

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

Microsoft 365 · Hochschule und Forschung · Exportkontrolle

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

Der Tenant kennt keine Außenwirtschaftsverordnung. Sie schon.

Dual-Use Technische Unterstützung Geheimhaltungsvereinbarung Vertraulichkeitsbezeichnungen DLP
Verwaltete Geräte Gäste gesperrt Keine Verschlusssachen

boddenberg.de

WISSEN

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

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

BERATUNG

Schutzklassen, Labels, DLP und Projektraum-Vorlagen konzipieren, gemeinsam mit Exportkontrolle, Drittmittelabteilung, Datenschutz und Personalrat.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Hochschulrechenzentrum, Fakultäts-IT und Projektleitungen: Purview, Conditional Access und der Alltag im geschützten Projektraum.

› [Schulungen für Hochschulen und Forschung](#)

Es gibt E-Mails, die man im Hochschulrechenzentrum nicht gern liest. Eine davon beginnt mit „Kurze Frage, ist wahrscheinlich nichts“ und endet mit dem Satz, dass ein Gastwissenschaftler die Konstruktionsunterlagen des Industriepartners seit drei Monaten aus dem Ausland abrufen konnte, weil jemand den Ordner „Projekt_alles“ mit einem Link für alle freigegeben hatte. Der Link war praktisch. Er war auch das Einzige an diesem Projekt, das wirklich funktioniert hat.

Exportkontrolle klingt nach Zoll, Gabelstapler und Containerhafen. Für Hochschulen und Forschungseinrichtungen ist sie etwas anderes: Sie betrifft Wissen, Software und Daten, die über E-Mail, Freigabelink, Videokonferenz oder den Laptop auf der Dienstreise den Weg ins Ausland finden. Dazu kommen Industriekooperationen mit Geheimhaltungsvereinbarung, bei denen der Partner sehr genau wissen möchte, wer auf seine Unterlagen zugreift. Microsoft 365 ist dabei weder Ursache noch Lösung, sondern der Ort, an dem beides passiert. Wer dort Schutzklassen, Vertraulichkeitsbezeichnungen und DLP-Regeln sauber aufsetzt, macht aus „ist wahrscheinlich nichts“ eine nachvollziehbare Entscheidung.

Dieser Beitrag gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#). Er richtet sich an Leitungen von Hochschulrechenzentren und IT-Servicezentren, CIOs, Kanzlerinnen und Kanzler, die Dezernate für Forschung und Drittmittel, Datenschutzbeauftragte und Personalräte sowie an IT- und Verwaltungsleitungen außeruniversitärer Forschungseinrichtungen. Universitätsklinika mit ihren eigenen Regeln für Gesundheitsdaten und kritische Infrastruktur bleiben hier bewusst außen vor.

FAKTEN · Das Wichtigste in Kürze

Exportkontrolle gilt auch für Hochschulen und Forschungseinrichtungen. Das BAFA stellt klar, dass die grundgesetzlich verbürgte Wissenschaftsfreiheit nicht von den außenwirtschaftsrechtlichen Vorschriften entbindet.

Erfasst ist nicht nur die Ausfuhr von Geräten, sondern auch der Transfer von Technologie: per E-Mail, auf Datenträgern, in der Cloud und als „technische Unterstützung“ in Form von Wissen im Kopf.

Nach Darstellung des BAFA kann bereits das Bereitstellen von Technologie für mögliche Zugriffe aus dem Ausland eine Ausfuhr sein. Ein Download ist nicht erforderlich.

Microsoft 365 bietet mit Vertraulichkeitsbezeichnungen, Verschlüsselung, DLP und Conditional Access wirksame Werkzeuge, um solche Zugriffe zu verhindern und zu dokumentieren. Die rechtliche Prüfung ersetzen sie nicht.

Eingestufte Verschlusssachen gehören nicht in einen gewöhnlichen Microsoft-365-Tenant. Das BSI hält die Verarbeitung von Verschlusssachen in Public-Cloud-Diensten nach dem SaaS-Modell derzeit für nicht möglich.

Warum Exportkontrolle auch Hochschulen trifft

Die Vorstellung, Exportkontrolle sei ein Thema für Rüstungsfirmen und Maschinenbauer mit Auslandsvertrieb, hält sich an Hochschulen hartnäckig. Sie ist bequem und falsch. Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) schreibt in seinen Informationen für die Wissenschaft unmissverständlich, dass sensibles Technologiewissen nicht nur in der Industrie, sondern auch in Instituten und Fachbereichen von Hochschulen vorhanden ist und diese Einrichtungen deshalb Adressaten der Kontrollvorschriften sind. Die Vorschriften gelten für juristische Personen wie die Hochschule ebenso wie für einzelne Wissenschaftler, unabhängig von Motivation und Zielrichtung der eigenen Arbeit. Entscheidend ist allein das objektive Missbrauchspotenzial.

Dual-Use: Güter mit zwei Gesichtern

Den rechtlichen Rahmen bilden auf europäischer Ebene die EU-Dual-Use-Verordnung (EU) 2021/821 und national das Außenwirtschaftsgesetz mit der Außenwirtschaftsverordnung. Dual-Use-Güter sind Waren, Software und Technologie, die überwiegend zivil genutzt werden, sich aber auch für militärische Zwecke oder für Massenvernichtungswaffen eignen. Das BAFA nennt in seiner Broschüre für Forschung und Wissenschaft eine ganze Reihe betroffener Disziplinen: Biologie und Biotechnologie, Chemie, Physik, Nukleartechnik, Energie- und Umwelttechnik, Informations- und Kommunikationstechnologie, Elektrotechnik, Luft- und Raumfahrt, Maschinenbau, Werkstoff- und Verfahrenstechnik. Mit anderen Worten: so ziemlich jede Fakultät, an der etwas gebaut, gemessen oder programmiert wird.

Das Beispiel, das das BAFA selbst anführt, ist in seiner Harmlosigkeit beunruhigend: Schaltfunkenstrecken aus der Medizintechnik lassen sich prinzipiell auch zum Zünden von Kernsprengköpfen verwenden. Wer an einem Lehrstuhl für Hochspannungstechnik arbeitet, denkt dabei an Nierensteine. Das Exportrecht denkt an etwas anderes. Beides ist legitim, nur eben nicht beides gleichzeitig ignorierbar.

