

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

Microsoft 365 · Hochschule · Identität

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

Sie stehen in keinem Quellsystem, aber in jedem Team. Bis jemand nachzählt.

Gastwissenschaftler Lehrbeauftragte **Emeriti** Stipendiaten Externe Doktoranden Industriepartner

Berufungskommission

boddenberg.de

WISSEN

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

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

BERATUNG

Sonderrollen sauber modellieren: Kontotyp, Sponsor, Laufzeit und Lizenz je Personengruppe, bevor der nächste Fund im Tenant auftaucht.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Rechenzentrum und Fakultäts-IT: B2B-Gäste, Zugriffspakete und Zugriffsüberprüfungen in Entra ID praktisch.

› [Schulungen für Hochschulen und Forschung](#)

Jede Hochschule hat Menschen, die eindeutig dazugehören und trotzdem in keinem System stehen. Der Gastwissenschaftler aus Kyoto, der für ein Semester am Institut forscht. Die Lehrbeauftragte aus der Wirtschaft, die seit elf Jahren jedes Wintersemester dasselbe Seminar hält und jedes Mal einen neuen Lehrauftrag unterschreibt. Der Emeritus, der immer noch jeden Dienstag kommt, Doktoranden betreut und eine Mailadresse hat, die älter ist als das Hochschulrechenzentrum in seiner heutigen Form. Dazu Stipendiaten, externe Doktoranden, Kolleginnen und Kollegen aus Industrieunternehmen in einem Verbundprojekt und die externen Mitglieder einer Berufungskommission, die für sechs Wochen sehr vertrauliche Unterlagen lesen sollen.

Campus-Management kennt Studenten, das Personalsystem kennt Mitarbeiterinnen und Mitarbeiter. Für alle anderen gibt es an vielen Hochschulen eine Mail an das Rechenzentrum, ein Formular aus dem Jahr 2009 oder einen Lehrstuhl-Admin mit guten Absichten. Das Ergebnis kennen Sie: Konten ohne Ablaufdatum, Gäste ohne Ansprechpartner und eine Lizenzzählung, die niemand erklären kann. Die Konten sind dabei nicht das eigentliche Risiko. Das Risiko ist, dass für sie niemand zuständig ist.

Dieser Beitrag zeigt, wie Sie diese Sonderrollen in Entra ID sauber abbilden: wann ein Mitgliedskonto richtig ist und wann ein Gastkonto, warum jedes Konto einen Sponsor und ein Ablaufdatum braucht, was Zugriffspakete und Zugriffsüberprüfungen leisten und welche Lizenz dafür im Tenant vorhanden sein muss. Er gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#) und setzt dort an, wo der Beitrag [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#) die Sonderrollen bewusst an die Seite gestellt hat.

Universitätsklinika haben mit ihrem Gesundheitsbetrieb eigene Regeln und sind hier nicht gemeint.

FAKTEN · Worum es in diesem Beitrag geht

Personengruppen: Gastwissenschaftler, Lehrbeauftragte, Emeriti, Stipendiaten, externe Doktoranden, Industriepartner, Mitglieder von Berufungskommissionen.

Kontotyp: Mitgliedskonto oder Gastkonto (B2B), mit Entscheidungsbaum.

Pflichtfelder: Sponsor und Ablaufdatum, ohne Ausnahme.

Werkzeuge: Zugriffspakete, Zugriffsüberprüfungen und Sponsoren in Entra ID, samt Lizenzvoraussetzungen.

Überblick: Tabelle Personengruppe, Kontotyp, Lizenz, Laufzeit, Verantwortung.

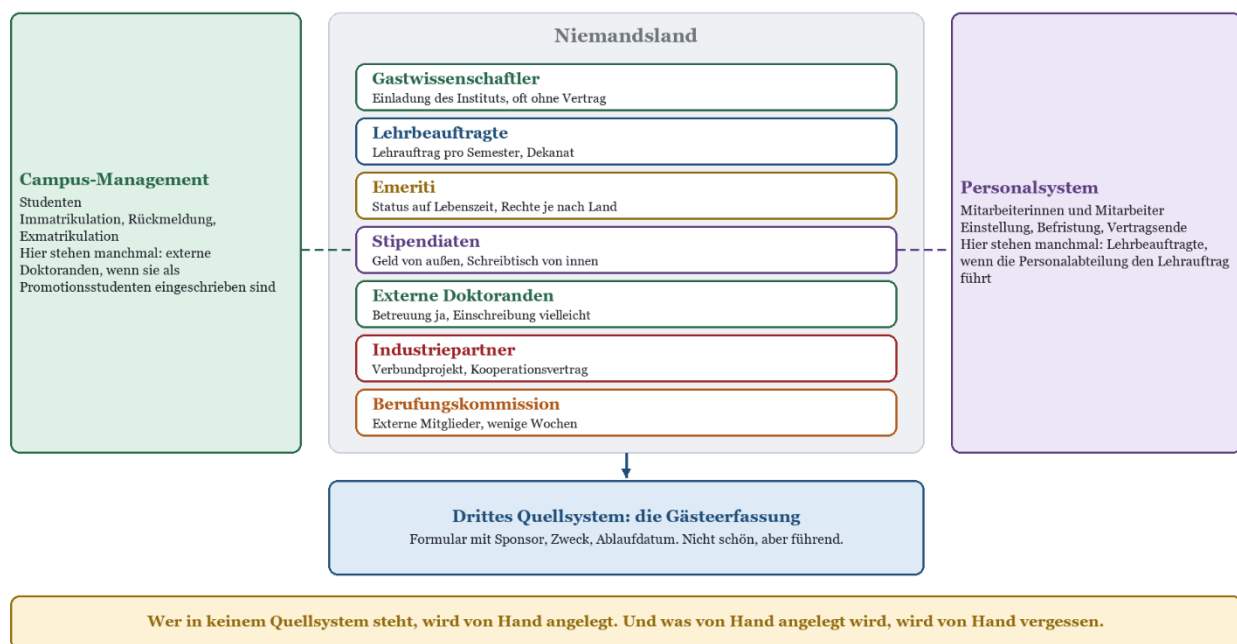
Die Menschen zwischen den Quellsystemen

Ein sauberer Identity Lifecycle beginnt mit der Frage, welches System für eine Person führend ist. Für Studenten ist es das Campus-Management, für Mitarbeiterinnen und Mitarbeiter das Personalsystem. Beide Systeme haben Anfang und Ende eingebaut: Immatrikulation und Exmatrikulation, Vertragsbeginn und Vertragsende. Das Identity-Management übernimmt diese Ereignisse, und mit etwas Disziplin folgen Konto, Gruppen und Lizenzen automatisch.

