten wir mit der Microsoft-365-Schulung für Hochschulen und Forschung an; für die Konzeption des Schutzkonzepts mit der Microsoft-365-Beratung für Hochschulen und Forschung.

Häufige Fragen

Gehören Prüfungsdaten überhaupt in Microsoft 365?

Die führenden Daten gehören ins Campus-Management-System. In Microsoft 365 landen trotzdem Arbeitsunterlagen: Notenlisten von Dozenten, Abstimmungen, Protokolle. Die Frage ist also nicht

ob, sondern wie geschützt. Wer keinen sicheren Arbeitsraum anbietet, bekommt die Daten trotzdem, nur unkontrolliert.

Reicht ein privates Team für ein Berufungsverfahren?

Es ist eine gute Basis, aber kein vollständiges Schutzkonzept. Dazu gehören ein Label, das Privatsphäre und Gastzugriff festschreibt, befristete Gäste, eine Aufbewahrungsbezeichnung und der Ausschluss aus Copilot-Antworten.

Wie bekommen externe Gutachter Zugriff, ohne dass wir Gastkonten horten?

Über namentliche Einladungen in die Verfahrens-Site mit automatischem Ablauf. SharePoint kann den Gastzugriff nach einer festgelegten Zahl von Tagen beenden; Zugriffspakete und Zugriffsüberprüfungen in Entra ID bieten mehr Steuerung, setzen aber zusätzliche Lizenzen voraus.

Vererbt sich das Label der Site auf die Dateien?

Nein. Ein Container-Label steuert Einstellungen der Site oder Gruppe. Dateien brauchen eigene Labels, etwa über eine Standardbezeichnung der Bibliothek oder über automatische Bezeichnung.

Wie halten wir Copilot von Berufungsakten fern?

Dauerhaft über eine DLP-Richtlinie für den Copilot-Speicherort mit dem Label als Bedingung. Übergangsweise über Restricted Content Discovery für einzelne Sites, die aber keine Berechtigungen ändert und eine Copilot-Lizenz voraussetzt. Die Grundlage bleiben korrekte Berechtigungen.

Wer legt die Aufbewahrungsfristen fest?

Die Fachabteilungen gemeinsam mit Justitiariat, Datenschutz und Archiv auf Grundlage von Landesrecht, Prüfungsordnungen und Aktenplan. Die IT setzt die Fristen technisch um, sie erfindet sie nicht.

Können wir Mail-Anhänge komplett verbieten?

Technisch lassen sich Anhänge mit bestimmten Labels oder Inhalten per DLP blockieren. Praktisch empfiehlt sich ein Start mit Warnungen und Richtlinientipps, damit der Wechsel zum Link gelernt wird, bevor Prozesse stehen bleiben.

Gilt das auch für außeruniversitäre Forschungseinrichtungen?

Ja, in leicht anderer Besetzung: Statt Berufungsverfahren gibt es Berufungen auf Leitungsstellen und Stellenbesetzungen, statt Prüfungsamt Promotionsangelegenheiten und Personalvorgänge. Je nach Rechtsform ist statt des Personalrats ein Betriebsrat zuständig. Die technische Mechanik bleibt dieselbe.

Fazit: Die Akte, die nicht mehr da ist, kann niemand mehr finden

Prüfungsdaten, Berufungsakten und Personalvorgänge sind keine Spezialfälle, sondern Alltag an jeder Hochschule. Sie verdienen trotzdem eine Sonderbehandlung: eigene Arbeitsräume, Labels auf Container und Datei, Gastzugriff mit Ablaufdatum, Links statt Anhänge, Aufbewahrung mit klarem Ende und einen Ausschluss aus der Copilot-Reichweite. Keine dieser Maßnahmen ist für sich spektakulär. Zusammen sorgen sie dafür, dass die nächste Kaffeegeschichte im Hochschulrechenzentrum von einem Fehlklick handelt, der folgenlos blieb.

Fangen Sie mit dem Bestand an, der am meisten schmerzt, meist dem Berufungsverfahren, und bauen Sie eine Vorlage, die schneller verfügbar ist als jede Ausrede. Binden Sie Datenschutz, Personalrat und Archiv von Anfang an ein, und behandeln Sie das Löschen als Teil des Verfahrens, nicht als lästige Pflicht danach. Wenn Sie dabei Unterstützung wollen, finden Sie die passenden Angebote in der Microsoft-365-Beratung für Hochschulen und Forschung.

WEITERLESEN · Weiterlesen

Für diesen Beitrag besonders passend aus der Serie:

› Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität

› Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden

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

› Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle

› SharePoint und OneDrive an der Hochschule: Speicherpool, Lehrstuhlwechsel und Exmatrikulation

› Exportkontrolle und vertrauliche Drittmittelprojekte: Sensitivity Labels und DLP in der Forschung

› Hochschulübergreifend zusammenarbeiten: B2B, mandantenübergreifender Zugriff und Verbundprojekte