Ausfuhr, Bereitstellen und technische Unterstützung

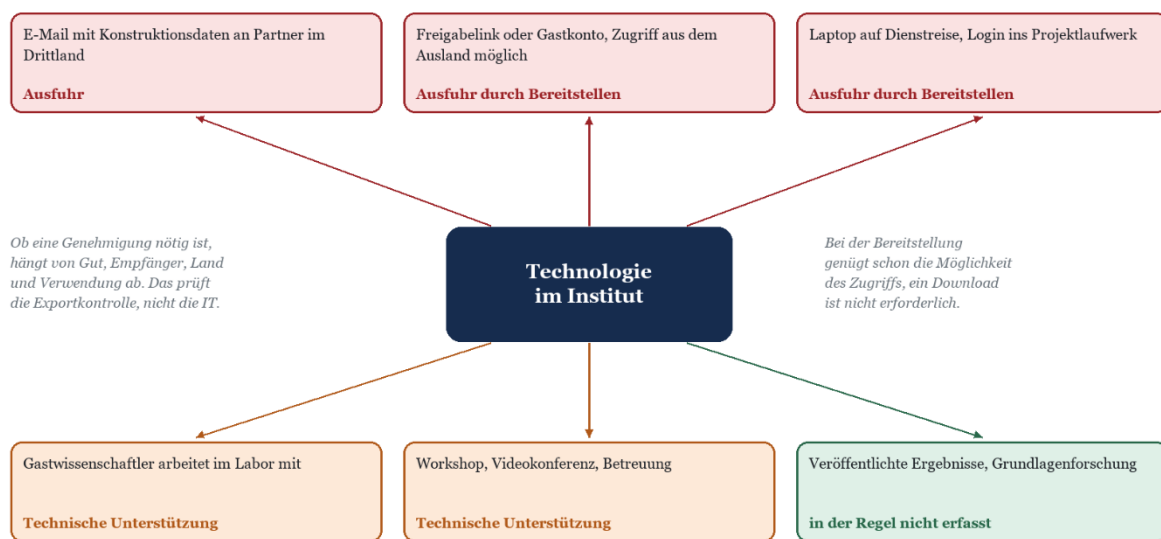
Für die IT ist die zentrale Unterscheidung die zwischen verkörperter und unverkörperter Technologie. Das BAFA-Merkblatt zum immateriellen Technologietransfer beschreibt es so: Liegt Technologie verkörpert vor, also als Datei, Zeichnung oder auf einem Datenträger, und wird sie in ein Drittland übertragen, ist das eine Ausfuhr. Unerheblich ist, wie sie übertragen wird, ob als USB-Stick im Handgepäck, als E-Mail-Anhang oder als Upload. Wird dagegen Wissen „im Kopf“ weitergegeben, durch Anleitung, Beratung, Ausbildung, in Seminaren, Workshops oder

Videokonferenzen, spricht das Recht von technischer Unterstützung. Das Merkblatt nennt ausdrücklich auch Projektkooperationen im akademischen Bereich.

Für den Microsoft-365-Betrieb ist ein dritter Begriff entscheidend: das Bereitstellen. Nach Darstellung des BAFA kann schon das Einräumen einer Zugriffsmöglichkeit von außerhalb der EU eine Ausfuhr sein. Ein tatsächlicher Download ist nicht erforderlich; es genügt, dass Technologie technisch erreichbar gemacht und damit „aus den Händen gegeben“ wird. Dabei kommt es nach dem Merkblatt nicht auf den Standort des Servers an, sondern auf den Standort dessen, der die Zugriffsrechte einräumt. Die Frage, in welchem Rechenzentrum Microsoft die Daten speichert, beantwortet die Exportkontrollfrage also nicht. Ein Freigabelink aus einem Tenant mit Datenstandort Deutschland an einen Empfänger im Drittland kann dieselbe Wirkung haben wie ein Paket mit Bauplänen.

Wie Wissen das Land verlässt

Typische Wege im Forschungsalltag, grob eingeordnet, ohne rechtliche Bewertung



Skizze 2: Die Technik entscheidet nicht, ob etwas genehmigungspflichtig ist. Sie entscheidet nur, ob es unbemerkt passiert

Grundlagenforschung und allgemein Zugängliches

Die gute Nachricht: Die Dual-Use-Verordnung kennt Ausnahmen, die für die Wissenschaft wichtig sind. Technologie, die bereits allgemein zugänglich ist, etwa weil sie veröffentlicht wurde, und Ergebnisse der Grundlagenforschung sind von der Kontrolle der Technologieweitergabe in weiten Teilen ausgenommen. Das BAFA weist aber darauf hin, dass diese Ausnahmen nicht alle Pflichten entfallen lassen und eng auszulegen sind. Anwendungsnahe Forschung, wie sie in Industriekooperationen typisch ist, fällt in der Regel nicht unter den Begriff der Grundlagenforschung. Und „wird ja sowieso irgendwann veröffentlicht“ ist kein Zustand, sondern eine Absicht.

Ebenso wichtig ist die Gegenrichtung: Nicht jede Auslandskooperation ist genehmigungspflichtig, und selbst wenn, ist sie nach Aussage des BAFA in der Regel genehmigungsfähig. Exportkontrolle ist also kein Kooperationsverbot, sondern ein Prüfauftrag. Die IT muss diese Prüfung nicht durchführen, aber sie muss dafür sorgen, dass das Ergebnis der Prüfung im Tenant auch tatsächlich gilt.

Gastwissenschaftler, Dienstreisen und Sanktionslisten

Drei Konstellationen tauchen in der Praxis immer wieder auf. Erstens Gastwissenschaftler: Das BAFA nennt die Zusammenarbeit mit Gästen am eigenen Institut ausdrücklich als möglichen

Anwendungsfall der technischen Unterstützung. Ein Gastkonto im Tenant mit Zugriff auf die Projekt-Site ist zusätzlich eine Form der Bereitstellung. Zweitens Dienstreisen: Das Merkblatt beschreibt den Fall eines Wissenschaftlers, der sich im Drittland mit seinem Laptop ins Netz seiner Einrichtung einloggt. Schon die Möglichkeit, auf genehmigungspflichtige Unterlagen zuzugreifen, kann eine Ausfuhr sein, ebenso das Mitführen der Daten auf dem Gerät. Drittens die personenbezogenen Sanktionen: Forschungseinrichtungen müssen sicherstellen, dass Kooperationspartner nicht auf einschlägigen Sanktionslisten stehen. Das ist keine IT-Aufgabe, aber ein Gastkonto sollte erst angelegt werden, wenn diese Prüfung erfolgt ist.

Wie Sie Gäste, Lehrbeauftragte und andere Sonderrollen in Entra ID sauber modellieren, mit Sponsor, Ablaufdatum und eigenem Lebenszyklus, beschreibt der Beitrag [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#). Für den Exportkontrollfall ist das die Voraussetzung: Wer nicht weiß, welche Gastkonten es gibt und wer sie verantwortet, kann auch nicht steuern, wer worauf zugreift.

HINWEIS · Keine Rechtsberatung

Dieser Beitrag beschreibt technische und organisatorische Maßnahmen. Ob ein Vorhaben genehmigungspflichtig ist, ob eine Ausnahme greift oder welche Genehmigungsform passt, entscheiden die Exportkontrollbeauftragten Ihrer Einrichtung, gegebenenfalls mit dem BAFA. Das BAFA stellt dafür ein Handbuch „Exportkontrolle und Academia“, ein Merkblatt zum immateriellen Technologietransfer und Hinweise zu internen Compliance-Programmen bereit. Länderlisten, Güterlisten und Genehmigungsarten ändern sich; maßgeblich ist der jeweils aktuelle Stand beim BAFA.

WARNUNG · Verantwortung ist nicht delegierbar

Das BAFA formuliert es deutlich: Jede Wissenschaftlerin, jeder Wissenschaftler und jede Forschungseinrichtung muss die eigene Verantwortung im Bereich der Exportkontrolle wahrnehmen. Ein Label an einer Datei verschiebt diese Verantwortung nicht ins Rechenzentrum. Es macht nur sichtbar, dass sie existiert.

Vertrauliche Industriekooperationen und das Schutzklassenmodell

Exportkontrolle ist der dramatischere Fall, die Geheimhaltungsvereinbarung der häufigere. Wer mit einem Unternehmen ein Drittmittelprojekt durchführt, unterschreibt in aller Regel eine Vertraulichkeitsklausel. Darin steht, welche Informationen vertraulich sind, wer sie sehen darf, wie sie zu schützen sind, ob Unterauftragnehmer oder Gäste einbezogen werden dürfen und was nach Projektende mit ihnen geschieht. Manche Verträge enthalten konkrete technische Anforderungen, etwa Verschlüsselung, Zugriffsprotokolle oder den Ausschluss privater Geräte; andere begnügen sich mit „angemessenen Maßnahmen nach dem Stand der Technik“, was im Streitfall genauso viel bedeutet, wie man vorher dokumentiert hat.