Die Sonderrollen fallen durch dieses Raster, und zwar nicht, weil jemand geschlampt hätte, sondern weil sie rechtlich und organisatorisch tatsächlich anders sind. Ein Gastwissenschaftler hat oft keinen Arbeitsvertrag mit der Hochschule, sondern eine Einladung und ein Stipendium von dritter Seite. Ein Lehrauftrag ist je nach Landesrecht ein öffentlich-rechtliches Rechtsverhältnis eigener Art und kein Arbeitsverhältnis. Emeriti und Professoren im Ruhestand haben je nach Bundesland unterschiedliche Rechte zu Lehre, Prüfung und Nutzung von Einrichtungen. Skizze 1 zeigt das Niemandsland, in dem diese Gruppen leben.

Skizze 1: Das Niemandsland zwischen den Quellsystemen

Campus-Management und Personalsystem decken die Masse ab. Die interessanten Fälle stehen dazwischen.



Schematisch. Welche Gruppe in welchem System auftaucht, regelt jede Hochschule anders.

Sieben Gruppen, sieben Logiken

- **Gastwissenschaftler:** Kommen über eine Einladung eines Instituts oder Lehrstuhls, häufig mit eigenem Stipendium oder bezahlt von der Heimateinrichtung. Aufenthalt von wenigen Wochen bis zu mehreren Jahren. Sie brauchen Zugang zu Projektdaten, Teams und oft zu Laborsystemen, aber selten eine Hochschuladresse für die Außenwirkung.
- **Lehrbeauftragte:** Halten Lehre im Namen der Hochschule, bewerten Prüfungsleistungen und tauchen im Vorlesungsverzeichnis auf. Der Lehrauftrag gilt meist für ein Semester und wird vom Dekanat oder der Fakultät erteilt. Viele kommen Semester für Semester wieder, mit Lücken dazwischen.
- **Emeriti und Professoren im Ruhestand:** Bleiben der Hochschule oft über Jahrzehnte verbunden, betreuen Doktoranden, sitzen in Gremien oder publizieren mit Hochschulaffiliation. Ein natürliches Ablaufdatum gibt es nicht. Das Rechenzentrum erfährt vom endgültigen Ende manchmal erst aus dem Nachruf im Hochschulmagazin.
- **Stipendiaten:** Werden von Stiftungen, Förderwerken oder dem Ausland finanziert, arbeiten am Institut wie Doktoranden oder Postdocs, stehen aber in keinem Personalsystem.
- **Externe Doktoranden:** Promovieren an der Hochschule, arbeiten aber anderswo, etwa in einem Unternehmen oder an einem außeruniversitären Institut. Ob sie eingeschrieben sind, regeln Promotionsordnung und Landesrecht unterschiedlich.
- **Industriepartner:** Arbeiten in einem Drittmittel- oder Verbundprojekt mit, haben einen Arbeitgeber mit eigenem Tenant und einen Kooperationsvertrag, der regelt, was sie sehen dürfen.
- **Mitglieder von Berufungskommissionen:** Externe Professoren und Gutachter, die für die Dauer eines Berufungsverfahrens Zugriff auf Bewerbungsunterlagen brauchen. Kurze Laufzeit, höchste Vertraulichkeit.

WARNUNG · Der Lehrstuhl-Admin ist kein Quellsystem

Wenn Sonderrollen über den kurzen Dienstweg angelegt werden, also per Mail an einen hilfsbereiten Administrator in der Fakultät, entsteht ein Konto ohne Herkunft. Niemand weiß später, wer es beantragt hat, wofür und bis wann. Der Administrator weiß es vielleicht noch, bis er selbst die Hochschule verlässt.

Die Lösung ist kein Verbot, sondern ein drittes Quellsystem: eine geordnete Gästeerfassung, die dieselben Pflichtfelder für alle Sonderrollen verlangt und ihre Daten an das Identity-Management liefert. Das kann ein Modul im IdM sein, ein Formular im Campus-Management oder ein schlichter Antragsprozess. Hauptsache, er ist der einzige Weg zum Konto.

Wie die Zuständigkeit zwischen zentralem Rechenzentrum und dezentraler Fakultäts-IT grundsätzlich aufgeteilt werden kann, behandelt der Beitrag [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#). Für die Sonderrollen gilt: Die Fakultät darf beantragen und sponsern, das Konto selbst entsteht zentral.

Mitgliedskonto oder Gastkonto: die eigentliche Entscheidung

Entra ID kennt zwei Grundformen. Ein Mitgliedskonto gehört zum Tenant der Hochschule, die Person meldet sich mit einer Kennung der Hochschule an, und die Hochschule verwaltet Passwort, MFA und Lebenszyklus. Ein Gastkonto über B2B-Zusammenarbeit ist dagegen ein Verweis auf eine Identität, die woanders lebt: im Tenant einer anderen Einrichtung, in einem Microsoft-Konto oder als E-Mail-Adresse, die sich per Einmalcode bestätigt. Die Person meldet sich zu Hause an und erhält im Tenant der Hochschule nur die Rechte, die ihr dort gegeben werden. Im Verzeichnis trägt das Konto den Benutzertyp Gast.

