

Digitale Souveränität an Hochschulen: Was realistisch ist und was Sonntagsrede bleibt

Microsoft 365 · Hochschule · Souveränität

Digitale Souveränität: Was realistisch ist und was Sonntagsrede bleibt

Souveränität ist kein Produkt, das man kauft. Sie ist eine Fähigkeit, die man übt, am besten bevor man sie braucht.

boddenberg.de

„Wir werden digital souverän.“
(Applaus. Kaffee. Weiter wie bisher.)

SONNTAGS-REDE

WISSEN	BERATUNG	SCHULUNG
Alle Beiträge der Serie zu Microsoft 365 in Hochschule und Forschung an einem Ort. › Microsoft 365 in Hochschule und Forschung	Souveränitätsziele sortieren, Exit-Fähigkeit aufbauen und eine Vorlage für Präsidium und Senat, die ohne Heilsversprechen auskommt. › Beratung für Hochschulen und Forschung	Für Rechenzentrum und Verwaltung: Datenstandort, Exportwege und Schlüsselverwaltung in Microsoft 365 verstehen und erklären. › Schulungen für Hochschulen und Forschung

Digitale Souveränität ist an Hochschulen das, was früher die „papierlose Verwaltung“ war: Jeder ist dafür, keiner weiß genau, was damit gemeint ist, und spätestens beim dritten Glas Sekt auf dem Neujahrsempfang hat das Präsidium sie bereits erreicht. Am Montag danach sitzt das Hochschulrechenzentrum dann vor derselben Frage wie vorher: Was genau sollen wir jetzt anders machen? Und mit welchem Personal?

Die Debatte leidet an zwei Heilsversprechen, die sich gegenseitig verdienen. Das eine lautet: Mit dem richtigen Rechenzentrumsstandort, der richtigen Datengrenze und dem richtigen Zusatzprodukt ist die Cloud eines US-Anbieters souverän genug, Thema erledigt. Das andere lautet: Wir lösen Microsoft per Senatsbeschluss ab, betreiben alles selbst und sind dann frei. Beide Versprechen haben einen wahren Kern. Beide scheitern an der Realität eines Campus mit Zehntausenden Konten, Verbundprojekten mit Industriepartnern, einer Verwaltung, die mit Ministerien kommuniziert, und einem Rechenzentrum, dessen ausgeschriebene Stellen schneller altern als die Server.

Dieser Beitrag trennt deshalb sauber, was hinter dem Schlagwort steckt, ordnet die aktuellen Angebote ein, ohne sie zu verkaufen, und landet bei dem Teil, den Sie heute schon gestalten können: Exit-Fähigkeit und Datenportabilität. Er ist Teil der Serie [Microsoft 365 in Hochschule und Forschung](#). Universitätsklinika und allgemeinbildende Schulen haben eigene Rahmenbedingungen und bleiben hier außen vor.

WICHTIG · Der Kernsatz dieses Beitrags

Souveränität ist kein Zustand, den man einkauft, sondern eine Fähigkeit, die man nachweisen kann:

die Fähigkeit, zu entscheiden, zu kontrollieren und notfalls zu wechseln. Der Anbieter kann die ersten beiden Teile unterstützen. Den dritten müssen Sie selbst bauen.

Begriffsklärung: Drei Souveränitäten und ein Schlagwort

Wer in einer Gremiensitzung „digitale Souveränität“ sagt, meint je nach Fakultät etwas völlig anderes. Die Informatik denkt an Quellcode und Eigenbetrieb, die Rechtswissenschaft an Drittstaatenzugriffe, die Verwaltung an Vertragslaufzeiten und das Präsidium an eine Schlagzeile, die nicht peinlich ist. Bevor Sie Maßnahmen beschließen, lohnt es sich, das Wort in drei handhabbare Teile zu zerlegen.

Skizze 1: Drei Ebenen, die in der Debatte gern verrührt werden

Je weiter unten, desto weniger hängt am Anbieter und desto mehr an Ihnen selbst.

Datensoeveränität

Frage: Wo liegen die Daten, wer kann technisch und rechtlich darauf zugreifen, wer hält die Schlüssel?

Anbieter liefert viel (Rechenzentrumsstandort, EU Data Boundary, Verschlüsselung). Restrisiko: Rechtsordnung des Anbieters.

Betriebssouveränität

Frage: Wer betreibt, wer hat Administratorzugriff, wer entscheidet über Updates, Funktionen und Abschaltungen?

In der Public Cloud weitgehend beim Anbieter. Partner- und Private-Cloud-Modelle verschieben einen Teil zurück, gegen Aufwand.

Wechselfähigkeit

Frage: Können Sie Daten, Identitäten und Prozesse in vertretbarer Zeit woanders hin bewegen, wenn Sie müssen oder wollen?

Liegt fast vollständig bei Ihnen: Formate, Exportwege, Identität, Verträge, Übung. Hier beginnt die Arbeit heute.

Schematisch. Die meisten Sonntagsreden handeln von Ebene 1, die meisten Krisen von Ebene 3.

