

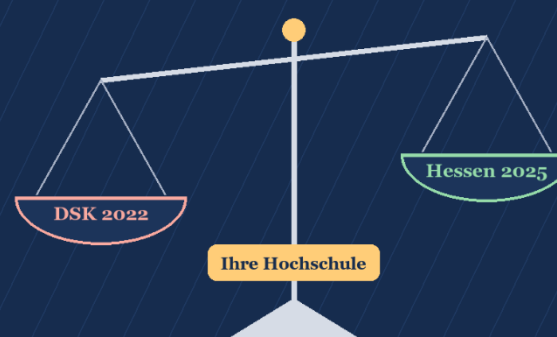
Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität

Microsoft 365 · Hochschule · Datenschutz

Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität

Sechzehn Länder, eine Datenschutzkonferenz, mehrere Meinungen – und ein Semesterstart, der auf keine davon wartet.

boddenberg.de



WISSEN

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

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

BERATUNG

Datenschutzkonzept, Dienstkatalog und Konfiguration, die vor Aufsicht und Personalrat bestehen sollen? Wir sortieren mit Ihnen.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Rechenzentrum, Datenschutz und Verwaltung: was der Tenant über wen verrät und wo man das abstellt.

› [Schulungen für Hochschulen und Forschung](#)

Fragen Sie in einer beliebigen Hochschule, ob Microsoft 365 datenschutzkonform ist, und Sie bekommen drei Antworten: Das Rechenzentrum sagt „kommt auf die Konfiguration an“, der Datenschutzbeauftragte sagt „die DSK hat doch 2022 ...“, und irgendein Professor sagt, er nutze das seit Jahren privat und lebe noch. Alle drei haben ein bisschen recht. Keiner hat eine Antwort, die man dem Präsidium vorlegen könnte, ohne dass die Kanzlerin oder der Kanzler eine Augenbraue hebt.

Dieser Beitrag sortiert die Lage nüchtern. Er erklärt, was die Datenschutzkonferenz 2022 tatsächlich festgestellt hat und was seitdem passiert ist, warum die Landesaufsichten nicht mit einer Stimme sprechen, welcher Rechtsrahmen an einer Hochschule gilt und – vor allem – was Hochschulen praktisch tun, um zwischen Aufsicht, Personalrat und Semesterstart einen vertretbaren Betrieb hinzubekommen. Den Gesamtüberblick über die Serie finden Sie auf der Seite [Microsoft 365 in Hochschule und Forschung](#). Warum der Campus generell anders tickt als eine Behörde, steht im Beitrag [Microsoft 365 an Hochschulen: Wo der Campus anders tickt als Verwaltung und Wirtschaft](#).

Zur Abgrenzung: Allgemeinbildende Schulen und ihre Schulträger sowie Universitätsklinika mit ihren Anforderungen aus dem Gesundheitswesen sind eigene Welten und bleiben hier außen vor. Und weil das Thema juristisch ist, gleich vorweg der Kasten, den niemand liest, der aber trotzdem stimmt.

HINWEIS · Keine Rechtsberatung

Dieser Beitrag beschreibt Positionen, Rechtsrahmen und Vorgehensmuster aus technischer und organisatorischer Sicht. Er ersetzt keine Rechtsberatung und keine Abstimmung mit Ihrem

Datenschutzbeauftragten, Ihrem Justiziariat oder Ihrer zuständigen Aufsichtsbehörde. Landesrecht unterscheidet sich, und die Positionen der Aufsichten entwickeln sich weiter. Maßgeblich ist der Stand in Ihrem Land zum Zeitpunkt Ihrer Entscheidung.

Die Lage: Was die DSK festgestellt hat und was seitdem passiert ist

Die Festlegung vom 24. November 2022

Am 24. November 2022 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, kurz DSK, den Bericht ihrer Arbeitsgruppe „Microsoft-Onlinedienste“ zur Kenntnis genommen und eine Festlegung getroffen. Deren Kern ist ein einziger Satz, der seitdem in jeder zweiten Senatssitzung zitiert wird – meist ungenau. Die DSK stellte fest, dass Verantwortliche den Nachweis, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des damaligen Datenschutznachtrags vom 15. September 2022 nicht führen können. Solange insbesondere die Transparenz über die Verarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt sei, könne dieser Nachweis nicht erbracht werden.

Bemerkenswert ist, was die Festlegung nicht sagt. Sie ist kein Verbot. Sie richtet sich nicht gegen eine einzelne Hochschule. Sie bewertet einen Vertragsstand, nicht die Software an sich. Und sie verschiebt die Last dorthin, wo sie nach der DSGVO ohnehin liegt: zum Verantwortlichen, der nachweisen muss, dass er die Grundsätze einhält. Das ist juristisch sauber und praktisch unangenehm, denn „Sie müssen nachweisen“ ist für ein Rechenzentrum ungefähr so beruhigend wie ein Brief vom Rechnungshof, der mit „Wir bitten um Stellungnahme“ beginnt.

FAKTEN · Was belegt ist (Stand Oktober 2026)

Datenschutzkonferenz: Festlegung vom 24.11.2022 – Nachweis eines datenschutzkonformen Betriebs auf Basis des Datenschutznachtrags vom 15.09.2022 nicht führbar, vor allem wegen fehlender Transparenz über die Verarbeitung für Microsofts eigene Zwecke.

Bereits im September 2020 war eine Bewertung der DSK zu dem Schluss gekommen, dass ein datenschutzgerechter Einsatz von Office 365 auf der damaligen Vertragsgrundlage nicht möglich sei.

Landesaufsicht Niedersachsen: im September 2023 Praxis-Tipps für Verträge mit Microsoft, erarbeitet zusammen mit sechs weiteren Aufsichtsbehörden – etwa zu Löschfristen, Unterauftragsverarbeitern und Verarbeitung zu eigenen Zwecken.

Microsoft: EU Data Boundary in drei Phasen, Phase 1 ab Januar 2023, Abschluss im Februar 2025.

Hessische Aufsicht (HBDI): Bericht vom 15.11.2025 – Microsoft 365 kann in Hessen unter Bedingungen datenschutzkonform genutzt werden.

Eine neue gemeinsame Bewertung der DSK zu Microsoft 365 haben wir auf der Website der DSK bis Redaktionsschluss nicht gefunden.