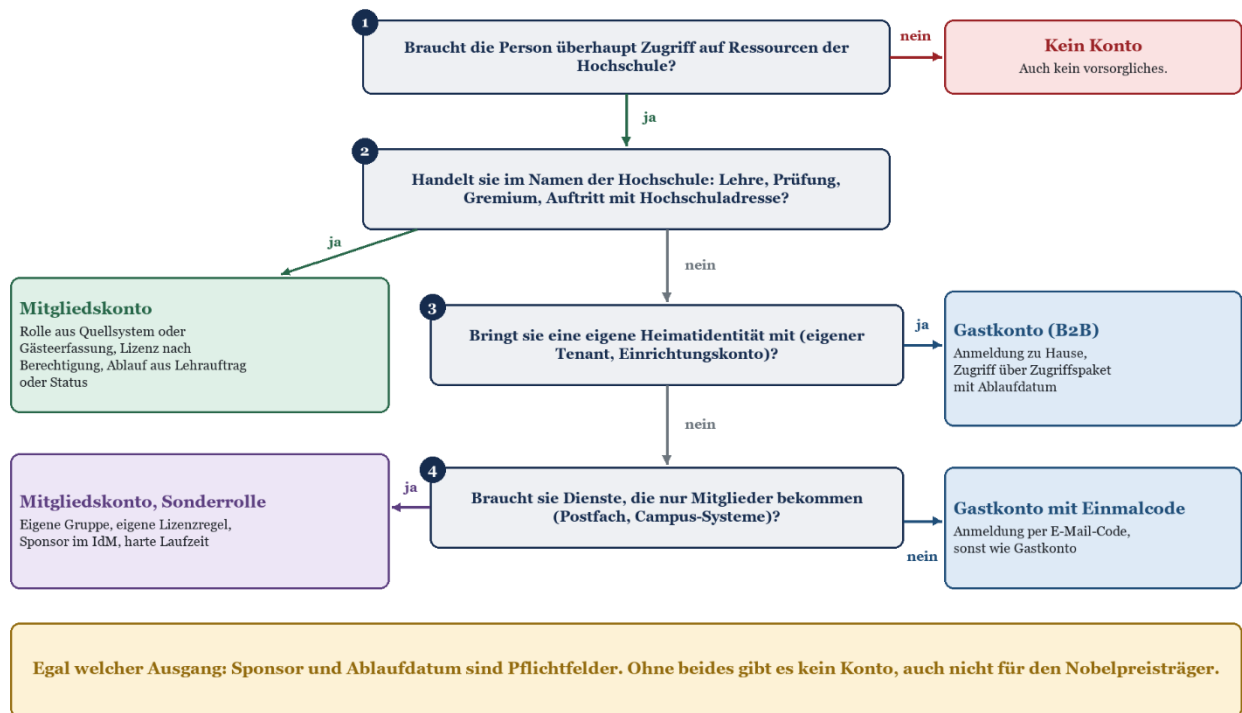
Beide Formen haben Vor- und Nachteile, und keine ist grundsätzlich die bessere. Das Gastkonto entlastet die Hochschule vom Passwort und vom Austritt aus der Heimateinrichtung: Verlässt der Gast seine eigene Universität, verliert er dort das Konto und kommt damit auch nicht mehr in den Hochschul-Tenant. Dafür kann der Gast kein eigenes Postfach unter der Hochschuldomäne nutzen und taucht in vielen lokalen Systemen nicht auf. Das Mitgliedskonto ist vollwertig, verlangt aber, dass die Hochschule den kompletten Lebenszyklus selbst führt.

Der Entscheidungsbaum

In der Praxis hat sich eine Reihenfolge von vier Fragen bewährt. Die erste ist die unbequemste: Braucht die Person überhaupt ein Konto? Eine Datei, die ein Gutachter einmal lesen soll, lässt sich auch anders übermitteln. Die zweite Frage entscheidet über die meisten Fälle: Handelt die Person im Namen der Hochschule? Wer lehrt, prüft, in einem Gremium sitzt oder mit der Hochschuladresse nach außen auftritt, bekommt ein Mitgliedskonto. Erst wenn das nicht der Fall ist, kommt die Frage nach der Heimatidentität.

Skizze 2: Entscheidungsbaum Mitgliedskonto oder Gastkonto

Vier Fragen, fünf Ausgänge. Die Reihenfolge ist Absicht.



Vereinfachte Darstellung. Landesrecht, Datenschutz und Lizenzbedingungen können einzelne Äste verschieben.

Der vierte Ast verdient einen zweiten Blick. Es gibt Personen ohne Heimatidentität, die trotzdem Dienste brauchen, die nur Mitglieder bekommen, etwa ein Stipendiat aus einem Land, dessen Heimateinrichtung keine brauchbare Identität liefert, und der ein Postfach und Zugang zum WLAN über eduroam braucht. Für solche Fälle ist ein Mitgliedskonto in einer eigenen Sonderrolle sauberer als ein Gastkonto, das man mit Ausnahmen verbiegt. Entscheidend ist, dass diese Sonderrolle eine eigene Gruppe, eine eigene Lizenzregel und eine harte Laufzeit bekommt.

TIPP • Keine Doppelkonten für Doppelrollen

Ein Gastwissenschaftler, der während seines Aufenthalts einen Lehrauftrag übernimmt, bekommt kein zweites Konto. Er wechselt in die stärkere Rolle, also ins Mitgliedskonto, und die Gästeerfassung liefert den Sponsor weiter. Wer stattdessen ein Gastkonto und ein Mitgliedskonto nebeneinander führt, hat zwei Anmeldungen, zwei OneDrives und nach dem Semester garantiert ein Konto zu viel.

Wie Doppelrollen im IdM aufgelöst werden, beschreibt der Beitrag zum Identity Lifecycle ausführlich.

Anmeldung mit der Heimatidentität

Kommt der Gast von einer Einrichtung mit eigenem Microsoft-Tenant, ist die Sache einfach: Er meldet sich mit seinem dortigen Konto an, und die mandantenübergreifenden Zugriffseinstellungen regeln, ob die Hochschule seiner MFA und dem Gerätestatus der Heimateinrichtung vertraut. Kommt er von einer Einrichtung ohne Microsoft-Tenant, bleibt in der Regel der Einmalcode per E-Mail oder ein Microsoft-Konto. Die naheliegende Frage, ob ein Gast sich nicht einfach mit seiner Kennung aus der DFN-AAI anmelden könnte, ist berechtigt, aber architektonisch eine eigene Geschichte. Der Beitrag [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#) zeigt, wo die beiden Welten zusammenpassen und wo nicht.