Für die Hochschule ist das ein Spagat. Die Freiheit von Forschung und Lehre lebt von offener Kommunikation, von Veröffentlichung und vom Austausch mit Kollegen weltweit. Der Industriepartner lebt von Vorsprung. Beides lässt sich vereinbaren, aber nicht im selben Teams-Kanal mit derselben Freigabeeinstellung. Es braucht Stufen.

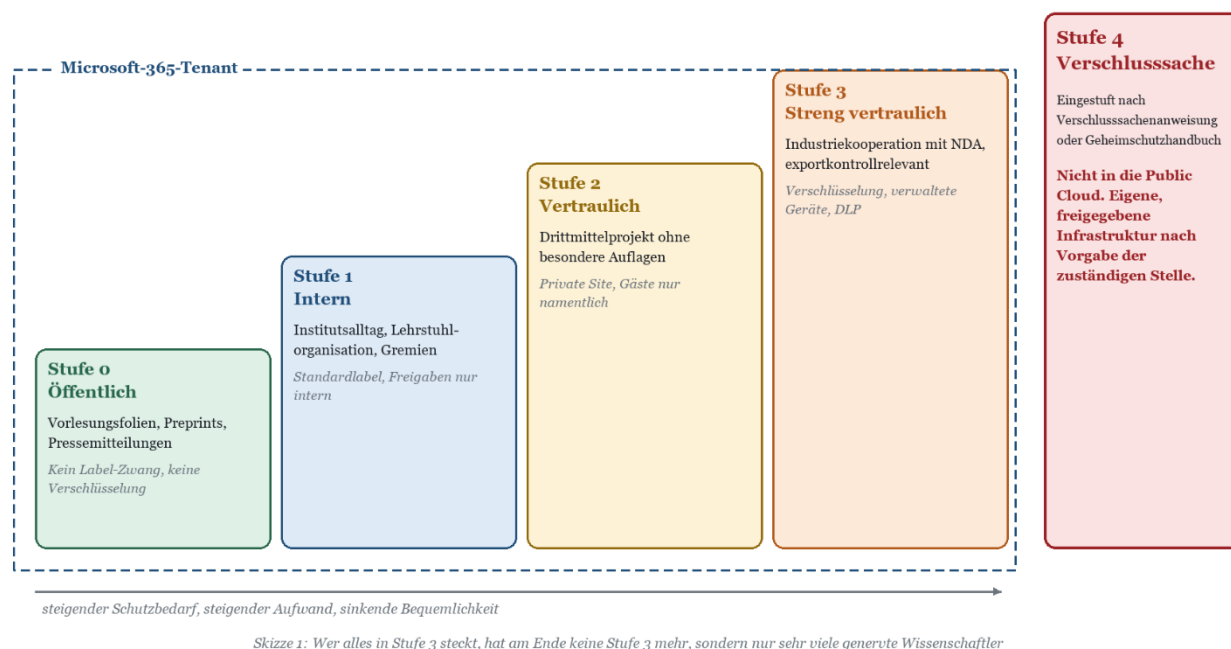
Ein Schutzklassenmodell für Forschungsprojekte

Bewährt hat sich ein Modell mit vier Stufen im Tenant und einer fünften, die ausdrücklich nicht im Tenant liegt. Die Namen sind Geschmackssache; wichtig ist, dass jede Stufe eine klare Bedeutung, ein eindeutiges Beispiel und eine festgelegte technische Wirkung hat. Mehr Stufen machen das

Modell nicht sicherer, sondern unbenutzbar. Wer zwölf Labels veröffentlicht, bekommt zwölf Varianten von „weiß nicht,nehm ich mal das mittlere“.

Schutzklassenmodell für Forschungsprojekte

Vier Stufen im Tenant, eine Stufe ausdrücklich draußen



Stufe 0 und 1 sind der normale Hochschulalltag. Stufe 2 ist das vertrauliche Drittmittelprojekt, bei dem der Personenkreis begrenzt ist, aber keine besonderen Auflagen bestehen. Stufe 3 ist die Industriekooperation mit Geheimhaltungsvereinbarung und alles, was die Exportkontrolle als relevant eingestuft hat. Stufe 4 sind Verschlusssachen; dazu weiter unten mehr. Die folgende Tabelle ordnet jeder Stufe Beispiele und Maßnahmen zu.

Schutzbedarf, Beispiele und Maßnahmen

Schutzbedarf	Beispiel	Technische Maßnahme	Organisatorische Maßnahme
Stufe 0 · Öffentlich	Vorlesungsfolien, Preprints, Pressemitteilungen, veröffentlichte Datensätze	Kein Label-Zwang; Freigabe auch extern möglich	Keine besondere; Hinweis auf Urheberrecht und Veröffentlichungsregeln
Stufe 1 · Intern	Institutsorganisation, Gremienunterlagen ohne Personenbezug, Lehrstuhlinterne	Standardlabel „Intern“; Freigaben auf die Organisation beschränkt	Hausregel zur Ablage; Schulung beim Onboarding
Stufe 2 · Vertraulich	Drittmittelprojekt ohne besondere Auflagen, Antragsentwürfe, Begutachtungen	Private Site mit Container-Label; Gäste nur namentlich und befristet; DLP warnt bei externer Weitergabe	Projektleitung benennt Mitglieder; Zugriffsüberprüfung pro Semester
Stufe 3 · Streng vertraulich	Industriekooperation mit NDA, exportkontrollrelevante Technologie, Konstruktionsdaten des Partners	Dateilabel mit Verschlüsselung für die Projektgruppe; Zugriff nur von verwalteten Geräten; keine Gäste ohne Freigabe; DLP blockiert externe Weitergabe, USB und Druck nach Bedarf	Exportkontrollprüfung vor Projektstart; Freigabe von Gästen durch Exportkontrolle; Zugriffsüberprüfung quartalsweise; Reiseregeln
Stufe 4 ·	Nach	Nicht in Microsoft 365;	Geheimschutzbeauftragter;

Verschlusssache	Verschlusssachenanweisung oder Geheimschutzhandbuch eingestuftes Material	freigegebene Infrastruktur nach Vorgabe der zuständigen Stelle	Sicherheitsüberprüfung der Projektmitglieder; eigene Prozesse
------------------------	---	--	---

TYPISCHE SITUATION · Das Label, das alle wollten

Aus einem Projekt bei einem kommunalen Verband: Dort wurde ein Label „Streng vertraulich“ mit Verschlüsselung eingeführt, gedacht für eine Handvoll Personalvorgänge. Nach drei Wochen trugen es Speisepläne, Urlaubslisten und die Einladung zum Sommerfest. Begründung: „Klang sicherer.“ Ergebnis: Externe Dienstleister konnten nichts mehr öffnen, der Helpdesk lief voll, und das Label hatte seine Signalwirkung verloren.