Was sich seitdem bewegt hat

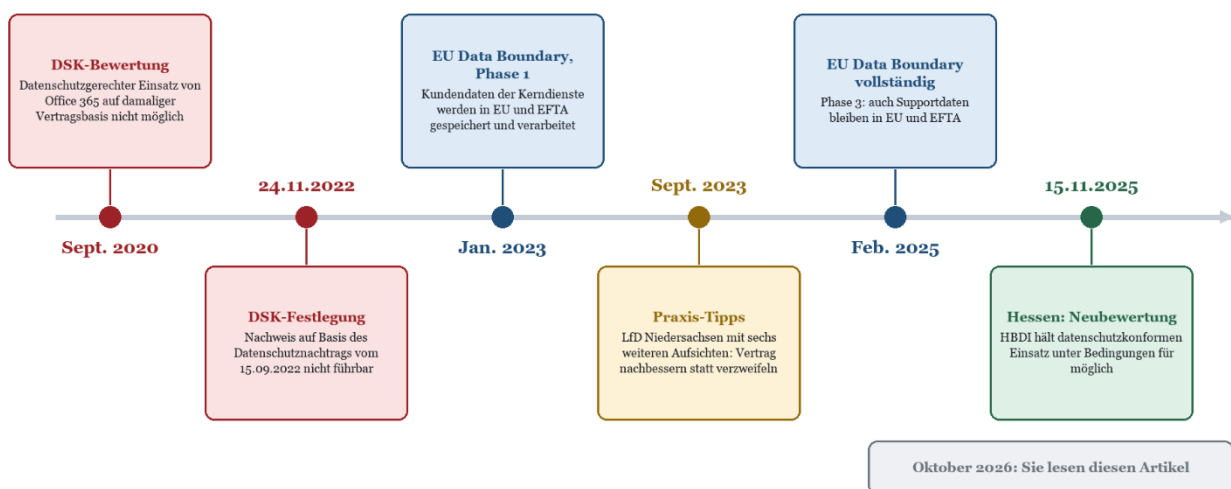
Seit 2022 hat sich an drei Stellen etwas verändert. Erstens die Datenflüsse: Microsoft hat die EU Data Boundary for the Microsoft Cloud in drei Phasen umgesetzt. Phase 1 ab Januar 2023 betraf Kundendaten der Kerndienste, darunter Microsoft 365. Mit Phase 3 im Februar 2025 werden nach Angaben von Microsoft auch Supportdaten – etwa Protokolle, die Kunden im Supportfall bereitstellen, und Notizen der Supportmitarbeiter – in der EU und EFTA gespeichert. Microsoft dokumentiert selbst, in welchen Fällen Daten die Grenze dennoch verlassen können, etwa bei

bestimmten Sicherheitsfunktionen. Die Data Boundary ist also eine Residenzzusage mit Fußnoten, keine Mauer.

Zweitens der Rechtsrahmen für Übermittlungen in die USA: Mit dem EU-US Data Privacy Framework existiert wieder ein Angemessenheitsbeschluss der EU-Kommission für zertifizierte US-Unternehmen. Ob er hält, wird man sehen; seine beiden Vorgänger haben es bekanntlich nicht bis zur Pensionierung geschafft. Für die Bewertung heute ist er aber geltendes Recht. Drittens die Verträge: Microsoft hat seinen Datenschutznachtrag mehrfach überarbeitet. Welche Fassung für Ihre Hochschule gilt, hängt davon ab, über welchen Vertrag Sie lizenzieren und wann Sie zuletzt verlängert haben – eine Frage, die man im Rechenzentrum gelegentlich erst beantworten kann, nachdem man die Beschaffung gefragt hat, die wiederum den Lizenzpartner fragt.

Skizze 1: Wie sich die Lage seit 2020 verschoben hat

Nur Ereignisse, die in Primärquellen belegt sind. Was dazwischen in Gremien geschah, ist Stoff für Memoiren.



Rot: Aufsicht skeptisch. Blau: Microsoft liefert. Gelb: Aufsicht hilft. Grün: eine Aufsicht dreht.

Hessen 2025: eine Aufsicht bewertet neu

Am 15. November 2025 hat der Hessische Beauftragte für Datenschutz und Informationsfreiheit einen Bericht veröffentlicht, nach dem Microsoft 365 in Hessen unter bestimmten Bedingungen datenschutzkonform genutzt werden kann. Vorausgegangen waren Gespräche mit Microsoft seit Anfang 2025. Die hessische Aufsicht hat die Kritikpunkte der DSK von 2022 einzeln neu bewertet und verweist auf die veränderten Rahmenbedingungen: Data Privacy Framework, EU Data Boundary, überarbeiteter Datenschutznachtrag. Nach ihrer Darstellung nutzt Microsoft für eigene Geschäftszwecke nur noch Protokoll- und Diagnosedaten, nicht aber Inhaltsdaten, und diese nur anonymisiert beziehungsweise aggregiert. Microsoft stellt zudem Dokumentationshilfen bereit.

Entscheidend für Sie ist das Kleingedruckte. Die Bewertung setzt voraus, dass die Verantwortlichen ihren Teil erledigen: konfigurieren, dokumentieren, Risiken bewerten. Sie ist kein Gütesiegel, das man ausdrucken und an die Tür des Rechenzentrums kleben kann. Und sie stammt von einer Landesaufsicht. Sie bindet keine andere Aufsichtsbehörde, auch wenn die hessische Aufsicht ihre Ergebnisse den Kolleginnen und Kollegen anderer Länder zur Verfügung stellt. Kritiker haben ihr vorgeworfen, sich zu sehr auf Vertragstexte zu stützen und zu wenig auf überprüfte tatsächliche Datenflüsse. Diese Debatte wird Ihnen in der nächsten Sitzung des Datenschutzausschusses begegnen, wenn es einen gibt.

WICHTIG · Hessen ist nicht Deutschland – und Ihr Land ist nicht Hessen

Hochschulen eines Landes unterliegen in aller Regel der Aufsicht ihres Landes. Eine Hochschule in

einem anderen Bundesland kann sich auf die hessische Bewertung als Argument stützen, nicht als Rechtsgrundlage. Fragen Sie im Zweifel Ihre eigene Aufsicht, wie sie die veränderte Lage einschätzt. Dass dabei unterschiedliche Antworten herauskommen, ist kein Fehler des Föderalismus, sondern seine Betriebsanleitung.