WICHTIG · Gastkonten richtig einschränken

Bevor Sie Gäste systematisch einladen, sollten die Grundeinstellungen stimmen: Wer darf Gäste einladen, dürfen Gäste andere Gäste einladen, was dürfen Gäste im Verzeichnis sehen, und welche Domänen sind zugelassen oder gesperrt. Microsoft selbst empfiehlt für geordnete Einladungen über Zugriffspakete, dass Gäste keine weiteren Gäste einladen dürfen.

Prüfen Sie außerdem die Richtlinien für bedingten Zugriff. Gäste haben selten registrierte Geräte und sitzen nicht im Campusnetz. Eine Richtlinie, die das verlangt, sperrt sie nicht nur aus den Ressourcen aus, sondern auch aus dem Portal, über das sie Zugriff überhaupt erst beantragen.

Sponsor und Ablaufdatum: zwei Pflichtfelder, keine Ausnahmen

Wenn Sie aus diesem Beitrag nur eine Regel mitnehmen, dann diese: Kein Sonderrollen-Konto ohne Sponsor und ohne Ablaufdatum. Der Sponsor ist eine Person an der Hochschule, die für das Konto inhaltlich geradesteht. Sie hat den Gast eingeladen, sie weiß, warum er Zugriff braucht, und sie ist die Ansprechpartnerin, wenn sich das ändert. Das Ablaufdatum ist der Zeitpunkt, zu dem das Konto ohne aktives Zutun endet. Verlängerung ist möglich, aber nur durch den Sponsor und nur bewusst.

Der Sponsor in Entra ID

Für Gastkonten bringt Entra ID ein eigenes Feld mit. Auf dem Benutzerobjekt gibt es die Eigenschaft Sponsoren, die auf eine Person oder eine Gruppe verweist. Wer einen Gast einlädt, wird automatisch als Sponsor eingetragen, sofern bei der Einladung niemand anders angegeben wird; bei der Einladung lassen sich bis zu fünf Sponsoren hinterlegen. Das Feld verleiht selbst keine Administratorrechte. Es ist eine Zuständigkeitsangabe, die Genehmigungs- und Überprüfungsprozesse nutzen können.

Zwei Details sollten Sie kennen. Erstens trägt Entra ID keinen Sponsor ein, wenn ein externer Benutzer über eine Freigabe in SharePoint eingeladen wird; Microsoft führt das als bekanntes Problem. Wer Freigaben an Unbekannte erlaubt, erzeugt also Gäste ohne Sponsor. Zweitens ist ein einzelner Mensch als Sponsor eine Sollbruchstelle. Verlässt die Professorin die Hochschule, zeigt das Feld ins Leere. Robuster ist eine Gruppe, etwa das Sekretariat und die Leitung eines Lehrstuhls, oder eine Regel im Austrittsprozess, die Sponsorschaften vor dem letzten Arbeitstag übergibt.

Für Mitgliedskonten in Sonderrollen führen Sie den Sponsor im Identity-Management und spielen ihn nach Entra ID aus, etwa als Vorgesetzten oder in einem eigens definierten Attribut. Wichtig ist nicht das Feld, sondern dass es befüllt, gepflegt und ausgewertet wird.

Das Ablaufdatum muss wirken, nicht nur dastehen

Ein Ablaufdatum im lokalen Active Directory beruhigt, wirkt aber in Entra ID nicht von selbst. Ein Konto, dessen Ablaufzeit lokal überschritten ist, kann sich in der Cloud weiter anmelden, solange es nicht deaktiviert wird. Das Datum braucht also einen Prozess, der es in eine Handlung übersetzt: das IdM, das zum Stichtag deaktiviert, ein Lebenszyklus-Workflow in Entra ID, der mit dem Austrittsdatum arbeitet, oder bei Gästen die Laufzeit einer Zuweisung zu einem Zugriffspaket.

Pflichtfeld	Inhalt	Wer pflegt	Was passiert ohne
Sponsor	Person oder Gruppe an der Hochschule, die inhaltlich verantwortlich ist	Antragsteller, bei Austritt der Nachfolger	Niemand fühlt sich zuständig; Überprüfungen laufen ins Leere
Ablaufdatum	Konkretes Datum, abgeleitet aus Lehrauftrag, Einladung, Projektlaufzeit oder Verfahren	Gästeerfassung, IdM	Konto lebt ewig; Lizenz und Zugriffe bleiben
Zweck	Lehrauftrag, Projekt, Verfahren, Betreuung	Antragsteller	Bei Verlängerung kann niemand prüfen, ob der Grund noch besteht
Organisationseinheit	Fakultät, Institut, Lehrstuhl	Gästeerfassung	Auswertungen und dezentrale Zuständigkeit unmöglich
Rolle	Eine der definierten Sonderrollen	Gästeerfassung, IdM	Keine Gruppenregel, keine Lizenzregel, Einzelfallbastelei

Laufzeiten, die zur Hochschule passen

Die Laufzeit sollte aus dem Anlass folgen, nicht aus einer pauschalen Zahl. Für Lehrbeauftragte ist das Semesterende plus eine Karenz für Nachprüfungen und Notenmeldungen der natürliche Stichtag. Für Gastwissenschaftler ist es das Ende der Einladung, für Industriepartner das Projektende laut Kooperationsvertrag, für Mitglieder einer Berufungskommission der Abschluss des Verfahrens. Bei Emeriti gibt es keinen Anlass mit Enddatum; hier ersetzt eine regelmäßige Bestätigung das Ablaufdatum, etwa jährlich durch das Dekanat. Das wirkt bürokratisch, ist aber die einzige Methode, die ohne Nachrufe als Datenquelle auskommt.

HINWEIS · Kein Ersatz für Rechtsberatung

Ob und wie lange personenbezogene Daten von Gästen, Lehrbeauftragten und Emeriti verarbeitet werden dürfen, regeln Hochschulgesetz, Landesdatenschutzgesetz und hochschuleigene Satzungen, und zwar je Bundesland unterschiedlich. Gleiches gilt für die Frage, ob der Personalrat bei Lehrbeauftragten oder Stipendiaten überhaupt zuständig ist. Stimmen Sie Laufzeiten, Löschfristen und Protokollierung mit der behördlichen Datenschutzbeauftragten oder dem behördlichen Datenschutzbeauftragten und gegebenenfalls dem Personalrat ab.