Datensoeveränität

Datensoeveränität fragt, wo Daten gespeichert und verarbeitet werden, wer technisch und rechtlich darauf zugreifen kann und wer die Schlüssel hält. Hier hat sich in den letzten Jahren am meisten bewegt, weil die Anbieter hier am meisten liefern können: Rechenzentren in Deutschland und der EU, Datengrenzen, kundenseitig verwaltete Schlüssel. Die unbequeme Restfrage bleibt die Rechtsordnung, der ein Anbieter mit Sitz außerhalb der EU unterliegt. Daran ändert kein Rechenzentrumsstandort etwas, er verschiebt nur, wie wahrscheinlich und wie aufwendig ein Zugriff wäre.

Betriebssouveränität

Betriebssouveränität fragt, wer den Dienst betreibt, wer administrativen Zugriff auf die Infrastruktur hat und wer entscheidet, wann sich Funktionen ändern. In einer Public Cloud lautet die ehrliche Antwort: überwiegend der Anbieter. Sie entscheiden über Konfiguration, nicht über den Releasezyklus. Wer das für Lehre und Forschung nicht akzeptabel findet, muss Betrieb zurückholen, sei es im eigenen Hochschulrechenzentrum, in einem Landes- oder Verbunddienst oder bei einem Partner. Das kostet Personal, und Personal ist an Hochschulen das knappste Gut nach Parkplätzen.

Wechselfähigkeit

Wechselfähigkeit ist der unterschätzte dritte Teil: Können Sie mit vertretbarem Aufwand und in vertretbarer Zeit Daten, Konten und Prozesse zu einem anderen Anbieter oder in den Eigenbetrieb bewegen? Hier hilft kein Produkt, hier helfen offene Formate, getestete Exportwege, ein eigenes Identitätsmanagement und Verträge, die den Auszug regeln. Die gute Nachricht: Das ist der Teil, auf den Sie den größten Einfluss haben. Die schlechte: Er ist so unspektakulär, dass er in keiner Pressemitteilung vorkommt.

Dimension	Kernfrage	Wer liefert	Typischer Irrtum
Datensouveränität	Wo liegen die Daten, wer kommt dran, wer hat die Schlüssel?	Überwiegend der Anbieter, ergänzt durch Ihre Konfiguration	„Rechenzentrum in Frankfurt“ beantwortet die Zugriffsfrage vollständig.
Betriebssouveränität	Wer betreibt, wer administriert, wer entscheidet über Änderungen?	Anbieter, Partner oder Eigenbetrieb, je nach Modell	Ein souveränes Etikett ändert, wer das Rechenzentrum betreibt, nicht automatisch, wer den Code schreibt.
Wechselfähigkeit	Kommen wir raus, wenn wir müssen?	Fast ausschließlich Sie selbst	„Wir können ja jederzeit kündigen.“ Kündigen ja, umziehen nicht.

FAKTEN · Was „souverän“ in Ausschreibungen und Strategiepapieren oft meint

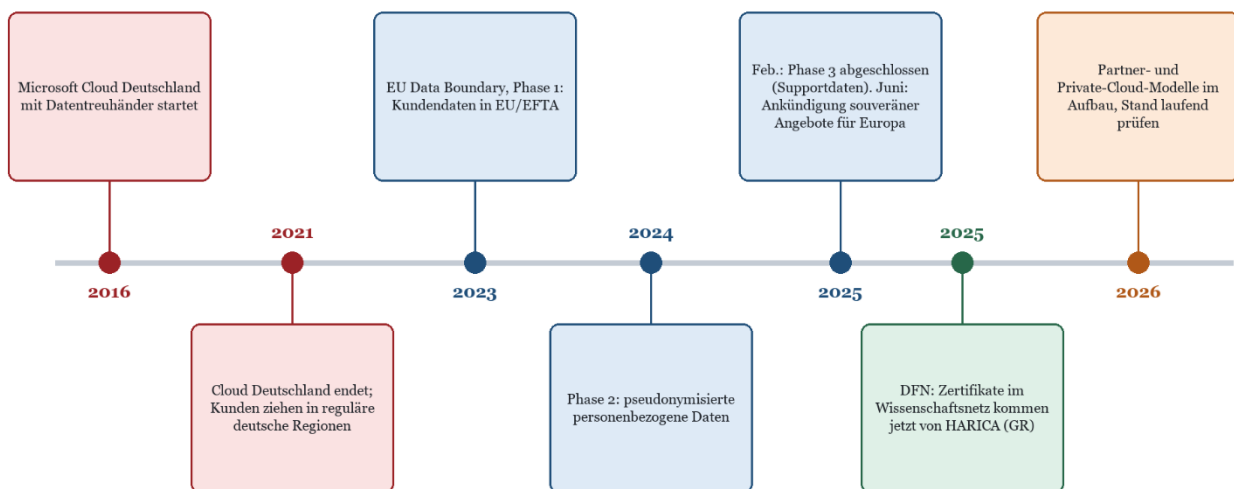
In Strategiepapieren von Bund und Ländern taucht Souveränität meist als Bündel auf: Wechselmöglichkeit, Gestaltungsfähigkeit und Einfluss auf Anbieter. Für eine Hochschule übersetzt heißt das: Sie wollen nicht von einem einzigen Anbieter erpressbar sein, Sie wollen eigene Anforderungen durchsetzen können, und Sie wollen Ihre Daten im Griff behalten. Kein einzelnes Produkt erfüllt alle drei Ziele.