Sechzehn Länder, mehrere Linien

Die Landesaufsichten sind unabhängig, und sie nutzen diese Unabhängigkeit. Statt eine Landkarte zu zeichnen, die beim Erscheinen schon veraltet wäre, lohnt sich ein Blick auf die Muster, die sich in Stellungnahmen, Tätigkeitsberichten und Gesprächen zeigen. Welches Muster Ihre Aufsicht gerade verfolgt, erfahren Sie aus deren aktuellem Tätigkeitsbericht und – zuverlässiger – aus einem Gespräch.

Lesart der Aufsicht	Was sie typischerweise sagt	Was das für Sie heißt
Festlegung von 2022 gilt fort	Nachweis weiterhin schwer, Verantwortliche tragen das volle Risiko	Dokumentation besonders gründlich, Datenschutz-Folgenabschätzung, Alternativen benennen
Vertrag nachbessern	Standardvertrag reicht nicht, Ergänzungen zu Löschung, Unterauftragnehmern, eigenen Zwecken	Prüfen, ob Ihr Rahmenvertrag solche Ergänzungen enthält oder ermöglicht
Neubewertung unter Bedingungen	Einsatz möglich, wenn konfiguriert, dokumentiert und überwacht wird	Konfiguration ist kein Nice-to-have, sondern Teil der Rechtmäßigkeit
Einzelfallbetrachtung	Keine pauschale Aussage, es kommt auf Dienst, Daten und Personengruppen an	Abgestufte Freigabe und Dienststeckbriefe sind Ihr bestes Argument

Der Rechtsrahmen: DSGVO, Landesdatenschutzgesetz und Hochschulgesetz

Eine staatliche Hochschule ist eine öffentliche Stelle des Landes. Das klingt banal, hat aber Folgen: Neben der DSGVO gilt nicht das Bundesdatenschutzgesetz, sondern in erster Linie das Landesdatenschutzgesetz, ergänzt um das Hochschulgesetz des Landes und die Satzungen der Hochschule. Die Verarbeitung stützt sich meist auf die Erfüllung einer Aufgabe im öffentlichen Interesse nach Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit einer Norm des Landesrechts, die diese Aufgabe beschreibt. Welche Norm das ist und wie konkret sie die Datenverarbeitung regelt, unterscheidet sich von Land zu Land erheblich.

Wer welches Recht anwendet

Einrichtung	Datenschutzrecht neben der DSGVO	Aufsicht in der Regel
Staatliche Universität, HAW, Kunst- oder Musikhochschule	Landesdatenschutzgesetz, Hochschulgesetz, Satzungen der Hochschule	Landesbeauftragte oder Landesbeauftragter für Datenschutz
Staatlich anerkannte private Hochschule	Bundesdatenschutzgesetz, ergänzend landesrechtliche Vorgaben zur Anerkennung	Aufsicht für den nicht-öffentlichen Bereich im jeweiligen Land
Kirchliche Hochschule	Kirchliches Datenschutzrecht, sofern der Träger eigenes Recht anwendet	Kirchliche Datenschutzaufsicht
Außeruniversitäres Institut	Je nach Rechtsform Bundesdatenschutzgesetz oder Landesrecht	Je nach Rechtsform und Sitz unterschiedlich

Für kirchliche Träger lohnt ein Blick in unseren Kompetenzbereich [Microsoft 365 in Kirche, Diakonie und Caritas](#), für außeruniversitäre Institute in den Beitrag [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#). Die Rechtsform entscheidet dort nicht nur über die Lizenz, sondern auch darüber, wer Ihnen auf die Finger schaut.

Was das Hochschulgesetz beiträgt – und was nicht

Die Hochschulgesetze der Länder enthalten Regeln zur Verarbeitung von Daten der Studenten, von der Bewerbung über Immatrikulation und Prüfungen bis zur Exmatrikulation, und häufig eine Ermächtigung, Einzelheiten durch Satzung zu regeln. Manche Länder haben nach der Pandemie ausdrücklich Regeln zu elektronischen Lehr- und Prüfungsformaten ergänzt, andere überlassen das den Hochschulsatzungen oder allgemeinen Normen. Wie weit eine solche Norm trägt, ob sie etwa auch eine Pflicht zur Nutzung eines bestimmten Cloud-Dienstes abdeckt, ist eine Frage für Ihr Justizariat, nicht für das Rechenzentrum.

Für die Mitarbeiterinnen und Mitarbeiter kommt das Dienstrecht hinzu, für die Datenverarbeitung im Dienstverhältnis gelten landesrechtliche Regeln auf Grundlage von Art. 88 DSGVO, und das Personalvertretungsgesetz des Landes regelt, wann der Personalrat mitbestimmt. Die Mitbestimmung ist bei Microsoft 365 praktisch immer berührt, weil die Systeme objektiv geeignet sind, Verhalten und Leistung zu überwachen. Wie man das aufsetzt, beschreibt der Beitrag [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#).

Auftragsverarbeitung: der Vertrag, über den alle reden

Microsoft verarbeitet die Daten Ihrer Hochschule als Auftragsverarbeiter nach Art. 28 DSGVO. Die Grundlage ist der Datenschutznachtrag, der in die Produktbedingungen eingebunden ist und über Ihren Lizenzvertrag gilt. Sie verhandeln ihn als einzelne Hochschule praktisch nicht nach. Was Sie tun können: prüfen, welche Fassung gilt, die Liste der Unterauftragsverarbeiter kennen und beobachten, die Datenkategorien Ihrer Dienste dokumentieren und die Stellen identifizieren, an denen Microsoft als eigener Verantwortlicher handelt. Genau dort lag 2022 der Hauptkritikpunkt der DSK.

Ein Rahmenvertrag auf Bundes- oder Landesebene kann zusätzliche Regelungen enthalten. Ob und welche, sollten Sie anhand des Vertragstextes klären und nicht anhand dessen, was jemand auf einer Tagung erzählt hat. Lizenzen und Verträge behandeln eigene Beiträge dieser Serie; hier genügt die Feststellung, dass der Vertrag die Voraussetzung ist, nicht die Lösung.