Hintergrund zu beiden Fragen liefern die Beiträge [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#) und [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#).

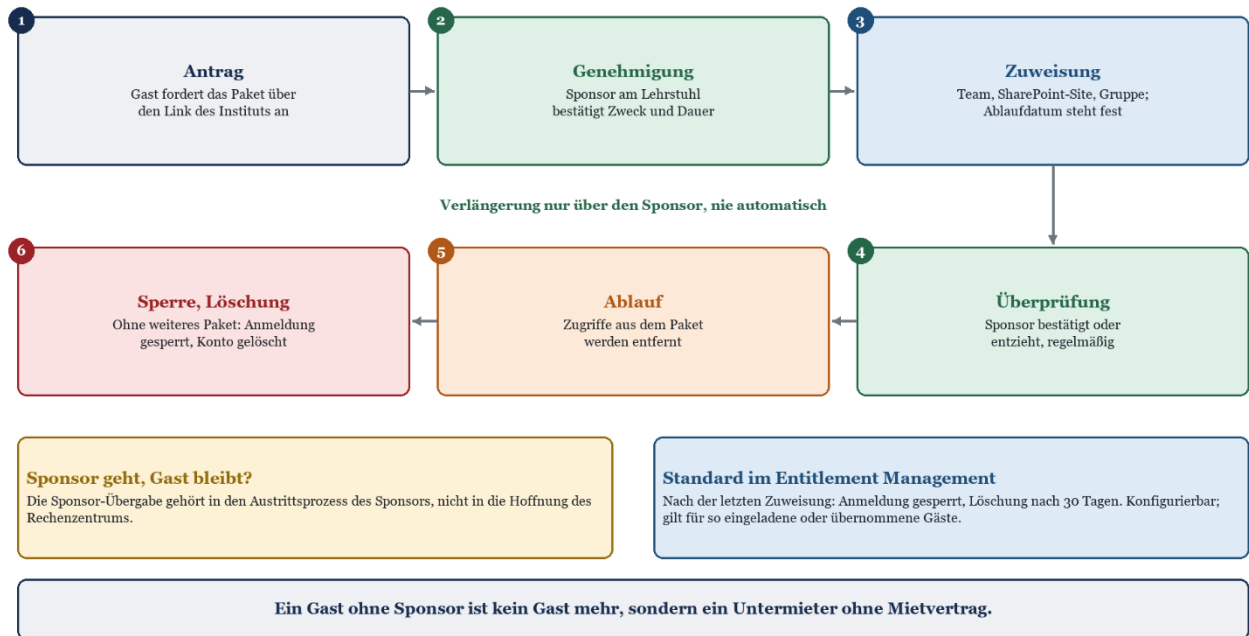
Zugriffspakete und Zugriffsüberprüfungen

Sponsor und Ablaufdatum sind Regeln. Damit sie nicht an der Disziplin einzelner Menschen hängen, bietet Entra ID zwei Werkzeuge aus dem Bereich ID Governance. Zugriffspakete aus der Berechtigungsverwaltung bündeln Ressourcen wie Gruppen, Teams, SharePoint-Sites und

Anwendungen. Ein Gast beantragt das Paket, ein Genehmiger stimmt zu, die Zuweisung erhält eine Laufzeit, und mit deren Ende werden die Zugriffe automatisch entzogen. Zugriffsüberprüfungen fragen in regelmäßigen Abständen bei Sponsoren, Gruppenbesitzern oder den Gästen selbst nach, ob der Zugriff noch nötig ist.

Skizze 3: Lebenslauf eines Gastzugangs über ein Zugriffspaket

Der Sponsor taucht an mehreren Stellen auf. Fällt er weg, hinkt der ganze Mechanismus.



Schematisch. Lizenzbedarf je Schritt: siehe Tabelle im Abschnitt zu Zugriffspaketen.

Für Gäste, die über ein Zugriffspaket in den Tenant gekommen sind, gilt eine Voreinstellung, die viele Rechenzentren unterschätzen: Verliert ein solcher Gast seine letzte Zuweisung, wird er standardmäßig für die Anmeldung gesperrt und nach 30 Tagen aus dem Verzeichnis entfernt. Beides ist konfigurierbar und betrifft nur Gäste, die über die Berechtigungsverwaltung eingeladen oder ausdrücklich in deren Lebenszyklus übernommen wurden. Ein Gast, der schon vorher im Tenant war, bleibt also, auch wenn sein Paket ausläuft. Für die Altbestände braucht es eine eigene Bereinigung.

Was ein Paket für die Hochschule sinnvoll macht

- **Ein Paket je Anlass, nicht je Person:** Gast am Institut X, Verbundprojekt Y, Berufungsverfahren Z. Die Inhalte pflegt der Sponsor oder die Fakultät, nicht das Rechenzentrum.
- **Genehmigung durch den Sponsor:** Die Genehmigungsstufe sollte bei der Person liegen, die den Gast kennt, nicht bei einer zentralen Stelle, die nur abnickt.
- **Laufzeit im Paket, nicht im Gedächtnis:** Ablauf nach Datum oder nach einer festen Zahl von Tagen, Verlängerung nur auf Antrag mit erneuter Genehmigung.
- **Verborgene Pakete mit Direktlink:** Externe sollen nicht im Portal stöbern, sondern den Link bekommen, den ihnen das Institut schickt.
- **Verbundene Organisationen:** Für wiederkehrende Partner, etwa eine Nachbaruniversität oder ein Unternehmen im Verbundprojekt, lässt sich die Organisation einmal hinterlegen und im Paket als zulässige Herkunft auswählen.

Was davon welche Lizenz braucht

Hier wird es kleinteilig, und hier lohnt sich der Blick in die aktuelle Dokumentation auf learn.microsoft.com, denn Microsoft hat das Lizenzmodell in den letzten Jahren mehrfach umgebaut. Stand der Dokumentation im Herbst 2026: Die Grundfunktionen der Berechtigungsverwaltung und der Zugriffsüberprüfungen sind in Entra ID P2 enthalten, also etwa in A5-Plänen. Erweiterte Funktionen verlangen Microsoft Entra ID Governance, das als Zusatz zu einem Plan mit Entra ID P1 oder P2 erworben wird; A3- und A5-Pläne erfüllen diese Voraussetzung. Microsoft hat außerdem angekündigt, neue Governance-Funktionen nicht mehr in P2 aufzunehmen.