Was die Anbieter heute liefern und was davon zu halten ist

Rechenzentrumsleiter haben ein gutes Gedächtnis, und das ist hier hilfreich. Die Liste der Souveränitätsversprechen ist lang, und nicht alle haben überlebt. Ein kurzer Blick zurück erklärt, warum Skepsis gegenüber neuen Etiketten berechtigt ist und warum man trotzdem nicht pauschal alles abtun sollte.

Skizze 2: Souveränitätsversprechen und was aus ihnen wurde

Auswahl, nicht vollständig. Die Linie zeigt: Modelle kommen und gehen, die Datenhaltung bleibt Ihre Aufgabe.



Daten verifiziert gegen Herstellerangaben und DFN-Dokumentation; Angebotsstand 2026 ändert sich laufend.

Der gescheiterte Vorläufer: Die Cloud mit Treuhänder

Microsoft hat ab 2016 eine eigene Cloud für Deutschland betrieben, bei der ein deutscher Datentreuhänder, eine Tochter der Deutschen Telekom, den Zugriff auf Kundendaten kontrollierte. Microsoft selbst kam nur unter Aufsicht des Treuhänders oder des Kunden an die Daten. Rechtlich war das Modell elegant, praktisch war es eine Insel: Funktionen kamen später oder gar nicht, und die Isolation vom globalen Netz machte den Betrieb teuer. Im September 2020 kündigte Microsoft das Ende an, Ende Oktober 2021 wurde die Cloud Deutschland geschlossen, die Kunden zogen in die regulären deutschen Rechenzentrumsregionen um.

Die Lehre daraus ist nicht, dass Souveränitätsmodelle grundsätzlich scheitern. Die Lehre ist, dass ein Sondermodell nur so lange lebt, wie es sich für den Anbieter rechnet. Wer seine Architektur vollständig auf ein solches Modell ausrichtet, sollte einen Plan B haben, und zwar einen, der nicht im Ordner „Später“ liegt.

EU Data Boundary: Viel Substanz, klare Grenzen

Die EU Data Boundary ist Microsofts Zusage, Kundendaten und personenbezogene Daten für die Kerndienste innerhalb von EU und EFTA zu speichern und zu verarbeiten. Sie wurde in drei Phasen umgesetzt: Ab Januar 2023 für Kundendaten der Kerndienste einschließlich Microsoft 365, ab Januar 2024 für pseudonymisierte personenbezogene Daten wie Systemprotokolle, und im Februar 2025 erklärte Microsoft die Datengrenze mit der dritten Phase für abgeschlossen. Diese umfasst Daten aus dem technischen Support, also Fallnotizen und vom Kunden bereitgestellte Protokolle.

Das ist ein echter Fortschritt, und Rechenzentrumsleute, die den Datenfluss in Supportfällen früher mühsam nachvollziehen mussten, wissen das zu schätzen. Es ist aber eine Zusage zum Ort der Verarbeitung, keine Zusage zur Rechtsordnung. Die Frage, ob ein US-Unternehmen von US-Behörden zur Herausgabe von Daten verpflichtet werden kann, die es in Europa speichert, beantwortet die Datengrenze nicht. Außerdem nennt Microsoft selbst Ausnahmen, etwa für bestimmte Sicherheitsfunktionen und für Dienste, die global arbeiten müssen. Lesen Sie die Dokumentation zur EU Data Boundary also nicht nur bis zur Überschrift.

FAKTEN · EU Data Boundary auf einen Blick

Geltungsbereich: Kerndienste der Microsoft Cloud, darunter Microsoft 365, Dynamics 365, Power

Plattform und die meisten Azure-Dienste.

Phase 1 (ab Januar 2023): Kundendaten. Phase 2 (ab Januar 2024): pseudonymisierte personenbezogene Daten. Phase 3 (abgeschlossen Februar 2025): Daten aus dem technischen Support.

Nicht enthalten: eine Aussage zur Rechtsordnung des Anbieters. Dokumentierte Ausnahmen gibt es; welche für Ihren Tenant relevant sind, prüfen Sie in der aktuellen Herstellerdokumentation.

Souveräne Angebote für Europa und den öffentlichen Sektor

Im Juni 2025 hat Microsoft ein Paket souveräner Angebote für Europa angekündigt. Dazu gehören eine Kontrollschicht, bei der Fernzugriffe von Microsoft-Technikern auf europäische Systeme durch in Europa ansässiges Personal genehmigt, überwacht und manipulationssicher protokolliert werden sollen, außerdem Optionen für extern verwaltete Schlüssel und eine private Variante, bei der zentrale Kommunikations- und Kollaborationsdienste auf eigener Infrastruktur laufen. Daneben gibt es Partnermodelle, bei denen ein Unternehmen mit Sitz in Deutschland die Plattform betreibt, im deutschen Markt insbesondere eine auf die öffentliche Verwaltung zugeschnittene Partnercloud im SAP-Umfeld.