Datenschutz-Folgenabschätzung: Pflicht, Kür oder Selbstschutz

Ob für Microsoft 365 insgesamt oder für einzelne Dienste eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich ist, hängt von Art, Umfang und Zweck der Verarbeitung ab. Bei einer Hochschule mit zehntausenden Studenten, Kommunikationsinhalten, möglicher Verhaltensauswertung und Übermittlungsrisiken in Drittländer kommen mehrere Kriterien zusammen, die die Aufsichts in ihren Listen für Verarbeitungen mit Folgenabschätzung nennen. In der Praxis führen viele Hochschulen sie deshalb ohnehin durch – nicht nur, weil sie es müssen, sondern weil die Folgenabschätzung das einzige Dokument ist, in dem Risiken und Gegenmaßnahmen einmal vollständig an einem Ort stehen.

Bewährt hat sich ein Aufbau in zwei Ebenen: eine Rahmen-Folgenabschätzung für die Plattform mit Vertrag, Datenflüssen, Datenresidenz, Identitäten und Grundkonfiguration, und darunter schlanke Ergänzungen je Dienst oder Funktion, etwa für Teams-Aufzeichnungen oder Copilot. So muss nicht bei jeder neuen Funktion das ganze Gebäude neu begutachtet werden, nur der Anbau.

TIPP · Dokumentationshilfen nutzen, aber nicht abschreiben

Microsoft und mehrere Aufsichten stellen Material bereit, das bei der Dokumentation hilft. Es ist ein guter Steinbruch. Eine Folgenabschätzung, in der „Ihre Organisation“ steht, wo „Fachbereich Physik“ stehen müsste, erkennt allerdings jeder Datenschutzbeauftragte nach drei Absätzen – und jede Aufsicht nach zwei.

Personengruppen: Wer eigentlich worin einwilligt

Eine Hochschule ist kein Unternehmen mit einer Belegschaft, sondern ein Gemeinwesen mit sehr unterschiedlichen Menschen: Studenten, Mitarbeiterinnen und Mitarbeiter in Verwaltung und Technik, Professoren und wissenschaftliche Mitarbeiter, studentische Hilfskräfte, Lehrbeauftragte, Gastwissenschaftler, Emeriti, Alumni, Bewerber in Berufungsverfahren. Für jede dieser Gruppen sieht die Rechtsgrundlage anders aus. Wer das ignoriert, landet beim beliebtesten Fehler im Hochschuldatenschutz: der Einwilligung als Allzweckwaffe.

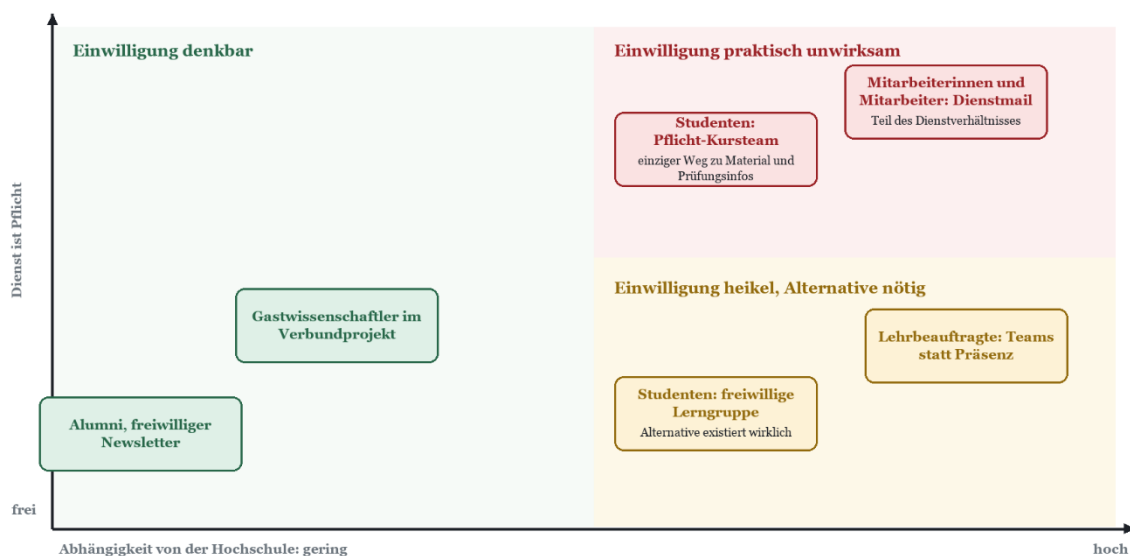
Warum die Einwilligung bei Pflichtdiensten nicht trägt

Eine Einwilligung ist nach der DSGVO nur wirksam, wenn sie freiwillig ist. Die DSGVO selbst weist darauf hin, dass bei einem klaren Ungleichgewicht, insbesondere gegenüber Behörden, Freiwilligkeit zweifelhaft ist. Wenn Kursmaterial, Prüfungsinformationen und die Kommunikation mit dem Prüfungsamt ausschließlich über ein Teams-Team laufen, kann ein Student nicht wirksam nein sagen, ohne sein Studium zu gefährden. Ein Häkchen beim ersten Login ändert daran nichts. Es dokumentiert nur, dass jemand weitergeklickt hat – was im Ernstfall eher gegen als für die Hochschule spricht.

Für Pflichtdienste braucht es deshalb eine gesetzliche Grundlage: die Aufgabe der Hochschule nach Hochschulgesetz, gegebenenfalls konkretisiert durch Satzung, und eine Verarbeitung, die für diese Aufgabe erforderlich ist. Wo die Grundlage dünn ist, hilft eine echte Alternative: Material auch im LMS, Sprechstunde auch per Mail oder vor Ort. Dann wird aus dem Pflichtdienst ein Angebot, und für Angebote kann die Einwilligung wieder ein Werkzeug sein. Die Grenze zwischen Teams und LMS beschreibt der Beitrag [Teams in Lehre und Hochschulverwaltung: Kursteams, Aufzeichnungen und die Grenze zum LMS](#).

Skizze 2: Wer kann bei welchem Dienst wirksam „ja“ sagen?

Schematisch: Je weiter rechts, desto abhängiger ist die Person von der Hochschule – und desto wertloser die Einwilligung.



Merksatz: Wer nicht nein sagen kann, sagt auch nicht wirksam ja. Rechtsgrundlage dann: Gesetz, nicht Häkchen.