Für Gäste gilt ein eigenes Modell. Funktionen aus P2 werden für Gäste nicht gesondert berechnet. Funktionen, die exklusiv zu ID Governance gehören, werden für Gäste nach monatlich aktiven Nutzern über ein verknüpftes Azure-Abonnement abgerechnet, und zwar je Gast mit mindestens einer Governance-Aktion im Monat. Ein kostenfreies Kontingent gibt es für diese Governance-Abrechnung nicht, und seit Januar 2026 setzt Microsoft die Verknüpfung durch. Zusätzlich muss im Tenant mindestens eine Governance-Lizenz für eine administrierende Person vorhanden sein. Für Mitgliedskonten zählt dagegen die Zahl der Mitglieder im Geltungsbereich einer Funktion, nicht die Zahl der zugewiesenen Lizenzen.

Funktion	Mitgliedskonten	Gastkonten	Hinweis
Zugriffspaket mit Antrag, Genehmigung, Ablauf	Entra ID P2 oder ID Governance	Keine Governance-Abrechnung, solange nur P2-Funktionen genutzt werden	Grundform für Gastwissenschaftler und Projektpartner
Sponsor aus dem Benutzerprofil als Genehmiger	ID Governance	Abrechnung je aktivem Gast über Azure-Abonnement	Interne und externe Sponsoren aus verbundenen Organisationen gehen bereits mit P2
Automatische Zuweisungsrichtlinien	ID Governance	Abrechnung je aktivem Gast	Sinnvoll für Sonderrollen-Gruppen aus dem IdM
Zugriffsüberprüfung von Gruppen und Paketen	Entra ID P2 oder ID Governance	Keine Governance-Abrechnung für P2-Funktionen	Regelüberprüfung durch Sponsor oder Gruppenbesitzer
Überprüfung nur inaktiver Benutzer	ID Governance	Abrechnung je Gast im Überprüfungsumfang	Das Werkzeug für Altbestände
Lebenszyklus-Workflows	ID Governance	Abrechnung je Gast bei Ausführung	Etwa Deaktivierung zum Austrittsdatum

FAKTEN · Lizenzregeln für Governance, kurz gefasst

Grundfunktionen der Berechtigungsverwaltung und der Zugriffsüberprüfungen: Entra ID P2 oder Microsoft Entra ID Governance.

Erweiterte Funktionen wie Sponsor als Genehmiger, automatische Zuweisung, Überprüfung inaktiver Benutzer und Lebenszyklus-Workflows: Microsoft Entra ID Governance.

Gäste: Abrechnung exklusiver Governance-Funktionen nach monatlich aktiven Nutzern über ein verknüpftes Azure-Abonnement, ohne Freikontingent.

Zählweise bei Mitgliedern: alle Mitglieder im Geltungsbereich, auch wer nur beantragen kann oder überprüft wird.

Stand: Microsoft-Dokumentation im Herbst 2026. Prüfen Sie vor jeder Entscheidung die aktuelle Fassung und Ihren Vertrag.

Welche Education-Pläne an Ihrer Hochschule welche Entra-Funktionen mitbringen, hängt am Vertrag. Der Beitrag [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#) sortiert die Pläne; die Frage, ob eine bestimmte Personengruppe überhaupt akademisch lizenzberechtigt ist, sollten Sie mit Ihrem Vertragspartner klären und nicht aus Gewohnheit beantworten.

TIPP · Ohne Governance-Lizenz geht auch etwas

Nicht jede Hochschule wird für Sonderrollen sofort Governance-Lizenzen kaufen, und das muss sie auch nicht. Der Kern des Sponsor-Prinzips funktioniert auch mit Bordmitteln: Sponsorfeld bei jeder Einladung befüllen, Ablaufdatum in der Gästefassung führen, das IdM oder ein geplantes Skript deaktiviert zum Stichtag, und einmal im Semester bekommt jeder Sponsor eine Liste seiner Gäste mit der Bitte um Bestätigung. Das ist weniger elegant, aber unendlich besser als nichts.

Die Sonderrollen im Überblick

Die folgende Tabelle fasst zusammen, wie sich die sieben Gruppen in typischen Konstellationen abbilden lassen. Sie ist ein Ausgangspunkt für die eigene Regelung, keine Norm. Insbesondere die Lizenzspalte hängt an Ihrem Vertrag und an der Berechtigung der jeweiligen Gruppe nach den akademischen Lizenzbedingungen.

Personengruppe	Kontotyp	Lizenz	Laufzeit	Wer verantwortet
Gastwissenschaftler	Gastkonto mit Heimatidentität ; Mitgliedskonto, wenn eigene Dienste nötig	Gast: keine eigene Microsoft-365-Lizenz für Zusammenarbeit ; Mitglied: nach Berechtigung	Ende der Einladung, höchstens ein Jahr je Zuweisung	Einladender Lehrstuhl, Institutsleitung
Lehrbeauftragte	Mitgliedskonto	Lizenz für Lehrpersonal, soweit vertraglich berechtigt	Semesterende plus Karenz für Prüfungen; Verlängerung mit neuem Lehrauftrag	Dekanat bzw. Fachbereich
Emeriti, Professoren im Ruhestand	Mitgliedskonto in eigener Sonderrolle	Eingeschränkt, Berechtigung gesondert prüfen	Unbefristet, aber jährliche Bestätigung	Dekanat, Fakultätsleitung
Stipendiaten	Gastkonto oder Mitgliedskonto in Sonderrolle	Je nach Kontotyp und Berechtigung	Laufzeit des Stipendiums	Betreuer, Professor, Institut
Externe Doktoranden	Mitgliedskonto, wenn eingeschrieben; sonst Gastkonto	Studentenlizenz bei Einschreibung, sonst keine	Rückmeldung bzw. Betreuungsvereinbarung	Betreuer, Promotionsbüro
Industriepartner	Gastkonto, möglichst aus dem Firmentenant	Keine eigene Lizenz	Projektende laut Kooperationsvertrag	Projektleitung, Drittmittelverwaltung
Berufungskommission (extern)	Gastkonto mit eng begrenztem Paket	Keine eigene Lizenz	Abschluss des Berufungsverfahrens	Vorsitz der Kommission, Berufsreferat