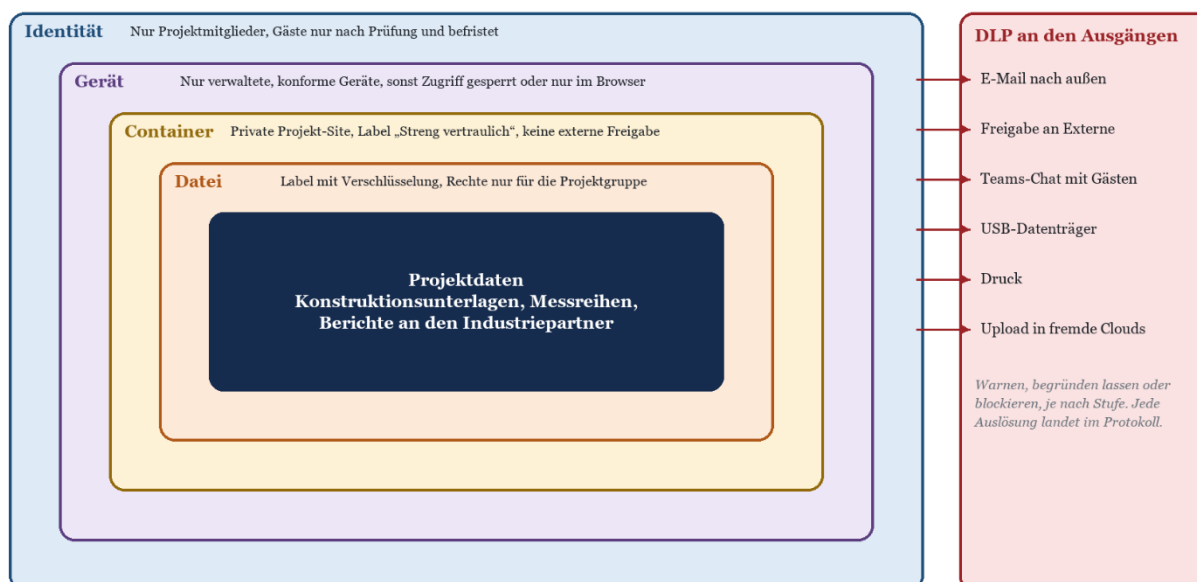
Übertragen auf die Hochschule ist die typische Situation dieselbe: Ein Lehrstuhl mit einem einzigen NDA-Projekt stuft vorsichtshalber alles auf Stufe 3. Die Lösung war damals wie heute dieselbe: Die höchste Stufe im Tenant wird nicht frei angeboten, sondern nur in Projekträumen, die nach Prüfung eingerichtet wurden, und als Standard für deren Bibliotheken gesetzt.

Technische Umsetzung in Microsoft 365

Die Werkzeuge liegen in Microsoft Purview und Microsoft Entra: Vertraulichkeitsbezeichnungen (Sensitivity Labels) für Dateien, E-Mails und Container, Verhinderung von Datenverlust (Data Loss Prevention, DLP) und Conditional Access. Keines davon ist neu, aber an Hochschulen sind sie oft nur halb eingeführt: Labels existieren, werden aber nicht genutzt; DLP läuft im Testmodus, seit jemand es vor drei Jahren eingeschaltet hat; Conditional Access kennt verwaltete Geräte nur vom Hörensagen. Das folgende Bild zeigt, wie die Bausteine für einen Projektraum der Stufe 3 zusammenspielen.

Der geschützte Projektraum in Schichten

Jede Schicht fängt ab, was die vorherige durchlässt



Skizze 3: Eine Schicht allein ist ein Vorschlag. Vier Schichten und DLP sind eine Hürde, keine Garantie

Vertraulichkeitsbezeichnungen mit Verschlüsselung

Ein Dateilabel mit Verschlüsselung ist das einzige Element der Kette, das mit der Datei reist. Wird ein Dokument mit dem Label „Streng vertraulich – Projekt“ heruntergeladen, per Mail weitergeleitet oder auf einen USB-Stick kopiert, bleibt es verschlüsselt. Öffnen kann es nur, wer in

der Rechtevergabe des Labels steht und sich mit einem passenden Konto anmeldet. Für Forschungsprojekte bewährt sich eine Rechtevergabe, die der Administrator fest im Label hinterlegt, gebunden an eine Projektgruppe, statt die Rechte den Nutzern beim Anwenden zu überlassen. Die Projektgruppe pflegt dann die Mitgliedschaft, nicht jedes einzelne Dokument.

Einige Einstellungen verdienen besondere Aufmerksamkeit. Der Offlinezugriff legt fest, wie lange ein Dokument ohne erneute Prüfung geöffnet werden kann; für Stufe 3 ist ein kurzer Zeitraum sinnvoll, damit ein entzogenes Recht auch tatsächlich greift. Ein Ablaufdatum für Inhalte passt zu Projekten mit festem Ende. Damit SharePoint und OneDrive verschlüsselte Office-Dateien verarbeiten können, also durchsuchen, gemeinsam bearbeiten und mit DLP prüfen, muss die Unterstützung von Vertraulichkeitsbezeichnungen für Office-Dateien in SharePoint und OneDrive aktiviert sein. Und schließlich braucht es eine geregelte Superuser-Funktion für den Rights-Management-Dienst, damit die Hochschule im Ernstfall, etwa bei einer Rechtsstreitigkeit oder nach dem Ausscheiden der Projektleitung, wieder an die eigenen Daten kommt. Wer diese Rolle hält, ist eine Frage für Präsidium und Personalrat, nicht für den diensthabenden Admin.

TIPP · Standardlabel für die Bibliothek

Eine Dokumentbibliothek in SharePoint lässt sich mit einem Standard-Vertraulichkeitslabel versehen. Neue oder hochgeladene Dateien ohne Label erhalten es automatisch. Für Projekträume der Stufe 3 ist das die wirksamste einzelne Maßnahme: Niemand muss daran denken, und niemand kann es vergessen.

Eingeschränkte Projekt-Sites

Container-Labels wirken auf Teams, Microsoft-365-Gruppen und SharePoint-Sites. Laut Microsoft-Dokumentation lassen sich damit unter anderem die Privatsphäre (öffentlich oder privat), der Zugang externer Nutzer, die externe Freigabe aus der Site, der Zugriff von nicht verwalteten Geräten, ein Authentifizierungskontext für Conditional Access, die Auffindbarkeit privater Teams und die Einladung anderer Teams in freigegebene Kanäle steuern. Für Stufe 3 heißt das: privat, keine Gäste, keine externe Freigabe, Zugriff nur über den Authentifizierungskontext „Verwaltetes Gerät erforderlich“, nicht auffindbar, freigegebene Kanäle nur intern.

Zwei Details aus der Dokumentation sind für die Planung wichtig. Erstens erben die Dateien in einem gelabelten Container dessen Label nicht. Das Container-Label schützt den Raum, nicht den Inhalt; für die Verschlüsselung braucht es zusätzlich Dateilabels oder ein Standardlabel für die Bibliothek. Zweitens wirkt das Ändern der Gastzugriffseinstellung eines Labels nur für neue Gäste. Wer bereits in einem Team ist, bleibt dort, bis jemand ihn entfernt. Wird ein Dokument mit höherer Einstufung in eine niedriger eingestufte Site hochgeladen, blockiert SharePoint das nicht, erzeugt aber ein Audit-Ereignis und eine Benachrichtigung an die Person und die Site-Besitzer. Diese Meldung ist ein guter Anlass für ein Gespräch, kein Grund zur Panik.