Personengruppe	Typische Rechtsgrundlage	Einwilligung realistisch?	Was daraus folgt
Studenten	Aufgabe der Hochschule nach Hochschulgesetz und Satzung	Nur bei echten Zusatzangeboten	Pflichtdienste gesetzlich abstützen, Alternativen anbieten, Informationspflichten ernst nehmen
Mitarbeiterinnen und Mitarbeiter	Dienstverhältnis, Landesrecht zum Datenschutz im Dienstverhältnis	Kaum, Abhängigkeitsverhältnis	Dienstvereinbarung mit dem Personalrat, Zweckbindung, keine Verhaltensauswertung
Professoren und Wissenschaftler	Dienstverhältnis, zusätzlich Freiheit von Forschung und Lehre	Eingeschränkt	Werkzeugwahl in der Lehre respektieren, Mindeststandard für Verwaltungskommunikation
Studentische Hilfskräfte	Arbeitsverhältnis und zugleich Studentenstatus	Kaum	Zwei Rollen, zwei Konten oder klare Trennung im Konto
Lehrbeauftragte, Gastwissenschaftler, Emeriti	Vertrag, Kooperation oder mitgliedschaftsähnliche Stellung	Teilweise	Befristung, Verantwortliche im Institut, Zugriffsumfang begrenzen
Alumni, Externe, Bewerber	Je nach Zweck: Einwilligung, Vertrag oder Verfahren	Ja, wenn freiwillig	Bewerberdaten aus Berufungsverfahren nicht in allgemeine Teams-Kanäle

Für die Sonderrollen gilt: Je kürzer jemand bleibt, desto wichtiger ist das Ablaufdatum. Wie man Gäste, Lehrbeauftragte und Emeriti in Entra ID abbildet, ohne dass Konten von Verstorbenen noch Jahre später Teams-Einladungen bekommen, steht im Beitrag [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#).

TYPISCHE SITUATION · Die Einwilligung, die keiner verweigern konnte

Typische Situation aus einem kommunalen Verband: Für eine neue Kollaborationsplattform sollten alle Mitarbeiterinnen und Mitarbeiter beim ersten Login einwilligen. Nach drei Wochen lag die Quote

bei hundert Prozent, was die Projektleitung als Erfolg meldete. Der Datenschutzbeauftragte meldete dasselbe als Problem: Wer nicht klickte, kam nicht an seine Dienstpost. Die Lösung war unspektakulär – Rechtsgrundlage Dienstverhältnis plus Dienstvereinbarung, Einwilligung nur noch für freiwillige Zusatzfunktionen.

Auf die Hochschule übertragen: Wenn Ihr Einwilligungsdialog eine Quote von hundert Prozent erreicht, sollten Sie nicht feiern, sondern prüfen, ob irgendwer überhaupt nein sagen konnte.

Was Hochschulen praktisch tun

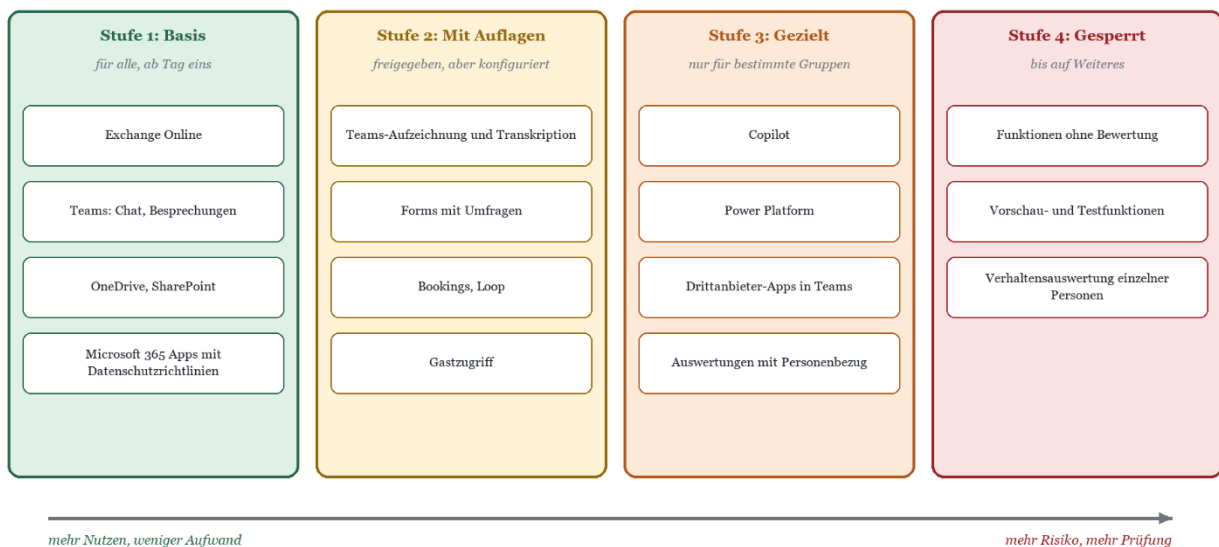
Zwischen „wir warten, bis die DSK sich einig ist“ und „wir schalten alles ein, die anderen machen das auch“ liegt ein breiter Korridor. In ihm bewegen sich die meisten Hochschulen, die Microsoft 365 produktiv nutzen. Drei Muster wiederholen sich: Dienste werden abgestuft freigegeben, die Datenschutzeinstellungen werden zentral gesetzt statt dem Zufall überlassen, und besonders schützenswerte Daten bekommen eigene Regeln oder bleiben draußen.

Dienste abgestuft freigeben

Microsoft 365 ist kein Produkt, sondern ein Warenhaus. Niemand muss alle Abteilungen gleichzeitig eröffnen. Eine Freigabe in Stufen – Basisdienste für alle, weitere Dienste mit Auflagen, bestimmte Funktionen nur für einzelne Gruppen, der Rest gesperrt – macht das Risiko beherrschbar und die Dokumentation überschaubar. Sie hat außerdem einen politischen Vorteil: Im Senat lässt sich über einen Dienstkatalog mit vier Stufen deutlich sachlicher streiten als über „Microsoft ja oder nein“.

Skizze 3: Dienste abgestuft freigeben

Beispielhafte Einordnung. Welcher Dienst in welcher Stufe landet, entscheidet Ihre Bewertung – nicht diese Skizze.