Lehrbeauftragte: die Semester-Pendler

Lehrbeauftragte sind der Fall, an dem sich zeigt, ob eine Regelung durchdacht ist. Der Lehrauftrag endet mit dem Semester, die Person kommt im nächsten Semester oft wieder. Löscht das Rechenzentrum das Konto pünktlich, sind Kursmaterial in OneDrive und die Mitgliedschaft im Kursteam weg. Lässt es das Konto aktiv, hat es nach ein paar Jahren eine stattliche Sammlung von Konten ehemaliger Lehrbeauftragter. Der Mittelweg ist eine Karenz: Nach Semesterende wird das Konto deaktiviert, aber nicht gelöscht, und ein neuer Lehrauftrag innerhalb der Frist aktiviert es wieder. Erst nach Ablauf der Frist folgt der übliche Austrittspfad.

Emeriti: das Konto auf Lebenszeit

Bei Emeriti wird es menschlich. Die Mailadresse ist für viele ein Teil der wissenschaftlichen Identität, und niemand im Rechenzentrum möchte derjenige sein, der einem verdienten Professor nach vierzig Jahren das Postfach abschaltet. Das muss auch niemand. Aber ein Konto in einer eigenen Sonderrolle mit reduzierten Rechten, einer jährlichen Bestätigung durch das Dekanat und einer klaren Regel für den Todesfall ist sowohl würdevoll als auch verwaltbar. Die Regel für den Todesfall betrifft dabei nicht nur das Konto, sondern auch den Zugang zu Daten, an denen noch andere arbeiten.

Berufungskommissionen: kurz und heikel

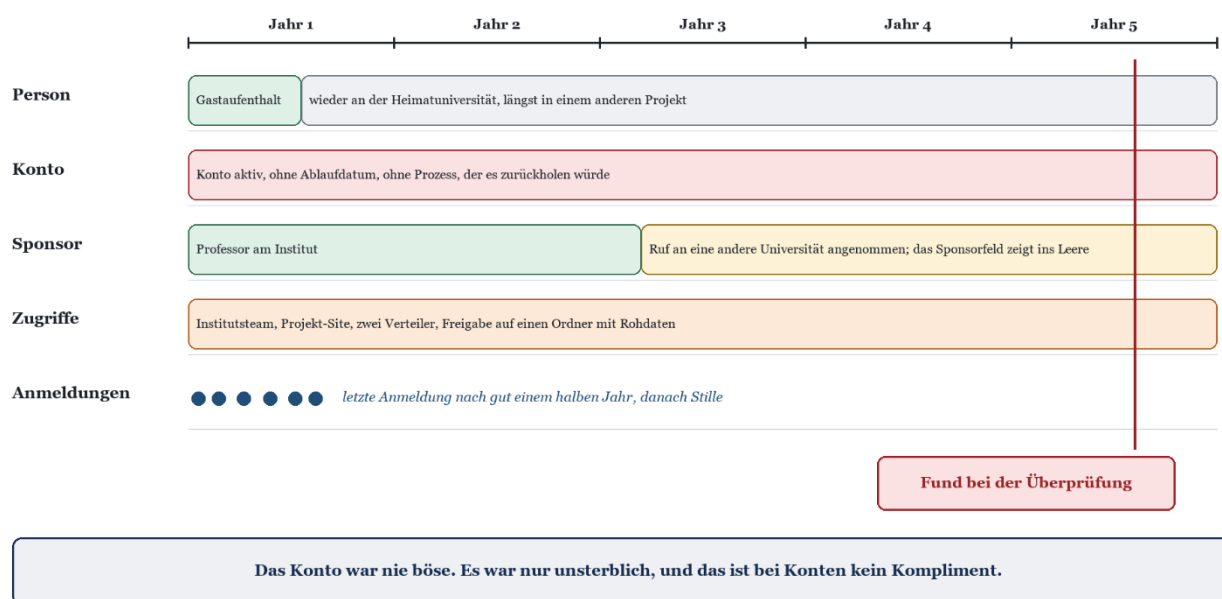
Externe Mitglieder einer Berufungskommission sind das Gegenteil der Emeriti: kurze Laufzeit, aber Zugriff auf Bewerbungsunterlagen, Gutachten und Protokolle, die zu den vertraulichsten Daten der Hochschule gehören. Hier passt ein Zugriffspaket je Verfahren mit genau einer SharePoint-Site oder einem Team, Genehmigung durch den Vorsitz, Ablauf zum Ende des Verfahrens und einer Bedingung, die das Herunterladen auf nicht verwaltete Geräte einschränkt. Was danach mit den Unterlagen passiert, regelt das Berufungsreferat, nicht das Ablaufdatum des Gastkontos.

Das Konto des Gastes, der seit vier Jahren wieder zu Hause ist

Am Ende landet jede Diskussion über Sonderrollen bei derselben Figur: dem Gast, der längst weg ist und dessen Konto noch da ist. Skizze 4 zeigt, wie das ohne jedes Fehlverhalten entsteht.

Skizze 4: Das Konto des Gastes, der seit vier Jahren wieder zu Hause ist

Typische Situation, schematisch. Niemand hat etwas falsch gemacht. Genau das ist das Problem.



Schematische Darstellung einer typischen Situation, keine reale Einrichtung.

TYPISCHE SITUATION · Unsterbliche Gastkonten

In einem kommunalen Verband fanden sich bei einer Bereinigung des Tenants Gastkonten externer Berater, deren Projekte seit Jahren abgeschlossen waren. Die Konten waren Mitglied in mehreren Teams, eines hatte noch Zugriff auf einen Ordner mit Vertragsunterlagen. Eingeladen hatte jeweils ein Projektleiter, der inzwischen selbst in einer anderen Behörde arbeitete. Ähnliche Funde gab es in einer Stadtverwaltung und in einem Krankenhausverbund; das Muster war jedes Mal dasselbe.