Daneben lohnt es sich, über die PowerShell-Einstellungen des Labels festzulegen, dass nur Site-Besitzer Inhalte und die Site selbst teilen dürfen. Zusammen mit einer Bereitstellung aus Vorlage, also einer Site, die das Hochschulrechenzentrum auf Antrag mit fertigem Label, Gruppe und Bibliothekseinstellungen anlegt, entsteht ein Projektraum, der sich nicht nachträglich versehentlich aufweichen lässt. Wie Sites, Speicher und Besitzerwechsel an der Hochschule grundsätzlich organisiert werden, behandelt der Beitrag [SharePoint und OneDrive an der Hochschule: Speicherpool, Lehrstuhlwechsel und Exmatrikulation](#).

Tabelle: Label-Konfiguration je Stufe

Einstellung	Stufe 1 · Intern	Stufe 2 · Vertraulich	Stufe 3 · Streng
-------------	------------------	-----------------------	------------------

			vertraulich
Verschlüsselung der Dateien	nein	optional	ja, Rechte für die Projektgruppe, kurzer Offlinezugriff
Kennzeichnung im Dokument	Fußzeile	Kopf- und Fußzeile	Kopf- und Fußzeile, Wasserzeichen
Privatsphäre des Containers	frei wählbar	privat	privat, nicht auffindbar
Gäste im Team	erlaubt	erlaubt, namentlich und befristet	gesperrt; Ausnahme nur nach Freigabe in eigenem Raum
Externe Freigabe der Site	nur Organisation	nur bestehende Gäste	nur Organisation
Nicht verwaltete Geräte	voller Zugriff	nur im Browser	gesperrt
Authentifizierungskontext	keiner	MFA	MFA und konformes Gerät
DLP-Verhalten	keines	Warnung mit Begründung	Blockieren, Ausnahme nur mit Begründung und Protokoll

DLP-Regeln

Labels beschreiben, was schützenswert ist. DLP sorgt dafür, dass es nicht unbemerkt hinausgeht. In Purview lassen sich Richtlinien für Exchange, SharePoint, OneDrive, Teams und, sofern die Geräte eingebunden sind, auch für Windows- und macOS-Endgeräte definieren. Für Forschungsprojekte sind zwei Arten von Bedingungen nützlich: das Vorhandensein eines bestimmten Labels und das Auftreten selbst definierter Muster, etwa projektinterner Kennzeichen oder Dokumentnummern des Industriepartners. Die eingebauten Typen für Kreditkartennummern und Ausweisdaten helfen hier wenig; ein Konstruktionsplan sieht für DLP zunächst einmal aus wie jede andere Datei.

Regel	Bedingung	Aktion	Hinweis
Externe Mail	E-Mail mit Anhang der Stufe 3 an Empfänger außerhalb der Organisation	Blockieren, Richtlinien Tipp, Meldung an Projektleitung	Ausnahmegruppe für freigegebene Partnerdomänen
Externe Freigabe	Datei der Stufe 2 oder 3 wird mit Externen geteilt	Stufe 2 warnen, Stufe 3 blockieren	Greift auch bei Freigaben aus OneDrive
Teams-Chat	Projektkennzeichen in Chat oder Kanal mit externen Teilnehmern	Nachricht blockieren, Hinweis an Absender	Erst im Testmodus beobachten
USB und Druck	Datei der Stufe 3 auf eingebundenem Endgerät	Kopieren auf Wechseldatenträger blockieren, Druck mit Begründung	Setzt eingebundene, verwaltete Geräte voraus
Fremde Clouds	Upload einer Datei der Stufe 3 in nicht freigegebene Cloud-Dienste im Browser	Blockieren	Liste erlaubter Dienste pflegen
Fehlendes Label	Datei in Projekt-Site der Stufe 3 ohne Label	Automatisch labeln oder Besitzer benachrichtigen	Ergänzt das Standardlabel der Bibliothek

WICHTIG · Erst beobachten, dann blockieren

Jede DLP-Richtlinie beginnt im Simulationsmodus. Nach zwei bis vier Wochen zeigt die Auswertung,

wie viele Treffer echte Risiken sind und wie viele das Weihnachtsrundschreiben der Fakultät. Wer sofort blockiert, produziert an einer Hochschule keinen Datenschutz, sondern einen Aufstand im Senat.

Zugriff nur von verwalteten Geräten

Hier wird es an Hochschulen unbequem. Ein großer Teil der Arbeit findet auf privaten oder lehrstuhleigenen Geräten statt, die das Hochschulrechenzentrum nie gesehen hat. Für Stufe 0 bis 2 ist das vertretbar, mit Browserzugriff ohne Download als Mittelweg. Für Stufe 3 nicht: Ein verschlüsseltes Dokument auf einem Gerät ohne Festplattenverschlüsselung, ohne Updates und mit fünf Familienmitgliedern als Mitnutzer ist nur auf dem Papier geschützt.

Technisch geht das über zwei Wege, die sich ergänzen. Die SharePoint-Einstellung für nicht verwaltete Geräte, über das Container-Label pro Site gesetzt, sperrt den Zugriff oder beschränkt ihn auf den Browser ohne Download; sie setzt eine Conditional-Access-Richtlinie mit app-erzwungenen Einschränkungen voraus. Der Authentifizierungskontext geht weiter: Er verlangt beim Zugriff auf die Site die Bedingungen einer eigenen Conditional-Access-Richtlinie, etwa ein als konform gemeldetes Gerät. Laut Dokumentation unterstützen nicht alle Apps Authentifizierungskontexte; Nutzer mit nicht unterstützten Apps werden abgewiesen. Das ist für Stufe 3 eher Feature als Fehler, sollte aber vor dem Start getestet werden, insbesondere mit Power-Automate-Flows und Drittanbieter-Werkzeugen. Wie Conditional Access an der Hochschule insgesamt aufgebaut wird, ohne den Helpdesk zu überrollen, beschreibt [MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps](#).

TIPP · Projektgeräte statt Gerätekrieg

Statt alle Geräte eines Lehrstuhls in die Verwaltung zu zwingen, stellen manche Einrichtungen für Stufe-3-Projekte gezielt verwaltete Projektgeräte bereit, physisch oder als virtuelle Arbeitsplätze. Das hält die Diskussion klein und die Freiheit der übrigen Arbeit groß.

Gastzugriff gezielt sperren

Gäste sind an Hochschulen der Normalfall und kein Sicherheitsvorfall. Für Stufe 3 aber gilt: Gäste nur, wenn die Exportkontrolle sie freigegeben hat, und dann namentlich, befristet und mit Sponsor. Technisch greifen mehrere Ebenen ineinander. Das Container-Label sperrt das Hinzufügen von Gästen zum Team. Die Einstellung für externe Freigabe verhindert Links an Externe. Die Rechtevergabe des Dateilabels schließt Konten außerhalb der Projektgruppe aus, auch wenn eine Datei auf anderem Weg nach draußen gelangt. Und regelmäßige Zugriffsüberprüfungen sorgen dafür, dass der Gast aus dem Vorjahr nicht zum Dauergast wird.

In Verbundprojekten mit anderen Hochschulen kommen die Einstellungen für den mandantenübergreifenden Zugriff hinzu, mit denen sich Zusammenarbeit pro Partnerorganisation erlauben oder sperren lässt. Details dazu stehen im Beitrag [Hochschulübergreifend zusammenarbeiten: B2B, mandantenübergreifender Zugriff und Verbundprojekte](#). Für den Industriepartner bewährt sich meist ein separater, ausdrücklich für den Austausch eingerichteter Raum mit geringerer Stufe, in den nur freigegebene Ergebnisse wandern, statt den Partner in den Kern des Projektraums zu holen.