Für Hochschulen ist die Einordnung nüchtern: Diese Angebote zielen zuerst auf Bundes- und Landesverwaltung und auf regulierte Branchen. Welche davon für eine Hochschule erreichbar sind, zu welchen Bedingungen und mit welchem Funktionsumfang, ändert sich derzeit schneller als jede Lizenzübersicht. Wir nennen deshalb bewusst keine Termine und keinen Leistungsumfang. Fragen Sie konkret nach, lassen Sie sich die Antwort schriftlich geben und vergleichen Sie den Funktionsumfang mit dem, was Ihre Fakultäten heute tatsächlich nutzen. Ein souveränes Angebot, in dem die Hälfte der Funktionen fehlt, wird an einer Hochschule binnen eines Semesters von Schatten-IT umzingelt.

Ansatz	Adressiert vor allem	Adressiert nicht	Einschätzung für Hochschulen
EU Data Boundary	Ort der Speicherung und Verarbeitung, Supportdaten	Rechtsordnung des Anbieters, Betrieb, Wechselfähigkeit	Gut dokumentieren und im Verarbeitungsverzeichnis nutzen; ist bereits da, kein Zusatzprojekt.
Kontrolle von Fernzugriffen durch europäisches Personal	Wer im Betrieb auf Systeme zugreift	Funktionsumfang, Wechselfähigkeit	Sinnvolle Ergänzung; Wirkung hängt von Ausgestaltung und Nachweisbarkeit ab.
Eigene Schlüssel (kundenseitig verwaltet)	Zugriff auf ruhende Daten	Daten in Verarbeitung, Metadaten, Komfortfunktionen	Für ausgewählte Kernbereiche prüfen; Schlüsselverlust ist eine eigene Katastrophe.
Partnercloud mit deutschem Betreiber	Betrieb und Rechtsraum des Betreibers	Abhängigkeit vom Softwarehersteller, Funktionsverzögerung	Verfügbarkeit für Hochschulen und Funktionsumfang konkret erfragen; Vorläufer beachten.
Private Variante auf eigener Infrastruktur	Betrieb, Netztrennung	Personalbedarf, Modernisierungstempo	Eher für Spezialbereiche als für den ganzen Campus.
Eigenbetrieb mit Open Source	Betrieb, Quellcode, Rechtsraum	Personal, Integrationsaufwand, Zusammenarbeit mit externen Partnern	Für viele Dienste etabliert; Koexistenz statt Ablösung ist der Normalfall.

HINWEIS · Keine Rechtsberatung

Ob und wie Drittstaatenzugriffe für Ihre Hochschule datenschutzrechtlich zu bewerten sind, hängt vom Landesdatenschutzgesetz, von der Position Ihrer Landesaufsicht und von der konkreten Verarbeitung ab. Die Landesdatenschutzgesetze und die Haltungen der Aufsichtsbehörden unterscheiden sich spürbar, und für privatrechtlich organisierte Forschungseinrichtungen gelten teils andere Regeln als für Körperschaften des öffentlichen Rechts. Beziehen Sie Ihre Datenschutzbeauftragten und das Justizariat ein, bevor Sie Zusagen in Strategiepapiere schreiben.

Wie die Bewertungen der Datenschutzkonferenz und der Landesaufsichten in die Praxis eines Hochschul-Tenants übersetzt werden, beschreibt ausführlich der Beitrag [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#).

Open Source als Souveränitätsantwort: richtig, aber nicht gratis

Die naheliegende Gegenposition lautet: Wer souverän sein will, betreibt Open Source selbst. Das stimmt für Betriebs- und Datensouveränität in hohem Maß, und viele Hochschulen tun es seit Jahrzehnten erfolgreich, vom Lernmanagementsystem über Videokonferenzen bis zum förderierten Chat. Es stimmt aber nur, wenn Personal, Betriebsprozesse und Sicherheitsupdates mitkommen. Ein selbst betriebener Dienst mit drei Monaten Patchrückstand ist nicht souverän, sondern ein Angebot an die Konkurrenz aus dem Darknet.

Auch Open Source erzeugt Abhängigkeiten: von einem Landesdienst, von einem Dienstleister, der ihn betreibt, oder von der einen Kollegin, die als Einzige weiß, wie das Ansible-Playbook funktioniert. Souveränität heißt hier: diese Abhängigkeiten kennen und bewusst eingehen. Wie Koexistenz praktisch aussieht, zeigt der Beitrag [Microsoft 365 oder Open Source? Koexistenz mit BigBlueButton, Nextcloud, Moodle und Matrix](#).

Ein Beispiel aus der Praxis: Der Zertifikatswechsel im Wissenschaftsnetz

Dass die Wissenschafts-Community Souveränität nicht nur diskutiert, sondern praktisch angeht, zeigt ein Fall, der vielen Rechenzentren noch in den Knochen steckt. Browserverankerte Server- und Nutzerzertifikate bezieht der DFN-Verein über den Trusted Certificate Service (TCS) von GÉANT. GÉANT realisiert den Dienst mit externen Anbietern, die über Ausschreibungen gefunden werden. Seit 2021 war das ein Anbieter mit Sitz außerhalb der EU.