An der Hochschule sieht die typische Situation so aus: Ein Gastwissenschaftler forscht ein halbes Jahr am Institut, wird ins Institutsteam und in die Projekt-Site aufgenommen und fährt zurück an seine Heimatuniversität. Sein Gastgeber nimmt zwei Jahre später einen Ruf an. Das Gastkonto hat kein Ablaufdatum, das Sponsorfeld zeigt auf ein gelöscht Konto, und die letzte Anmeldung liegt Jahre zurück. Gefährlich wird es, wenn die Heimatidentität kompromittiert wird: Dann kommt ein Angreifer mit einem gültigen Gastkonto in Teams, die niemand mehr im Blick hat.

Die Bereinigung ist technisch einfach, organisatorisch zäh. Inaktive Gäste lassen sich über die letzte Anmeldung finden; eine Zugriffsüberprüfung, die nur inaktive Benutzer erfasst, nimmt dabei Arbeit ab, verlangt aber ID Governance. Wichtiger als die einmalige Aufräumaktion ist, dass neue Gäste nur noch mit Sponsor und Ablaufdatum hereinkommen. Sonst steht dieselbe Aktion in vier Jahren wieder an.

WARNUNG · Vorsicht beim Massenlöschen

Wer im ersten Schwung alle Gäste ohne Anmeldung im letzten Jahr löscht, trifft auch die externe Gutachterin, die nur einmal im Jahr für das Promotionsverfahren hereinschaut, und den Kooperationspartner, dessen Projekt gerade ruht. Deaktivieren Sie zuerst, informieren Sie die Sponsoren und löschen Sie nach einer Frist. Gelöschte Benutzer lassen sich in Entra ID eine begrenzte Zeit wiederherstellen; verlassen sollten Sie sich darauf nicht.

FAQ: Sonderrollen in Entra ID

Brauchen Gastwissenschaftler mit Gastkonto eine eigene Microsoft-365-Lizenz?

Für die Zusammenarbeit in Teams, SharePoint und OneDrive der Hochschule in der Regel nicht; der Gast nutzt die freigegebenen Ressourcen, ohne selbst lizenziert zu werden. Für Funktionen aus Entra ID gilt das Modell nach monatlich aktiven Nutzern, für exklusive Governance-Funktionen eine eigene Abrechnung je aktivem Gast. Braucht der Gast eigene Dienste wie ein Postfach der Hochschule, ist ein Mitgliedskonto mit Lizenz der richtige Weg.

Können Lehrbeauftragte nicht einfach ein Gastkonto bekommen?

Technisch ja, fachlich meist nicht. Lehrbeauftragte handeln im Namen der Hochschule, bewerten Prüfungsleistungen und brauchen Zugriff auf Systeme, die Gäste nicht erreichen. Ein Mitgliedskonto mit Semester-Laufzeit und Karenz ist sauberer als ein Gastkonto mit Ausnahmen.

Was passiert mit dem Konto eines Emeritus?

Das regelt idealerweise eine eigene Sonderrolle: Mitgliedskonto mit reduzierten Rechten, jährliche Bestätigung durch das Dekanat und eine klare Regel für den Todesfall. Welche Rechte Emeriti an Ihrer Hochschule haben, folgt aus Landesrecht und Grundordnung und ist nicht überall gleich.

Reicht ein Ablaufdatum im Active Directory?

Nein. Das lokale Ablaufdatum verhindert die Anmeldung in der Cloud nicht von selbst. Sie brauchen einen Prozess, der das Konto zum Stichtag tatsächlich deaktiviert, sei es im IdM, über einen Lebenszyklus-Workflow oder über die Laufzeit eines Zugriffspakets.

Wer darf Sponsor sein?

Eine Person oder Gruppe an der Hochschule, die den Gast kennt und den Zweck beurteilen kann, typischerweise Professoren, Institutsleitungen oder Projektleitungen. Gruppen sind robuster als Einzelpersonen. Studentische Hilfskräfte, die den Gast praktisch betreuen, sind gute Ansprechpartner, aber keine Sponsoren.

Brauchen wir für Zugriffspakete zwingend ID Governance?

Für die Grundfunktionen nicht; die sind in Entra ID P2 enthalten. Für Sponsoren als Genehmiger aus dem Benutzerprofil, automatische Zuweisungen, die Überprüfung inaktiver Benutzer und Lebenszyklus-Workflows schon. Prüfen Sie den aktuellen Stand auf learn.microsoft.com, bevor Sie planen.

Wie gehen wir mit dem Altbestand um?

Erst inventarisieren, dann deaktivieren, dann Sponsoren fragen, dann löschen. Gäste, die schon vor der Einführung von Zugriffspaketen im Tenant waren, fallen nicht automatisch unter deren Lebenszyklus und müssen eigens bereinigt oder übernommen werden.

Fazit: Jedes Konto braucht einen Paten und ein Verfallsdatum

Sonderrollen sind kein Randthema. An einer großen Universität sind es schnell einige tausend Konten, und es sind genau die, über die in keinem Quellsystem ein Ende eingetragen ist. Die Technik in Entra ID ist ausreichend: Mitgliedskonten mit Sonderrollen, Gastkonten mit Heimatidentität, Sponsoren, Zugriffspakete mit Laufzeit und Zugriffsüberprüfungen. Was fehlt, ist an vielen Hochschulen die Regel, dass ohne Sponsor und Ablaufdatum kein Konto entsteht, und ein drittes Quellsystem, das diese Regel durchsetzt.

Wer das einmal sauber aufsetzt, hat danach weniger Arbeit, nicht mehr. Die Fakultäten beantragen selbst, die Sponsoren entscheiden selbst, und das Rechenzentrum muss nicht mehr raten, wem das Konto gehört, das seit vier Jahren schweigt. Die Lehrbeauftragte aus der Wirtschaft kommt trotzdem jedes Wintersemester wieder. Nur ihr Konto weiß jetzt auch, warum.

WEITERLESEN · Weiterlesen

Die Serie zu Microsoft 365 in Hochschule und Forschung. Für diesen Beitrag besonders passend:

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#)
- › [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#)
- › [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#)
- › [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#)
- › [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)
- › [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#)
- › [Microsoft-365-Beratung für Hochschulen und Forschung](#)
- › [Microsoft-365-Schulung für Hochschulen und Forschungseinrichtungen](#)