Ein Dienst darf die Stufe wechseln. Nach oben häufiger, als man denkt.

Technisch stehen dafür Lizenzzuweisung über Gruppen, das Deaktivieren einzelner Dienstpläne innerhalb einer Lizenz, App-Richtlinien in Teams und die Steuerung von Unternehmensanwendungen in Entra ID zur Verfügung. Die Stufen sollten sich in Gruppen abbilden lassen, die aus dem Identitätsmanagement gespeist werden – sonst pflegt irgendwann jemand die Copilot-Freigaben in einer Excel-Tabelle, und das ist der Anfang vom Ende.

Dienst, Risiko, Stellschraube

Die folgende Übersicht ist kein Freigabekatalog, sondern eine Arbeitsgrundlage für Ihre eigene Bewertung. Sie nennt je Dienst das Risiko, das in Hochschulen typischerweise diskutiert wird, und die Stellschraube, mit der man ihm begegnet.

Dienst	Typisches Risiko	Stellschraube
Exchange Online	Dienstliche und private Kommunikation vermischt, Weiterleitung an externe Postfächer	Automatische Weiterleitung nach außen unterbinden, Aufbewahrung regeln, Nutzungsregeln
Teams: Chat und Besprechungen	Präsenz- und Aktivitätsinformationen als Verhaltensdaten, offene Besprechungen	Lobby-Einstellungen, Präsenzanzeige in Dienstvereinbarung regeln, Gastzugriff gezielt
Teams: Aufzeichnung und Transkription	Bild, Stimme und Wortbeiträge von Studenten, unklare Speicherdauer	Aufzeichnung nur für bestimmte Rollen, Ablaufdatum für Aufzeichnungen, Hinweis vorab
OneDrive und SharePoint	Freigaben an „Jeden mit dem Link“, Daten Ausgeschiedener bleiben liegen	Freigabelinks einschränken, Standard auf intern, Aufbewahrung und Löschung beim Austritt
Forms	Umfragen mit Gesundheits- oder Prüfungsdaten, anonym gedacht, nicht anonym umgesetzt	Vorlagen und Schulung, sensible Erhebungen über dafür vorgesehene Werkzeuge
Microsoft 365 Apps	Diagnosedaten, optionale verbundene Dienste, die Inhalte an Clouddienste senden	Diagnosedatenebene und verbundene Dienste per Richtlinie festlegen
Nutzungsberichte im Admin Center	Auswertung einzelner Personen durch Administratoren	Namen in Berichten verbergen, Zugriff auf Berichte rollenbasiert und protokolliert
Copilot	Überberechtigte Freigaben werden plötzlich auffindbar, Personalratsfrage	Berechtigungen vorher bereinigen, nur für definierte Gruppen, eigene Bewertung
Power Platform und Drittanbieter-Apps	Datenabflüsse zu weiteren Anbietern, Schatten-IT mit Konnektoren	Zustimmung für Apps durch Administratoren, Richtlinien zur Verhinderung von Datenverlust

WARNUNG · Aufzeichnungen sind die Wurzel vieler Beschwerden

Eine Vorlesung aufzuzeichnen ist das eine. Eine Seminardiskussion mit Wortbeiträgen von Studenten aufzuzeichnen und für unbestimmte Zeit im OneDrive eines Dozenten liegen zu lassen, ist etwas ganz anderes. Regeln Sie, wer aufzeichnen darf, wie Teilnehmer vorher informiert werden und wann Aufzeichnungen ablaufen – bevor die erste Beschwerde bei der Aufsicht landet und nicht danach.

Telemetrie und optionale verbundene Dienste konfigurieren

Die Microsoft 365 Apps senden Diagnosedaten an Microsoft. Administratoren können per Richtlinie festlegen, auf welcher Ebene das geschieht: erforderliche Diagnosedaten, zusätzlich optionale Diagnosedaten oder keine. Ist nichts konfiguriert, sendet der Client standardmäßig auch optionale Diagnosedaten. Benutzer, die mit ihrem Hochschulkonto angemeldet sind, können die Ebene auf ihrem Gerät nicht selbst ändern. Das ist gut, wenn Sie sich entschieden haben, und schlecht, wenn nicht.

Daneben gibt es die verbundenen Dienste: Funktionen, die Inhalte an Clouddienste senden, etwa für Übersetzung, Designvorschläge oder Diktat. Microsoft trennt Dienste, die Inhalte analysieren, Dienste, die Online-Inhalte herunterladen, und zusätzliche optionale verbundene Dienste. Jede

Gruppe lässt sich per Richtlinie ein- oder ausschalten. Ist die Richtlinie für optionale verbundene Dienste nicht gesetzt, stehen sie den Benutzern zur Verfügung. Die Einstellungen lassen sich über Gruppenrichtlinien, Intune oder den Cloudrichtliniendienst für Microsoft 365 verteilen – letzterer auch für Geräte, die die Hochschule nicht verwaltet, solange sich jemand mit dem Hochschulkonto anmeldet. Die Einzelheiten beschreibt Microsoft in der [Übersicht der Datenschutzeinstellungen für Microsoft 365 Apps](#).

TIPP · Die Datenschutzeinstellungen als eigene Konfigurationsseite dokumentieren

Legen Sie für jede Datenschutzrichtlinie fest: gewählter Wert, Begründung, wer entschieden hat, wann geprüft. Eine Seite, nicht mehr. Diese Seite ist im Gespräch mit Aufsicht und Personalrat mehr wert als jede Präsentation – und beim nächsten Wechsel im Rechenzentrum der einzige Grund, warum niemand die Einstellungen „mal eben zurücksetzt“.

Telemetrie gibt es nicht nur in den Apps. Auch Windows, die mobilen Apps und die Administrationsoberflächen erzeugen Daten über Nutzung und Verhalten. Im Admin Center lässt sich einstellen, dass Benutzer-, Gruppen- und Webseitenamen in Nutzungsberichten verborgen werden. Für Hochschulen mit Personalrat ist das kein Detail, sondern meist ein Punkt der Dienstvereinbarung.