Dann kündigte dieser Anbieter seinen Vertrag mit GÉANT, und die Leistungserbringung endete zum 10. Januar 2025. Der DFN-Verein hat daraufhin zum Dezember 2024 HARICA beauftragt, einen griechischen Vertrauensdiensteanbieter, der aus dem akademischen Umfeld kommt. HARICA übernahm kurzfristig im Auftrag des DFN und längerfristig im Rahmen von GÉANT TCS. Die teilnehmenden Einrichtungen wurden ab Dezember 2024 schrittweise angebunden, sodass Zertifikate schon vor dem Ende des alten Dienstes beim neuen Anbieter beantragt werden konnten.

Was lernt man daraus für die Souveränitätsdebatte? Erstens: Die Abhängigkeit war real, und sie hat zugeschlagen, nicht durch einen Drittstaatenzugriff, sondern durch eine schnöde Vertragskündigung. Zweitens: Die Community war wechselfähig, weil es eine gemeinsame Beschaffungsstruktur, eine dokumentierte Schnittstelle und einen Verein gab, der handeln konnte. Drittens: Auch ein gelungener Wechsel hat in vielen Rechenzentren über die Feiertage Arbeit verursacht, von neuen Antragswegen bis zu Automatisierungen, die angepasst werden mussten. Wechselfähigkeit heißt nicht, dass ein Wechsel nichts kostet. Sie heißt, dass er überhaupt möglich ist.

FAKTEN · Zertifikatsdienst im Wissenschaftsnetz

TCS ist ein PKI-Angebot, das der DFN-Verein über GÉANT bezieht. Der vorherige Anbieter beendete seinen Vertrag mit GÉANT; der Dienst über ihn endete zum 10. Januar 2025.

Der DFN-Verein beauftragte zum Dezember 2024 HARICA, einen griechischen Vertrauensdiensteanbieter. Aktueller Dienstleister laut DFN-Dokumentation ist HARICA.

Wie Nutzerzertifikate aus diesem Dienst in Outlook und Exchange Online zum Einsatz kommen, behandelt ein eigener Beitrag dieser Serie.

TYPISCHE SITUATION · Typische Situation: Der Dienst, an den niemand dachte

Aus Projekten bei öffentlichen Auftraggebern kennen wir dieses Muster: In einer Stadtverwaltung stand bei der Souveränitätsanalyse die große Kollaborationsplattform im Mittelpunkt, mit Workshops, Gutachten und Vorlagen für den Rat. Als ein kleiner, zugekaufter Dienst für Signaturen und Zertifikate kurzfristig wegfiel, gab es dafür weder eine Übersicht der Abhängigkeiten noch einen Ersatzweg. Die Arbeit erledigten am Ende zwei Administratoren an einem Wochenende.

An einer Hochschule sieht das typischerweise genauso aus: Die Diskussion kreist um Microsoft 365, während Zertifikate, Lizenzserver für Fachsoftware, SMS-Dienste für die Mehrfaktor-Anmeldung oder das Campus-Management-System mindestens genauso kritisch sind. Ein Souveränitätsinventar, das nur die sichtbaren Dienste erfasst, ist ein Inventar der Sonntagsrede.

Exit-Strategie und Datenportabilität: Was Sie heute schon gestalten können

Kommen wir zum Teil, der keine Pressemitteilung braucht. Exit-Fähigkeit bedeutet nicht, dass Sie Microsoft 365 verlassen wollen. Sie bedeutet, dass Sie es könnten, und dass Sie wissen, was es kosten würde. Diese Fähigkeit verändert die Verhandlungsposition beim nächsten Rahmenvertrag, die Gesprächslage mit der Landesaufsicht und, nicht zu unterschätzen, die Nachtruhe der Rechenzentrumsleitung.

Skizze 4: Exit-Fähigkeit in sechs Schritten

Kein Auszug, sondern die Fähigkeit dazu. Wer sie hat, verhandelt anders.



Schritte 1 bis 4 sind Rechenzentrumsarbeit, Schritt 5 gehört der Verwaltung, Schritt 6 allen gemeinsam.

Inventar und Formate

Am Anfang steht ein ehrliches Inventar: Welche Daten liegen wo, in welchem Umfang, in welchem Format, und welche Prozesse hängen daran? Für Microsoft 365 heißt das Postfächer, OneDrive-

Konten, SharePoint-Websites, Teams mit Kanälen und Chats, Formulare, Power-Automate-Flows und die vielen kleinen Power-Apps, die ein Dezernat irgendwann gebaut hat. Dateien in Office-Formaten sind gut portabel, weil die Formate offen dokumentiert sind. Schwieriger sind Strukturen und Metadaten: Berechtigungen, Versionsstände, Chatverläufe, Verknüpfungen zwischen Diensten. Ein Teams-Kanal lässt sich exportieren, ein Teams-Kanal mit seinem Kontext deutlich schwerer.

Eine Ablagestruktur, die sich an Organisationseinheiten und Aufbewahrungsfristen orientiert statt an der Vorliebe des jeweiligen Lehrstuhls, ist übrigens nicht nur Souveränitätsarbeit, sondern auch Voraussetzung für Löschkonzepte, Exmatrikulation und Lehrstuhlwechsel. Selten zählt sich Ordnung so mehrfach aus.