Standort, Dienstreise und Länderregeln

Conditional Access kann Anmeldungen nach Land einschränken. Das klingt nach einer eleganten Antwort auf das Dienstreiseproblem und ist es nur zum Teil. Die Standortbestimmung beruht auf IP-Adressen und lässt sich mit einem VPN umgehen; sie verhindert Versehen, keine Absicht.

Außerdem ersetzt eine technische Länderregel keine exportrechtliche Bewertung, welche Länder in welchem Projekt kritisch sind; diese Liste gehört in die Hand der Exportkontrolle, nicht in die Konfiguration eines Admins, der sie aus einem Blogartikel abgeschrieben hat. Sinnvoll ist eine Reiseregeln: Vor Dienstreisen mit Projektbezug meldet die Projektleitung Reiseziel und Zeitraum, die Exportkontrolle entscheidet, und die IT setzt das Ergebnis um, notfalls durch vorübergehenden Ausschluss aus der Projektgruppe und ein sauberes Reisegerät.

FAKTEN · Lizenzfrage im Blick behalten

Nicht jede der beschriebenen Funktionen ist in jedem Education-Lizenzplan enthalten. Manuelle Labels, automatische Klassifizierung, Endpoint-DLP und erweiterte SharePoint-Funktionen sind unterschiedlich lizenziert, und die Zuordnung ändert sich. Prüfen Sie den aktuellen Stand in der Microsoft-Purview-Servicebeschreibung, bevor Sie ein Konzept versprechen, das der Vertrag nicht trägt. Grundlagen zu den Plänen erklärt der Beitrag [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#).

Die Grenze: Verschlusssachen gehören nicht in den Tenant

Es gibt eine Kategorie, bei der alle bisher beschriebenen Maßnahmen die falsche Antwort sind: staatlich eingestufte Verschlusssachen. Manche Hochschulinstitute und viele Einrichtungen der Ressortforschung arbeiten in Projekten, deren Unterlagen nach der Verschlusssachenanweisung oder, bei Aufträgen aus dem Bereich der geheimschutzbetreuten Wirtschaft, nach dem Geheimschutzhandbuch eingestuft sind. Für diese Unterlagen gelten eigene Regeln, eigene Zuständigkeiten und eigene Freigabeverfahren.

Das BSI hat 2026 einen Leitfaden für den Einsatz von Cloud-Lösungen im VS-Kontext der Bundesverwaltung veröffentlicht. Er ist auf den niedrigsten Geheimhaltungsgrad, VS – Nur für den Dienstgebrauch, ausgerichtet und enthält zwei Aussagen, die die Diskussion an jeder Hochschule abkürzen: Die Verarbeitung von Verschlusssachen im PaaS- oder SaaS-Servicemodell einer Public Cloud ist nach dem Leitfaden zum aktuellen Zeitpunkt noch nicht möglich. Und auch im IaaS-Modell kommt die Verarbeitung in einer Public Cloud derzeit nur bis VS-NfD in Betracht, und dann nur nach einer Freigabe durch die verantwortliche Stelle mit Risikobewertung im Einzelfall. Microsoft 365 ist ein SaaS-Dienst. Die Frage, ob ein Sensitivity Label „VS-NfD“ heißen darf, erübrigt sich damit.

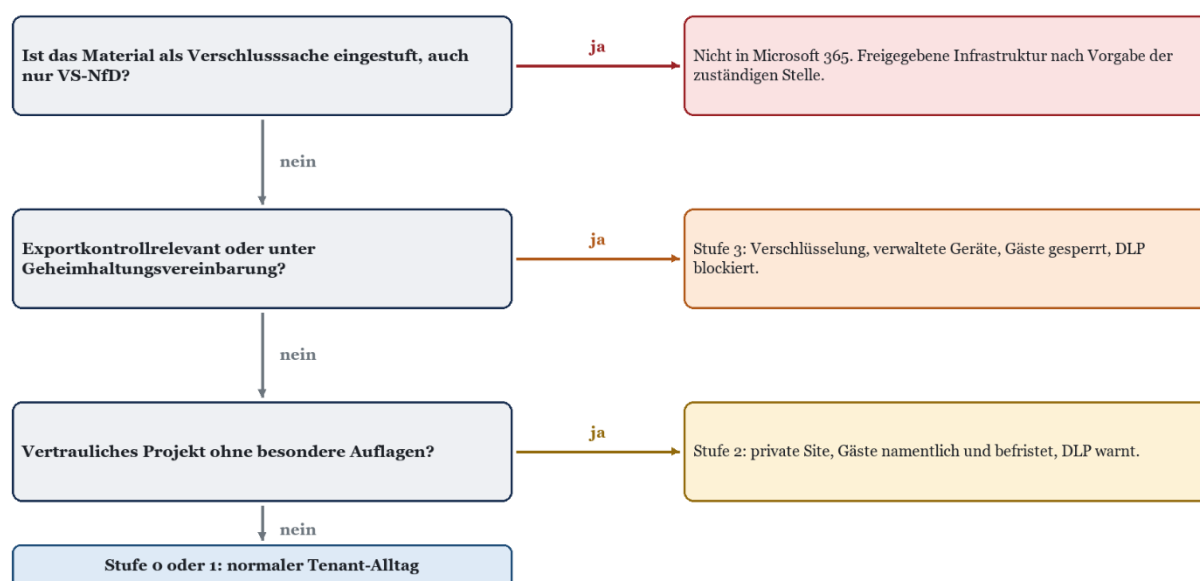
WARNUNG · Kein Label namens „VS-NfD“

Legen Sie im Tenant kein Label an, das wie ein staatlicher Geheimhaltungsgrad heißt. Es suggeriert, dass Verschlusssachen dort verarbeitet werden dürften, und lädt genau dazu ein. Eine Vertraulichkeitsbezeichnung ist eine Kennzeichnung mit Schutzwirkung, aber keine vom BSI zugelassene Lösung für Verschlusssachen. Wer Verschlusssachen bearbeitet, braucht eine eigene, freigegebene Umgebung nach Vorgabe der zuständigen Stelle, und Ihr Geheimschutzbeauftragter weiß, welche.

Für den Tenant bedeutet das zweierlei. Die Hausregel muss klar sagen, dass eingestufte Unterlagen weder hochgeladen noch per Mail verschickt noch in Teams besprochen werden. Und es braucht einen definierten Weg für den Fall, dass es doch passiert: Wer wird informiert, wie wird die Datei entfernt, was geschieht mit Versionen, Papierkorb und Aufbewahrungskopien? Das klingt pessimistisch. Es ist nur realistisch.

Gehört das in den Tenant, und wenn ja, wohin?

Drei Fragen vor dem ersten Hochladen



Skizze 5: Im Zweifel fragt man die Exportkontrolle, nicht den Kollegen, der „das schon immer so gemacht“ hat

Was Labels grundsätzlich nicht leisten

Auch unterhalb der Verschlussachen hat Technik Grenzen, und es ist ehrlicher, sie zu benennen, als sie in einer Präsentation fürs Präsidium wegzulassen. Ein Label verhindert kein Bildschirmfoto mit dem Smartphone, kein Abtippen und kein Gespräch auf dem Flur. Es verhindert nicht, dass jemand mit berechtigtem Zugriff Inhalte in eine neue, ungelabelte Datei kopiert, wenn die Rechte das erlauben. Und es verhindert schon gar nicht die technische Unterstützung, die per Definition im Kopf stattfindet. Was Labels und DLP leisten, ist dreierlei: Sie verhindern Versehen, sie erschweren Absicht, und sie dokumentieren, was geschehen ist. Das ist viel. Es ist nur nicht alles.