Was nicht in den Tenant gehört – oder nur mit eigenen Regeln

Nicht jede Datenart passt in jeden Dienst. Prüfungsakten, Berufungsunterlagen, Personalvorgänge, Gesundheitsdaten aus Studien oder Daten mit Exportkontrollbezug brauchen eigene Regeln: Klassifizierung, eingeschränkte Bereiche, Verschlüsselung oder schlicht ein anderes System. Das ist keine Niederlage für Microsoft 365, sondern normales Informationsmanagement. Vertiefend dazu: [Prüfungsdaten, Berufungsakten, Personalvorgänge: Besonders schützenswerte Daten im Hochschul-Tenant](#) und [Forschungsdaten in Microsoft 365: Was geht, was nicht, und wo das Forschungsdatenmanagement beginnt](#).

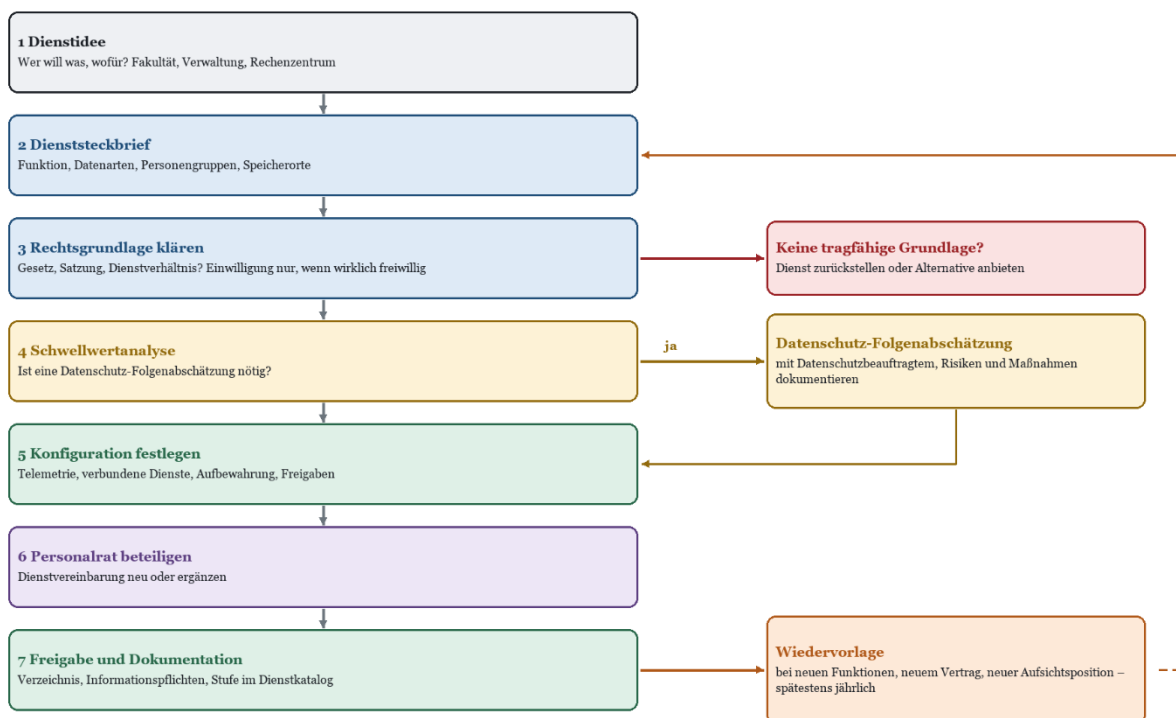
Und wo Microsoft 365 nicht passt, läuft an Hochschulen ohnehin längst etwas anderes: Nextcloud für die Ablage, Moodle oder ILIAS als LMS, BigBlueButton für Lehrveranstaltungen, Matrix für den Chat. Koexistenz ist der Normalfall, nicht die Ausnahme. Wie man die Grenzen zieht, beschreibt [Microsoft 365 oder Open Source? Koexistenz mit BigBlueButton, Nextcloud, Moodle und Matrix](#).

Von der Dienstidee zur Freigabe: der Entscheidungsweg

Die meisten Datenschutzprobleme mit Microsoft 365 entstehen nicht durch böse Absicht, sondern durch Abkürzungen. Ein Lehrstuhl findet eine Funktion praktisch, ein Admin schaltet sie ein, und ein halbes Jahr später fragt der Datenschutzbeauftragte, wer das genehmigt hat. Die Antwort „niemand, es war ja schon da“ ist ehrlich, aber nicht hilfreich. Ein verbindlicher Weg von der Dienstidee bis zur Freigabe verhindert das – und er muss nicht bürokratisch sein, nur verbindlich.

Skizze 4: Von der Dienstidee bis zur Freigabe

Ein Weg, kein Naturgesetz. Reihenfolge und Zuständigkeiten regelt Ihre Hochschule selbst.



Der häufigste Fehler: mit Schritt 5 anfangen, weil die Admins ihn am besten können.

Wer an welchem Schritt beteiligt ist

Rolle	Beitrag im Entscheidungsweg
Hochschulrechenzentrum	Dienststeckbrief, technische Bewertung, Konfiguration, Betrieb und Protokollierung
Datenschutzbeauftragter	Beratung zur Rechtsgrundlage, Schwellwertanalyse, Begleitung der Folgenabschätzung
Justizariat	Auslegung von Hochschulgesetz, Satzung und Vertrag, Satzungsänderungen vorbereiten
Personalrat	Mitbestimmung, Dienstvereinbarung, Prüfung auf Leistungs- und Verhaltenskontrolle
Kanzler und Präsidium bzw. Rektorat	Verantwortung als Verantwortlicher, Freigabeentscheidung, Ressourcen
Fakultäten und Fachbereiche	Bedarf formulieren, Pilotgruppen stellen, Regeln in Lehre und Forschung umsetzen
Informationssicherheit	Schutzbedarf, Sicherheitsmaßnahmen, Abgleich mit dem Sicherheitskonzept

TYPISCHE SITUATION · Die Folgenabschätzung als lebendes Dokument

Typische Situation aus einer Stadtverwaltung: Die Datenschutz-Folgenabschätzung für die Plattform war gründlich, abgestimmt und wurde feierlich abgeheftet. Zwei Jahre später hatte der Hersteller ein Dutzend neue Funktionen ausgerollt, drei davon mit eigenen Datenflüssen, und niemand hatte nachgezogen. Erst eine neue Aufzeichnungsfunktion fiel dem Personalrat auf. Seitdem gibt es dort eine Wiedervorlage im Quartal: Was ist neu, was ändert sich, welche Stufe? Eine Stunde, drei Beteiligte, ein Protokoll.