Exportwege testen, nicht nur dokumentieren

Microsoft 365 bietet mehrere Wege, Daten herauszubekommen: die eDiscovery-Werkzeuge für Postfächer und Dateien, Programmierschnittstellen über Microsoft Graph, Synchronisation und Migrationswerkzeuge. Jeder Weg hat Grenzen bei Volumen, Metadaten und Geschwindigkeit. Diese Grenzen kennen Sie erst, wenn Sie es versucht haben. Wählen Sie deshalb einmal im Jahr einen abgegrenzten Bereich, zum Beispiel ein abgeschlossenes Verbundprojekt oder das Archiv einer Gremiengeschäftsstelle, und exportieren Sie ihn probeweise in ein Zielsystem. Protokollieren Sie Dauer, Aufwand und was verloren ging.

TIPP · Der Probeexport als Jahresritual

Ein Probeexport ist die günstigste Souveränitätsmaßnahme, die es gibt. Er kostet ein paar Tage Arbeit, liefert harte Zahlen für die nächste Strategiediskussion und deckt Lücken auf, bevor sie unter Zeitdruck auffallen. Legen Sie ihn in die vorlesungsfreie Zeit, niemals in die Woche vor Semesterbeginn.

Identität: Der eigentliche Anker

Die wichtigste Exit-Maßnahme hat mit Microsoft 365 nur indirekt zu tun: Führen Sie Identitäten im eigenen Identitätsmanagement, gespeist aus Campus-Management und Personalverwaltung, und provisionieren Sie von dort in Entra ID. Dann ist der Cloud-Tenant ein angeschlossenes System unter mehreren, so wie das LMS, die Bibliothek oder die DFN-AAI-Föderation. Wer dagegen Entra ID zur einzigen Quelle der Wahrheit gemacht hat, muss bei einem Wechsel zuerst die Wahrheit wiederfinden. Viele Hochschulen haben diese Architektur ohnehin, weil sie aus der Zeit vor der Cloud stammt. Das ist einer der seltenen Fälle, in denen historisch gewachsene IT ein Vorteil ist.

Verträge und Beschaffung

Der vertragliche Teil liegt bei Kanzler, Dezernat und Beschaffung, gehört aber in dieselbe Planung. Prüfen Sie, welche Fristen nach Vertragsende für den Datenexport gelten, wie Löschung nachgewiesen wird und was mit Daten in Sicherungen passiert. Viele Hochschulen beziehen Lizenzen über Rahmenverträge, auf deren Gestaltung sie einzeln wenig Einfluss haben. Umso wichtiger ist es, die eigenen Anforderungen über Gremien und Verbände einzubringen. Wie Hochschul-IT-Verantwortliche sich organisieren und gemeinsam auftreten, zeigt der Zertifikatsfall oben: Gemeinsam ist man wechselfähiger als allein.

WARNUNG · Exit-Plan ohne Personal ist ein Gedicht

Ein Exit-Plan, der voraussetzt, dass ein Rechenzentrum mit dauerhaft unbesetzten Stellen im Ernstfall nebenbei einen neuen Dienst für Zehntausende Konten aufbaut, ist Literatur. Schreiben Sie in den Plan, welche Kapazität er braucht, woher sie kommen soll und wer darüber entscheidet. Wenn

die Antwort „niemand“ lautet, ist das eine wichtige Information für das Präsidium.

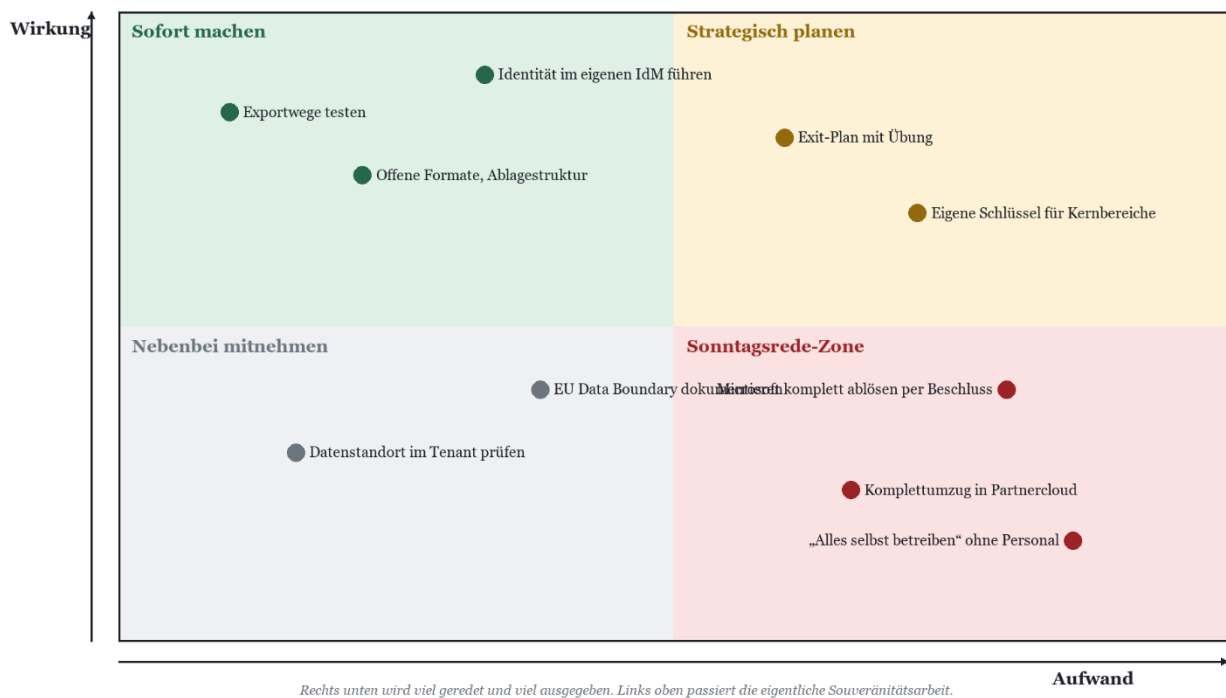
Souveränitätsziele, Maßnahmen und ihr echter Nutzen