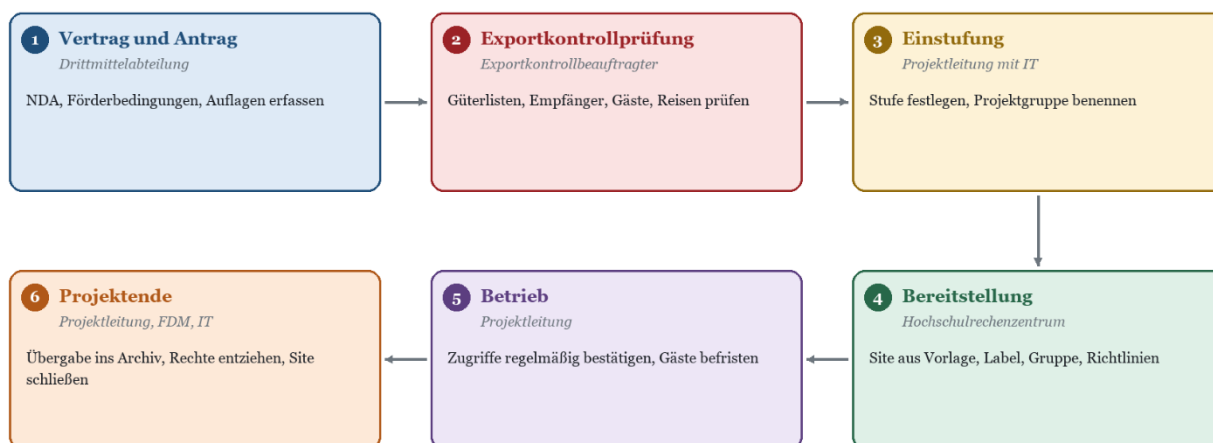
Hinzu kommt die Abhängigkeit vom Anbieter selbst. Wer die Frage stellt, ob ein US-amerikanischer Cloud-Anbieter grundsätzlich auf Projektdaten zugreifen könnte, stellt eine berechtigte Frage, die eine Konfiguration nicht beantwortet. Für Projekte, bei denen der Vertrag oder die Exportkontrolle genau das ausschließen will, gibt es Optionen mit eigener Schlüsselhoheit oder eben eine Bearbeitung außerhalb von Microsoft 365. Die Abwägung dazu beschreibt der Beitrag [Digitale Souveränität an Hochschulen: Was realistisch ist und was Sonntagsrede bleibt](#).

Organisation: Wer prüft, wer stuft ein, wer räumt auf

Die Technik ist in wenigen Wochen eingerichtet. Die Organisation dauert länger, und an ihr scheitern die meisten Vorhaben. Die Exportkontrolle sitzt an vielen Hochschulen im Forschungsdezernat oder in der Drittmittelabteilung, manchmal als halbe Stelle, manchmal als Zusatzaufgabe der Justiziarin. Das Hochschulrechenzentrum erfährt von Industriekooperationen oft erst, wenn das Team schon existiert. Und an außeruniversitären Instituten kommt die Frage hinzu, was die Zentrale der Forschungsgesellschaft vorgibt und was das Institut selbst regelt; dazu mehr im Beitrag [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#).

Vom Vertrag zum Projektraum und zurück

Sechs Schritte, fünf Stellen, ein Ablaufdatum



Skizze 4: Schritt 6 ist der, den alle vergessen. Der Industriepartner vergisst ihn nicht

Rolle	Aufgabe im Prozess	Typischer Stolperstein
Drittmittelabteilung	Erfasst Geheimhaltungsvereinbarungen und Auflagen, meldet neue Projekte mit Schutzbedarf	Vertrag liegt vor, aber niemand informiert die IT
Exportkontrollbeauftragter	Prüft Güter, Empfänger, Gäste und Reisen, gibt Gastzugänge frei	Wird erst nach Projektstart gefragt
Projektleitung	Legt mit der IT die Stufe fest, benennt Mitglieder, bestätigt Zugriffe regelmäßig	Delegiert alles an die studentische Hilfskraft
Hochschulrechenzentrum	Stellt Projekträume aus Vorlage bereit, betreibt Labels, DLP und Conditional Access	Baut Einzellösungen statt Vorlagen
Datenschutzbeauftragte	Bewertet Protokollierung und DLP-Auswertungen, berät bei personenbezogenen Projektdaten	Wird mit Exportkontrolle verwechselt
Personalrat	Beteiligung bei DLP, Protokollierung und Auswertungen nach Landespersonalvertretungsrecht	Erfährt von DLP aus der Richtlinienmeldung
Fakultäts-IT	Unterstützt vor Ort, betreut Projektgeräte	Hat eigene Admin-Rechte und eigene Ideen

DLP, Protokolle und der Personalrat

DLP und Audit erzeugen Daten über das Verhalten von Mitarbeiterinnen und Mitarbeitern: Wer hat wann was an wen geschickt, wer hat eine Warnung übergangen. Das ist in allen Bundesländern ein Thema der Mitbestimmung, aber die Ausgestaltung unterscheidet sich. Die Landespersonalvertretungsgesetze regeln Beteiligungsrechte bei technischen Einrichtungen zur Verhaltens- und Leistungskontrolle unterschiedlich, und auch die Frage, ob und wie wissenschaftliches Personal erfasst ist, wird nicht überall gleich beantwortet. Sinnvoll ist eine Regelung in der Dienstvereinbarung, die festlegt, wofür DLP-Auswertungen genutzt werden dürfen, wer sie einsehen darf und wie lange sie aufbewahrt werden. Wie das konkret aussehen kann, beschreibt der Beitrag [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#). Die datenschutzrechtliche Seite, einschließlich der Unterschiede zwischen den

Landesdatenschutzgesetzen, behandelt [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#).

HINWEIS · Landesrecht unterscheidet sich

Hochschulgesetze, Landesdatenschutzgesetze und Personalvertretungsgesetze sind Ländersache. Ob für eine DLP-Einführung Mitbestimmung, Mitwirkung oder Anhörung gilt und welche Rolle die Landesbeauftragten für den Datenschutz spielen, hängt vom Bundesland und vom Träger ab. Klären Sie das mit Justizariat, Datenschutzbeauftragten und Personalrat, bevor die erste Richtlinie scharf geschaltet wird.

Projektende: Der vergessene Schritt

Geheimhaltungsvereinbarungen enden nicht mit dem Projekt. Viele verlangen, dass Unterlagen nach Ablauf zurückgegeben oder vernichtet werden, oft mit Ausnahme dessen, was für die gute wissenschaftliche Praxis aufbewahrt werden muss. Hier treffen Vertraulichkeit und Forschungsdatenmanagement aufeinander: Was als Beleg für Veröffentlichungen aufbewahrt werden muss, gehört geordnet ins Archiv oder Repositorium, mit passenden Zugangsbeschränkungen; was der Vertrag zur Löschung vorsieht, wird gelöscht und dokumentiert. Die Abgrenzung zwischen Projektraum und Archiv beschreibt [Forschungsdaten in Microsoft 365: Was geht, was nicht, und wo das Forschungsdatenmanagement beginnt](#). Für den Projektraum heißt das: Ablaufdatum bei der Einrichtung setzen, Rechte zum Projektende entziehen, Site schreibschützen und nach Klärung der Aufbewahrung schließen.