Auf die Hochschule übertragen: Das Nachrichtencenter im Admin Center ist Ihr Frühwarnsystem.

Wer es liest, erfährt von neuen Funktionen, bevor Studenten sie in Social Media finden.

Wie Kommunen und Landesbehörden mit derselben Frage umgehen, mit anderem Personal, aber oft derselben Aufsicht, zeigt unser Kompetenzbereich [Microsoft 365 in der öffentlichen Verwaltung](#). Ein Blick über den Zaun lohnt sich, gerade weil die Verwaltung beim Thema Dienstvereinbarung meist ein paar Jahre Vorsprung hat. Wenn Sie den Weg für Ihre Hochschule aufsetzen oder eine vorhandene Bewertung prüfen lassen wollen, unterstützen wir Sie mit [Microsoft-365-Beratung für Hochschulen und Forschung](#); für Rechenzentrum, Datenschutz und Verwaltung gibt es passende [Microsoft-365-Schulungen für Hochschulen und Forschungseinrichtungen](#).

Einen größeren Rahmen für diesen Entscheidungsweg, inklusive Vorlage für das Präsidium, beschreibt der Beitrag [Microsoft-365-Einführung an der Hochschule: Konzeptionsphase in 4,5 Tagen und die Vorlage fürs Präsidium](#). Und wer die Datenschutzfrage mit der grundsätzlichen Frage nach Abhängigkeiten verbindet, findet in [Digitale Souveränität an Hochschulen: Was realistisch ist und was Sonntagsrede bleibt](#) die ehrliche Fortsetzung.

FAQ: Microsoft 365 und Datenschutz an der Hochschule

Hat die DSK Microsoft 365 an Hochschulen verboten?

Nein. Die DSK hat am 24. November 2022 festgestellt, dass Verantwortliche den Nachweis eines datenschutzkonformen Betriebs auf Grundlage des damaligen Datenschutznachtrags nicht führen können. Das ist eine Bewertung eines Vertragsstands, kein Verbot. Die Pflicht zum Nachweis liegt bei Ihrer Hochschule als Verantwortlicher.

Gilt die hessische Neubewertung auch in unserem Land?

Nicht unmittelbar. Die Bewertung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit vom 15. November 2025 betrifft seinen Zuständigkeitsbereich. Sie ist ein gewichtiges Argument, aber Ihre eigene Landesaufsicht kann zu einer anderen Einschätzung kommen. Fragen Sie im Zweifel nach.

Reicht die EU Data Boundary für einen datenschutzkonformen Betrieb?

Nein, sie ist ein Baustein. Sie regelt, wo Daten gespeichert und verarbeitet werden, mit dokumentierten Ausnahmen. Rechtsgrundlage, Konfiguration, Zweckbindung, Löschung und Mitbestimmung bleiben Ihre Aufgabe.

Können Studenten in die Nutzung von Teams einwilligen?

Nur, wenn sie wirklich die Wahl haben. Ist Teams der einzige Weg zu Lehrmaterial oder Prüfungsinformationen, ist die Einwilligung nicht freiwillig. Dann braucht es eine gesetzliche Grundlage aus Hochschulgesetz und Satzung oder eine echte Alternative.

Brauchen wir eine Datenschutz-Folgenabschätzung?

In vielen Fällen ja, und auch wo es zweifelhaft ist, lohnt sie sich. Bewährt hat sich eine Rahmen-Folgenabschätzung für die Plattform und ergänzende Bewertungen für einzelne Dienste wie Aufzeichnungen oder Copilot. Die Schwellwertanalyse sollte Ihr Datenschutzbeauftragter begleiten.

Welche Einstellungen sollten wir zuerst setzen?

Diagnosedatenebene und verbundene Dienste der Microsoft 365 Apps per Richtlinie, Freigabelinks in OneDrive und SharePoint, Gastzugriff, Aufzeichnungsrechte in Teams und das Verbergen von Namen in Nutzungsberichten. Entscheidend ist weniger die Reihenfolge als dass jede Entscheidung dokumentiert ist.

Dürfen Professoren in der Lehre auf Microsoft 365 verzichten?

Die Freiheit von Forschung und Lehre lässt in der Werkzeugwahl Spielraum. Für die Kommunikation mit der Verwaltung und für Prüfungsabläufe kann die Hochschule verbindliche Wege festlegen. Wo die Grenze verläuft, ist eine Frage des Landesrechts und der Satzung.

Wie oft müssen wir die Bewertung erneuern?

Immer dann, wenn sich etwas Wesentliches ändert: neuer Vertrag, neue Funktionen mit eigenen Datenflüssen, neue Position Ihrer Aufsicht. Unabhängig davon empfiehlt sich eine regelmäßige Wiedervorlage, mindestens jährlich.

Fazit: Nicht auf die eine Antwort warten

Die Frage „Ist Microsoft 365 datenschutzkonform?“ wird Ihnen niemand mit Ja oder Nein beantworten, der seriös bleiben will. Die DSK hat 2022 einen Vertragsstand bewertet, Microsoft hat Datenflüsse und Verträge seitdem verändert, eine Landesaufsicht hat neu bewertet, andere halten sich bedeckt. Wer auf die bundeseinheitliche Erlösung wartet, wartet möglicherweise bis zur Emeritierung – und betreibt bis dahin ohnehin irgendeine Form von Microsoft 365, nur eben undokumentiert.

Tragfähiger ist der Weg, den viele Hochschulen gehen: Rechtsgrundlage je Personengruppe klären, Dienste abgestuft freigeben, Datenschutzeinstellungen zentral setzen und dokumentieren, eine Folgenabschätzung, die lebt, eine Dienstvereinbarung, die hält, und ein verbindlicher Weg von der Dienstidee bis zur Freigabe. Das macht aus dem Datenschutz kein gelöstes Problem, aber ein beherrschtes. Und beherrscht ist an einer Hochschule ungefähr das Beste, was man über irgendetwas sagen kann.

WEITERLESEN · Weiterlesen

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

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [Microsoft 365 an Hochschulen: Wo der Campus anders tickt als Verwaltung und Wirtschaft](#)
- › [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#)
- › [Microsoft 365 in der öffentlichen Verwaltung](#)
- › [Microsoft-365-Beratung für Hochschulen und Forschung](#)