Die folgende Tabelle ordnet typische Ziele aus Strategiepapieren konkreten Maßnahmen zu. Die Spalte „Was es wirklich bringt“ ist bewusst unfreundlich formuliert. Sie ist die Spalte, die in Vorlagen für den Senat meistens fehlt.

Souveränitätsziel	Maßnahme	Aufwand	Was es wirklich bringt
Daten in der EU	EU Data Boundary dokumentieren, Datenstandort im Tenant prüfen	Gering	Belegbare Aussage zum Verarbeitungsort; keine Aussage zur Rechtsordnung.
Kontrolle über Zugriffe	Zugriffsprotokolle, Genehmigung von Supportzugriffen, Rollenmodell für Administratoren	Mittel	Nachvollziehbarkeit; ersetzt keine Vertragsprüfung.
Schutz besonders sensibler Daten	Eigene Schlüssel oder doppelte Verschlüsselung für ausgewählte Bereiche	Mittel bis hoch	Starker Schutz für ruhende Daten; Komfortfunktionen und Suche leiden, Schlüsselverwaltung wird kritisch.
Unabhängigkeit vom Anbieter	Eigenes Identitätsmanagement als führende Quelle	Mittel, oft schon vorhanden	Größter Einzelhebel für jeden späteren Wechsel.
Wechselfähigkeit	Offene Formate, Ablagestruktur, jährlicher Probeexport	Gering bis mittel	Harte Zahlen statt Vermutungen; bessere Verhandlungsposition.
Vertragliche Absicherung	Exportfristen, Löschnachweis, Kündigungsfolgen klären	Mittel	Rechtssicherheit für den Auszug; wirkt nur mit technischer Vorbereitung.
Betrieb in eigener Hand	Dienste selbst oder im Landes- und Verbundbetrieb betreiben	Hoch	Echte Betriebssouveränität, wenn Personal und Patchprozesse mitwachsen.
Komplettwechsel in eine Partnercloud	Migration aller Dienste	Sehr hoch	Anderer Betreiber, gleicher Softwarehersteller; Funktionsumfang und Verfügbarkeit vorab konkret prüfen.
Microsoft vollständig ablösen	Senatsbeschluss plus Migrationsprojekt	Sehr hoch	Kann sinnvoll sein; ohne Personal, Exitplan und Fakultätsrückhalt entsteht vor allem Schatten-IT.

Skizze 3: Aufwand gegen Wirkung, ehrlich eingeschätzt

Qualitative Einordnung aus Projekterfahrung, keine Messung. Ihre Lage kann andere Positionen ergeben.



Wer was beitragen muss

Souveränität ist keine Rechenzentrumsaufgabe allein. Das Präsidium muss Ziele festlegen und Ressourcen bereitstellen, der Kanzler die vertragliche Seite und die Personalplanung verantworten, Datenschutzbeauftragte die Bewertung beisteuern und der Personalrat einbezogen werden, wenn sich Werkzeuge und damit Arbeitsweisen ändern. Wie Dienstvereinbarungen aussehen, die Funktionen statt Produkte regeln und deshalb einen Wechsel überstehen, beschreibt [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#). Die Personalvertretungsgesetze der Länder unterscheiden sich dabei, und privatrechtlich organisierte Forschungseinrichtungen arbeiten mit dem Betriebsverfassungsgesetz.

- **Präsidium oder Rektorat:** Ziele priorisieren, Ressourcen zusagen, Ehrlichkeit über Zielkonflikte zulassen.
- **Kanzler und Dezernate:** Verträge, Beschaffung, Haushalt und Stellenplan.
- **Hochschulrechenzentrum:** Inventar, Identität, Exportwege, Probeexport, Betrieb.
- **Fakultäten und Institute:** Anforderungen aus Forschung und Lehre benennen, dezentrale Dienste offenlegen.
- **Datenschutzbeauftragte und Personalrat:** früh beteiligen, nicht erst bei der Abstimmung.