TYPISCHE SITUATION · Der Dienstleister, der nie gegangen ist

Aus einem Krankenhausverbund: Ein externer Dienstleister erhielt für ein Migrationsprojekt Gastzugänge zu mehreren Teams. Das Projekt endete, der Vertrag auch, die Gastkonten nicht. Bei einer Überprüfung zwei Jahre später hatten sie noch Zugriff, inzwischen auf deutlich mehr als ursprünglich, weil die Teams gewachsen waren.

Die typische Situation an der Hochschule: Das Kooperationsprojekt mit dem Industriepartner ist abgeschlossen, die Gastkonten der Ingenieure des Partners bleiben aktiv, und im selben Team läuft längst das Folgeprojekt mit einem Wettbewerber. Abhilfe schaffen Ablaufdaten für Gastkonten, Zugriffsüberprüfungen und ein Projektende-Termin, der im Kalender der Projektleitung steht, nicht nur im Vertrag.

Schulung statt Strafandrohung

Die beste Label-Taxonomie nützt nichts, wenn Wissenschaftler sie für eine Schikane der Verwaltung halten. Erfolgreich sind kurze, fallbezogene Formate: Was darf in welchen Raum, was tue ich vor einer Dienstreise, was mache ich, wenn DLP mich stoppt. Für das Hochschulrechenzentrum und die Fakultäts-IT kommt die Betriebsseite hinzu, also Labels pflegen, DLP-Auswertungen lesen, Conditional Access testen. Wer dafür Unterstützung möchte, findet sie in unserer [Microsoft-365-Schulung für Hochschulen und Forschung](#).

FAQ: Exportkontrolle, Labels und DLP in der Forschung

Ist die Exportkontrolle für Hochschulen überhaupt relevant, wenn wir nur Grundlagenforschung betreiben?

Die Ausnahme für Grundlagenforschung ist wichtig, aber eng. Sobald Forschung anwendungsnah wird, etwa in Industriekooperationen, greift sie häufig nicht. Zudem betrifft die Exportkontrolle

auch Geräte, Software und die Zusammenarbeit mit Gästen. Ob ein konkretes Vorhaben erfasst ist, klärt Ihre Exportkontrolle.

Reicht es, wenn die Daten in einem Rechenzentrum in Deutschland liegen?

Nein. Nach Darstellung des BAFA kommt es beim Bereitstellen nicht auf den Serverstandort an, sondern darauf, ob ein Zugriff aus dem Ausland ermöglicht wird und wer ihn einräumt. Der Datenstandort ist für Datenschutz und Souveränität relevant, für die Exportkontrolle allein aber nicht entscheidend.

Dürfen wir VS-NfD-Unterlagen in Microsoft 365 ablegen, wenn wir sie verschlüsseln?

Nicht im regulären Tenant. Das BSI hält die Verarbeitung von Verschlusssachen in Public-Cloud-Diensten nach dem SaaS-Modell derzeit für nicht möglich. Ein Sensitivity Label ist keine zugelassene VS-Lösung. Sprechen Sie mit Ihrem Geheimschutzbeauftragten über eine freigegebene Umgebung.

Wie viele Labels sollten wir einführen?

So wenige wie möglich. Vier Stufen für Dateien und Container decken die meisten Forschungseinrichtungen ab. Projektspezifische Varianten der höchsten Stufe, etwa mit eigener Rechtegruppe, lassen sich als Unterlabels abbilden, sollten aber nicht frei für alle sichtbar sein.

Können Gastwissenschaftler an einem Stufe-3-Projekt mitarbeiten?

Ja, wenn die Exportkontrolle zugestimmt hat. Dann erhält der Gast ein namentliches, befristetes Konto mit Sponsor, wird in die Projektgruppe aufgenommen und bekommt bei Bedarf ein verwaltetes Gerät. Was nicht geht: „erstmal reinnehmen, prüfen wir später“.

Was passiert mit verschlüsselten Dateien, wenn die Projektleitung die Hochschule verlässt?

Die Rechte hängen an der Projektgruppe, nicht an der Person. Deshalb bleibt der Zugriff für die übrigen Mitglieder erhalten. Für den Fall, dass niemand mehr berechtigt ist, braucht es eine geregelte Superuser-Funktion, deren Nutzung protokolliert und mit Datenschutz und Personalrat abgestimmt ist.

Blockiert DLP nicht die normale wissenschaftliche Kommunikation?

Nur wenn man es falsch einführt. DLP-Regeln greifen gezielt bei gelabelten Inhalten der Stufen 2 und 3 und beginnen im Simulationsmodus. Die öffentliche und interne Kommunikation bleibt unberührt.

Ersetzt Geoblocking per Conditional Access die Reiseprüfung?

Nein. Länderbasierte Regeln beruhen auf IP-Adressen, lassen sich umgehen und bilden keine exportrechtliche Bewertung ab. Sie sind eine Ergänzung gegen Versehen, keine Prüfung.

Gilt das auch für Kunst- und Musikhochschulen?

Exportkontrolle betrifft sie seltener, Geheimhaltungsvereinbarungen dagegen durchaus, etwa bei Kooperationen mit Unternehmen, Verlagen oder bei unveröffentlichten Werken. Das Schutzklassenmodell funktioniert dort genauso, meist mit weniger Stufen.

Fazit: Der Tenant schützt, was Sie ihm beibringen

Exportkontrolle und Geheimhaltung sind an Hochschulen keine exotischen Randthemen, sondern Alltag in jeder Fakultät, in der angewandt geforscht wird. Microsoft 365 bringt die Werkzeuge mit, um vertrauliche Projekte wirksam abzuschotten: Vertraulichkeitsbezeichnungen mit Verschlüsselung, private Projekt-Sites, DLP an den Ausgängen, Zugriff nur von verwalteten Geräten und gezielt gesperrte Gastzugänge. Richtig kombiniert, machen sie aus dem offenen Campus-Tenant einen Ort, an dem auch der Industriepartner ruhig schläft.

Zwei Dinge können sie nicht. Sie ersetzen weder die rechtliche Prüfung durch die Exportkontrolle noch die Grenze zu den Verschlussachen, die nach Aussage des BSI derzeit nicht in SaaS-Dienste der Public Cloud gehören. Wer das akzeptiert, baut ein schlankes Schutzklassenmodell, stellt Projekträume aus Vorlage bereit und verankert Prüfung, Einstufung und Projektende in einem Prozess, den Drittmittelabteilung, Exportkontrolle und Hochschulrechenzentrum gemeinsam tragen. Wenn Sie dieses Modell für Ihre Hochschule oder Ihr Institut konzipieren wollen, unterstützen wir Sie mit der [Microsoft-365-Beratung für Hochschulen und Forschung](#). Und die E-Mail mit „ist wahrscheinlich nichts“? Die kommt dann seltener. Und wenn doch, wissen Sie, wo Sie nachsehen.

WEITERLESEN · Weiterlesen

Für diesen Beitrag besonders passend aus der Serie:

- › [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#)
- › [Forschungsdaten in Microsoft 365: Was geht, was nicht, und wo das Forschungsdatenmanagement beginnt](#)
- › [Hochschulübergreifend zusammenarbeiten: B2B, mandantenübergreifender Zugriff und Verbundprojekte](#)
- › [MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps](#)
- › [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#)
- › [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)
- › [Digitale Souveränität an Hochschulen: Was realistisch ist und was Sonntagsrede bleibt](#)
- › [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#)