Für außeruniversitäre Forschungseinrichtungen kommt eine weitere Ebene hinzu: Oft legt eine Zentrale Rahmenbedingungen fest, die das einzelne Institut nur begrenzt beeinflussen kann. Wie man damit umgeht, beschreibt [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#). Wer Souveränitätsziele, Exitplan und eine Vorlage für Präsidium und Senat gemeinsam erarbeiten will, findet Unterstützung bei [Microsoft-365-Beratung für Hochschulen und Forschung](#). Damit Rechenzentrum und Verwaltung Datenstandort, Schlüsselverwaltung und Exportwege in Microsoft 365 selbst beherrschen, gibt es [Microsoft-365-Schulung für Hochschulen und Forschung](#).

FAQ: Digitale Souveränität an der Hochschule

Ist Microsoft 365 mit der EU Data Boundary souverän?

Es ist datenseitig deutlich besser aufgestellt als vor einigen Jahren, weil Kundendaten, pseudonymisierte personenbezogene Daten und Supportdaten der Kerndienste in EU und EFTA verarbeitet werden. Die Rechtsordnung des Anbieters, der Betrieb und Ihre Wechselfähigkeit sind damit aber nicht geklärt. Souverän im vollen Sinn macht es Sie nicht, es reduziert ein bestimmtes Risiko.

Sollten wir auf ein souveränes Partnerangebot umsteigen?

Das lässt sich nicht pauschal beantworten. Prüfen Sie, ob das Angebot für Hochschulen überhaupt verfügbar ist, welchen Funktionsumfang es hat und wie es um Laufzeiten und Kosten steht. Denken Sie an den Vorläufer mit Datentreuhänder, der nach wenigen Jahren eingestellt wurde, und planen Sie den Rückweg mit.

Ist Open Source automatisch souveräner?

Bei Betrieb und Quellcode in der Regel ja, sofern Sie den Dienst tatsächlich selbst oder in einem vertrauenswürdigen Verbund betreiben und pflegen können. Ohne Personal und Patchprozesse entsteht eine andere Abhängigkeit, nämlich die von Glück.

Was ist die wirksamste Maßnahme mit dem geringsten Aufwand?

Ein eigenes Identitätsmanagement als führende Quelle und ein jährlicher Probeexport eines abgegrenzten Datenbereichs. Beides ist unspektakulär und verschafft Ihnen Fakten statt Meinungen.

Was hat der Zertifikatswechsel im DFN mit Microsoft 365 zu tun?

Direkt wenig, im Prinzip viel. Er zeigt, dass Abhängigkeiten auch durch Vertragskündigungen wirksam werden und dass gemeinsame Strukturen einen geordneten Wechsel ermöglichen. Dieselbe Logik gilt für jeden Clouddienst.

Brauchen wir eigene Schlüssel für Microsoft 365?

Für ausgewählte, besonders schützenswerte Bereiche kann das sinnvoll sein. Für den gesamten Tenant überwiegen meist die Nachteile: Funktionen fallen weg, und ein verlorener Schlüssel ist ein Datenverlust mit Ansage. Entscheiden Sie bereichsweise.

Wer sollte bei uns über Souveränitätsziele entscheiden?

Die Hochschulleitung, vorbereitet durch Rechenzentrum, Verwaltung, Datenschutz und Personalrat und mit Rückkopplung zu Senat und Fakultäten. Ein Rechenzentrum kann Optionen aufzeigen, verbindliche Prioritäten und Ressourcen muss das Präsidium setzen.

Gilt das alles auch für Kunst- und Musikhochschulen?

Ja, nur kleiner. Gerade kleine Häuser mit wenigen IT-Stellen profitieren von Exportfähigkeit und eigenem Identitätsmanagement, weil sie einen Eigenbetrieb großer Dienste selten stemmen können und auf Verbund- oder Landesangebote angewiesen sind.

Fazit: Weniger Rede, mehr Probeexport

Digitale Souveränität an Hochschulen ist weder durch ein Zusatzprodukt zu kaufen noch durch einen Senatsbeschluss herbeizuführen. Die EU Data Boundary hat beim Datenort echte Fortschritte gebracht, souveräne Partner- und Private-Cloud-Modelle sind in Bewegung und verdienen eine nüchterne Prüfung, und Open Source bleibt für viele Dienste die bessere Wahl, solange Personal und Betrieb mitwachsen. Keiner dieser Wege nimmt Ihnen die eigentliche Arbeit ab.

Diese Arbeit heißt Wechselfähigkeit: ein ehrliches Inventar, offene Formate, ein eigenes Identitätsmanagement, getestete Exportwege, Verträge mit klaren Auszugsregeln und eine jährliche Übung. Der Zertifikatswechsel im Wissenschaftsnetz hat gezeigt, dass die Community das kann, wenn es darauf ankommt. Machen Sie es für Ihr Haus genauso, nur bitte nicht erst über die Feiertage. Die Sonntagsrede darf dann gern bleiben. Sie hat dann nur endlich einen Montag.

WEITERLESEN • Weiterlesen

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

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)
- › [Microsoft 365 oder Open Source? Koexistenz mit BigBlueButton, Nextcloud, Moodle und Matrix](#)
- › [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 Forschung](#)